Az informatikai biztonság matematikai alapjai

Gonda János

HIBAKORLÁTOZÁS

Budapest, 2007

Lektorálta xxxx

Utolsó módosítás: 2018. szeptember 02.

Előszó

Ez a jegyzet az ELTE-n tartott Algebrai kódoláselmélet című tárgy anyagát tartalmazza. A tárgy egyrészt a mesterképzésben, másrészt a doktori iskolában kerül előadásra. A teljes jegyzet a két kurzus együttes anyagát tartalmazza. Az első tizennégy és a 20. fejezet ajánlott az első részhez, míg a további fejezetek azon doktoranduszok számára, akik már a reguláris képzés keretében is tanulták a tárgyat. Tekintettel arra, hogy a tárgy heti két (tan)órában, egy-egy félév keretében kerül előadásra, az anyag ehhez a szűkre szabott időkerethez igazodik, így is az ennyi idő alatt elmondható ismeretek mennyiségének felső határát súrolva, esetleg ezt a korlátot kissé át is lépve. Éppen erre való tekintettel szükséges megjegyezni, hogy bizonyos részek a tényleges előadás és számonkérés során többé vagy kevésbé tömöríthetőek, belőlük egyes részek kihagyhatóak vagy csupán érintőlegesen kerülhetnek szóba. Ez függhet az előadó ízlésétől, a tárgyat hallgatók összetételétől és „előéletétől", a tárgyban tanultakra esetleg támaszkodó további tárgyaktól, az adott félév tényleges hosszától, és még más körülményektől is.

Miről szól a tárgy és ez a jegyzet? A címük szerint az algebrai kódoláselméletről, illetve a hibakorlátozó kódokról. A címek ilyen formán egy teljes, lezárt témát ígérnek a hallgatónak illetve olvasónak. A valóság ezzel szemben lényegesen szegényesebb. A már említett időkorlátot figyelembe véve nem vállalkozhattunk másra, és a valóság is az, hogy csupán az említett témakör egy kis, bár viszonylag jól körülhatárolható részével foglalkozzunk. Amiről szó lesz, az lényegében véve a véletlen hibát javító blokk-kódok elmélete, illetve ennek is csak egy része. Nem foglalkozunk gyakorlati kérdésekkel, csupán érintjük a hibacsomó-javító kódokat, szóba sem kerülnek az egyébként fontos konvolúciós kódok, és csupán burkoltan, más nézőpontból, a kapcsolatot még csak meg sem említve tárgyalunk bizonyos algebrai geometriai kódokat. Igen szűkre szabottan, majdhogynem ismeretterjesztő szinten beszélünk a hibakorlátozás valószínűségi kérdéseiről, ami annyiban érthető, hogy a tárgy a kódolás algebrai vonatkozásaival foglalkozik. Nagyon kevés szó van nemlineáris kódokról, bár helyenként a szokásosnál általánosabban tárgyalunk egyes kérdéseket, kiterjesztve a fogalmakat a nemlineáris kódokra is. Végül a lineáris kódok jelenlegi ismeretanyaga is lényegesen bővebb annál, mint ami egy ilyen csaknem bevezető jellegű tárgy anyagába belefér. Természetesen az összeválogatott anyag sok egyéb mellett a válogatást végző személyiségétől, ízlésétől is függ, vagyis nem nélkülöz bizonyos szubjektivitást sem.

Mivel algebrai kódokról van szó, az anyag megértéséhez szükség van algebrai ismeretekre. Ez részben lineáris algebrát, részben általános algebrai ismereteket (csoportokkal, gyűrűkkel, testekkel, polinomokkal kapcsolatos fogalmakat) jelent, jelenti azonban azt is, hogy lényegesen támaszkodik az általában sokkal kisebb részben oktatott véges testek bizonyos fokú ismeretére. Jóllehet a gyakorlatban alkalmazott kódok túlnyomó többsége bináris, ez nem jelenti azt, hogy csak ilyen kódok vannak és csak ilyeneket használnak a gyakorlatban, sőt, van olyan igen fontos kódosztály, amelyben csak triviális, és így lényegében véve használhatatlan formában léteznek a bináris kódok. Éppen ezért mindenütt általánosan, tetszőleges szimbólumhalmaz, illetve lineáris kód esetén tetszőleges véges test fölött tárgyaljuk a kódokat, és ezen belül utalunk a bináris kódok esetleges speciális tulajdonságaira.

A téma iránt mélyebben érdeklődő olvasó az irodalomjegyzékben említett könyvekből szerezhet további ismereteket, éppen ezért nem csak olyan könyveket soroltunk ott fel, amelyek szorosan kapcsolódnak az általunk kifejtett részletekhez.

Végül néhány jelölésről szólunk. Ebben a jegyzetben $\mathbb{N}^+$ a pozitív egész számokat jelöli, és $\mathbb{N}$ jelöli a nemnegatív egész számokat. Egy polinomot például f-fel, és nem $f(x)$-szel jelölünk, megfelelően annak, hogy a polinom egy formális kifejezés, amelyet az együtthatói határoznak meg. Az f polinomhoz tartozó polinomfüggvény jele $\hat{f}$. A mátrixokat és vektorokat félkövér betű jelöli, a halmazokat dőlt betű, és egy struktúrát a hozzá tartozó halmaztól a betű típusa különbözteti meg, például az A halmazra épített struktúra jele $\mathcal{A}$. Végül a q-elemű test jele ebben a jegyzetben $\mathbb{F}_q$.

Tartalomjegyzék

1. A hibakorlátozásról

Az adatok tárolás illetve átvitel során megváltozhatnak, meghibásodhatnak, ezért szeretnénk olyan eljárást megadni, amellyel kiolvasáskor illetve a vétel helyén észre tudjuk venni, hogy sérült az adat, sőt, amennyiben lehetséges, helyre tudjuk állítani az eredeti állapotot. A fenti cél megvalósítását szolgálja a hibakorlátozás.

Nyilván irreális kívánság, hogy bármely meghibásodást észrevegyünk, hiszen ha egy üzenet úgy sérül, hogy a megváltozott jelsorozat maga is egy értelmes üzenet, akkor semmilyen eszközzel nem vesszük észre a változást. Az is nyilvánvaló, hogy a javításhoz legalábbis észlelni kell a hibát, így minden hibajavító kód egyben jelezni is képes a hibát, de ez visszafelé nem igaz. Ahhoz ugyanis, hogy javítani tudjunk, ahhoz a hiba észlelésén túl azt is tudni kell, hogy az üzenet mely pontján történt a hiba, és milyen hiba lépett fel. Ez utóbbi feltétel automatikusan teljesül, ha az üzenet kódja bináris, hiszen ekkor a meghibásodás azt jelenti, hogy ha a vétel helyén 1-est olvasunk, és tudjuk, hogy ez a bit hibás, akkor az eredeti jegy csakis 0 lehetett, és fordítva.

Mivel a hibakorlátozás szempontjából elvileg közömbös, hogy adattárolásról vagy adatátvitelről van szó, ezért bármelyikről is szólunk, az a másikra is érvényes.

Tegyük fel, hogy az eredeti adatok egy-egy tetszőleges bájtot jelentenek. Ekkor persze semmilyen hibajelzés nem valósítható meg, hiszen bárhol is sérül a bájt, ismét egy érvényes adatot, nevezetesen egy bájtot kapunk. Egészítsünk ki minden bájtot egy kilencedik bittel olymódon, hogy a kilenc bitből vagy páros, vagy páratlan számú legyen 1 (de mindegyik bájtot azonos rendszer szerint, vagyis vagy mindegyiket párosra egészítjük ki, vagy mindegyiket páratlanra, előre rögzített, és a vétel helyén is ismert módon). Ez azt jelenti, hogy ha az eredeti bájt $b_0b_1b_2b_3b_4b_5b_6b_7$, ahol minden $7 \geq i \in \mathbb{N}$-re $b_i \in \{0,1\}$, akkor $b_8 = \left(\bigoplus_{i=0}^{7} b_i\right) \oplus c$, ahol $\oplus$ modulo 2 összeadást jelent (tehát 0 az értéke, ha a közönséges összeg páros, és 1, ha a szokásos összeg páratlan), és c éréke 0, ha páros számú 1-re akarunk kiegészíteni, míg $c = 1$ az ellenkező esetben. b_8 az úgynevezett **paritásbit**. Ha most az átvitel során egy bit meghibásodik, akkor az egyesek számának paritása (vagyis hogy ez a szám páros illetve páratlan) az ellenkezőjére változik, és ezt a vétel helyén az egyesek leszámlálásával könnyen ellenőrizni tudjuk, bármelyik bit is hibásodott meg (tehát akár a paritásbit is lehet hibás), a rendszer egyetlen hibát biztosan észrevesz, és így jelez. Két hiba esetén azonban az egyesek számának paritása változatlan, hiszen vagy két nulla változott 1-re, vagy két 1-es nullára, és mindkét esetben az 1-esek száma kettővel változott, vagy egy 0 1-re, egy 1-es pedig 0-ra változott, amikor az 1-esek száma változatlan, így két hibát ez a rendszer biztosan nem jelez. A fentiek egyszerű folytatásaként könnyű belátni, hogy ez a módszer minden olyan esetben jelez, amikor egy kiegészített bájtban páratlan számú bit hibásodik meg, és soha nem jelez, ha a meghibásodott bitek száma páros. Azt is könnyen beláthatjuk, hogy ez a kódolás hibajavításra nem alkalmas, hiszen csak annyit tudunk, ha egyáltalán tudunk (vagyis ha páratlan számú hiba történt), hogy a kapott adat biztosan nem azonos a küldeménnyel, de bármely bit meghibásodása ugyanolyan eredményt ad, így semmiképpen nem tudjuk megállapítani, hogy melyik bittel történt a baj. Ezt a hibakorlátozást így főleg olyan helyen érdemes alkalmazni, ahol a hibák egymástól függetlenül lépnek fel, és igen kicsi a hiba valószínűsége, továbbá hiba esetén lehetőség van ismétlésre. Ezeknek a kívánalmaknak többé-kevésbé megfelel a számítógép operatív memóriája, így ezekben szinte mindig ezt a fajta hibakorlátozást alkalmazzák, mégpedig a páratlanra való kiegészítéssel. Amikor bekapcsoljuk a számítógépet, és a képernyőn egyre növekvő számot látunk, akkor a gép memóriáját ellenőrzi oly módon, hogy ismert 9-bites adatot ír a memória minden rekeszébe, majd kiolvassa, és megnézi, hogy azt kapta-e, amit adott. A normális működés során minden alkalommal, amikor a gép memóriájába egy bájt beírása történik, a gép automatikusan kiszámítja a bájthoz tartozó paritásbitet, és ezzel együtt tárolja az adatot, majd kiolvasáskor ellenőrzi, hogy a 9 bit paritása páratlan-e, ha nem, akkor hibajelzést ad, míg ha igen, akkor elhagyja a 9. bitet, és a 8-bites bájtot átadja a további feldolgozásra. Az aszinkron adatátvitelnél is alkalmazzák az egyszerű paritásbites ellenőrzést; ilyenkor szokásos a párosra való kiegészítés is.

Most bővítsük az előbbi módszert. Legyen egy adatblokkunk, amelyben minden bájtot egy-egy paritásbittel látunk el az előbb ismertetett módon. Egymás alá írva a blokk így kiegészített bájtjait, összesen kilenc oszlopot kapunk. Most a korábbiakhoz hasonlóan minden oszlopot egészítsünk ki legalul egy-egy paritásbittel:

$$\begin{array}{cccc|c} b_{0,0} & \dots & b_{0,j} & \dots & b_{0,7} & b_{0,8} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ b_{i,0} & \dots & b_{i,j} & \dots & b_{i,7} & b_{i,8} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ b_{n-1,0} & \dots & b_{n-1,j} & \dots & b_{n-1,7} & b_{n-1,8} \\ \hline b_{n,0} & \dots & b_{n,j} & \dots & b_{n,7} & b_{n,8} \end{array}$$

ahol $n > i \in \mathbb{N}$-re $b_{i,0}b_{i,1}b_{i,2}b_{i,3}b_{i,4}b_{i,5}b_{i,6}b_{i,7}$ a blokk i-edik bájtja, és $b_{i,8} = \left(\bigoplus_{j=0}^{7} b_{i,j}\right) \oplus c_V$ ennek a bájtnak a paritásbitje (c_V minden bájt esetén azonos), míg $8 \geq j \in \mathbb{N}$-re $b_{n,j} = \left(\bigoplus_{i=0}^{n-1} b_{i,j}\right) \oplus c_L$ az úgynevezett ellenőrző bájt (szokás az egyes bájtok ellenőrzését végző paritásbiteket **VRC**-nek nevezni, ami a ***V**ertical **R**edundancy **C**heck* kezdőbetűiből álló rövidítés, és ami keresztirányú ellenőrzést jelent, míg az ellenőrző bájt az **LRC**, azaz ***L**ongitudinal **R**edundancy **C**heck*, a hosszirányú ellenőrzés). Ez a rendszer egyetlen hiba esetén képes azt javítani. Ha ugyanis $b_{i,j}$ és csak ez a bit hibás, akkor pontosan egy hiba van az i-edik bájtban, tehát ennek ellenőrzése során hibajelzést kapunk, az összes többi bájt ellenőrzése azt adja, hogy azokban nincs hiba, és hasonlóan, a j-edik és csak a j-edik oszlop ellenőrzésénél hibajelzésre kerül sor, vagyis a két eredményből azt kapjuk, hogy az i-edik bájt j-edik bitje és csak ez a bit hibás, amit ennek a bitnek az invertálásával kijavíthatunk. Minden olyan esetben azonban, amikor az i-edik és csak az i-edik bájtban valamint a j-edik oszlopban és csak a j-edik oszlopban kapunk hibajelzést, azt gondoljuk, hogy ez a bit hibásodott meg, és ezt „javítjuk", vagyis változtatjuk az ellenkezőjére, pedig könnyen beláthatjuk, hogy ellenőrzéskor ugyanerre az eredményre jutunk akkor is, ha minden oszlopban és minden bájtban, kivéve a j-edik oszlopot és i-edik bájtot, páros számú hiba lép fel (ebbe beleértve a hibátlan esetet is 0 hibával), míg a kitüntetett i-edik bájtban és j-edik oszlopban a hibák száma páratlan, tehát ha például az i-edik bájtban a $j+1$-edik bit, valamint az $i+1$-edik bájt j-edik és $j+1$-edik bitje hibásodik meg, és más hiba nem történik. A vétel helyén semmilyen módszerrel nem tudjuk eldönteni, hogy valóban egy hiba történt-e, és így helyesen javítunk, vagy a megfigyelt hibajelzés több hiba együttes hatása, aminek következtében vagy egy addig helyes bitet javítunk helytelenre, vagy egy tényleg hibás bitet javítunk, de még további, felderítetlen hiba is van a vett üzenetben. Hasonlóan előfordulhat, hogy volt hiba, de mi nem vesszük észre, nevezetesen ha minden bájtban és minden oszlopban a hibák száma páros; ennek tipikus példája, amikor négy hiba egy téglalap négy sarkában lép fel, ahol a téglalap két éle egy-egy bájtban van. Végül előfordulhat, hogy egynél több bájtban, vagy/és egynél több oszlopban kapunk hibajelzést, amikor biztosan tudjuk, hogy volt hiba, de a hibák száma egynél nagyobb, így javításra ebben a rendszerben nincs lehetőségünk; ennek legegyszerűbb példája, amikor pontosan két hiba lép fel. A most ismertetett rendszert nevezhetjük **kétdimenziós paritásellenőrzés**nek; ilyet használnak nagy mágnesszalagos tárolóknál (egy bizonyos rögzítési mód esetén, mert többféle is létezik), ahol egymás mellé írják ki egy kiegészített bájt 9 bitjét, és az adatokat mindig blokkosan tárolják (egyébként ilyenkor az LRC után még egy egy vagy két 9-bites bájtból álló további ellenőrző szót is kiírnak, ez az úgynevezett **CRC**, a ***C**yclic **R**edundancy **C**heck*, ciklikus ellenőrzés), ebben az esetben vízszintesen páratlanra, míg függőlegesen párosra egészítenek ki, vagyis $c_V = 1$ és $c_L = 0$. Ilyenkor érdekes kérdés, hogy az ellenőrzőbájt 8-as indexű bitjének értéke azonos-e, ha vízszintesen és függőlegesen számítjuk, és ha nem, akkor milyen c_V és c_L érékeknél lesz az így számított két érték biztosan azonos, illetve ha nem mindig azonos, akkor milyen további feltételtől függ az egyezés, ám ezeket a kérdéseket házi feladatnak hagyjuk.

Egy további hibajavító kódot ismertetünk, az úgynevezett **Hamming-kód**ot, amely szintén egy hiba javítására alkalmas. Legyen $r \geq 2$ egész szám, $n = 2^r - 1$ és $k = n - r$. Most készítsük el azt az $r \times n$ méretű **H** mátrixot, amelyben az $n \geq j \in \mathbb{N}^+$ indexre a j-edik oszlopban a j szám kettes számrendszerbeli felírásának jegyei találhatóak, vagyis ha $j = \sum_{i=0}^{r-1} a_i^{(j)} 2^i$, akkor a mátrix i-edik sorának j-

edik oszlopában, ahol $r > i \in \mathbb{N}$ és $n \geq j \in \mathbb{N}^+$, $H_{i,j} = a_i^{(j)}$ áll (mivel $j \leq n < 2^r$, ezért j biztosan felírható r jeggyel a kettes alapú számrendszerben). Legyen például $r = 3$, ekkor $n = 2^3 - 1 = 7$ és $k = 4$, továbbá $\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$. $r > t \in \mathbb{N}$-re 2^t kettes számrendszerben való felírása olyan, amelyben a 0-tól kezdődő indexelés mellett a t-edik és csak a t-edik jegy 1, az összes többi 0, ezért a $\mathbf{H}$ mátrix r darab oszlopa, amely a 2^t-alakú indexhez tartozik, egy egységmátrixot ad (az előbbi példában az 1., a 2. és 4.), így a mátrix rangja legalább r, ugyanakkor annál nagyobb nem lehet, hiszen r sora van, vagyis $\text{rang}(\mathbf{H}) = r$. Legyen most $\mathbf{c}^T = c_1 \dots c_n$ egy n-méretű sorvektor, amellyel $\mathbf{Hc} = \mathbf{0}$, ahol $\mathbf{c}$ az előbbi $\mathbf{c}^T$-hez tartozó oszlopmátrix, és $\mathbf{0}$ az r-méretű, csupa 0-ból álló oszlopmátrix (a műveleteket modulo 2 végezzük). Az előbbi mátrixegyenlet egy r egyenletből álló n-ismeretlenes homogén lineáris egyenletrendszer. Az együtthatómátrix rangja r, ezért az n darab c_i közül $n - r = k$ szabadon választható, például azok, amelyek indexe nem 2^t-alakú, és a maradék r komponens egyértelműen meghatározható. Legyen $C = \{(c_1 \dots c_n) \in \{0,1\}^n | \mathbf{Hc} = \mathbf{0}\}$, vagyis azon n-dimenziós bináris vektorok halmaza, amelyeknek $\mathbf{H}$-val vett szorzata $\mathbf{0}$. Láttuk, hogy az ilyen vektorokban k komponens szabadon választható (persze nem bármelyik k, csak azok, amelyekkel a kimaradt komponensekhez tartozó indexek $\mathbf{H}$ reguláris részmátrixát határozzák meg, például a fenti példán nem jó választás az utolsó négy komponens, mert a mátrix első három oszlopa lineárisan összefüggő), legyenek ezért a kódolandó üzenetek k-bitesek, és egy-egy ilyen üzenetet egészítsünk ki r bittel úgy, hogy a kapott n-bites vektor eleme legyen a C halmaznak. Tegyük fel, hogy egy ilyen n-bites üzenet az átvitel során megsérül. Ez azt jelenti, hogy bizonyos bitek az ellenkezőjükre változnak, amit úgy is megkaphatunk, ha ezekhez a bitekhez hozzáadunk 1-et modulo 2 (hiszen $0 \oplus 0 = 0 = 1 \oplus 1$ és $0 \oplus 1 = 1 = 1 \oplus 0$), vagyis tegyük fel, hogy $\mathbf{c}$ az eredeti n-bites vektor, és $\boldsymbol{\varepsilon}^T = \varepsilon_1 \dots \varepsilon_n$ a **hibavektor**, akkor a vétel helyére a $\mathbf{v} = \mathbf{c} + \boldsymbol{\varepsilon}$ vektor érkezik. Számítsuk ki a $\mathbf{Hv}$ szorzatot. Mivel $\mathbf{c}$ kódszó, tehát $\mathbf{Hc} = \mathbf{0}$, és a mátrixszorzás disztributív, ezért $\mathbf{Hv} = \mathbf{H}(\mathbf{c} + \boldsymbol{\varepsilon}) = \mathbf{Hc} + \mathbf{H}\boldsymbol{\varepsilon} = \mathbf{H}\boldsymbol{\varepsilon}$. Ha a $\mathbf{H}$ mátrixban a j-edik oszlopot $\mathbf{h}_j$-vel jelöljük, akkor $\mathbf{Hv} = \mathbf{H}\boldsymbol{\varepsilon} = \sum_{j=1}^{n} \mathbf{h}_j \varepsilon_j = \sum_{\varepsilon_j = 1} \mathbf{h}_j$, hiszen ε_i értéke csak 0 és 1 lehet. Ha pontosan egy hiba lépett fel, akkor egy és csak egy indexre, mondjuk s-re lesz ε_j nullától különböző, és ekkor $\mathbf{Hv} = \mathbf{h}_s$. De $\mathbf{H}$ konstrukciója következtében $\mathbf{h}_s$ éppen s kettes számrendszerbeli felírása, vagyis $\mathbf{Hv}$ éppen a hiba helyét adja. Legyen például az előbbi 3×7-es $\mathbf{H}$ mátrixhoz $\mathbf{c}^T = 0100101$, ekkor ellenőrizhető, hogy $\mathbf{Hc} = \mathbf{0}$, vagyis $\mathbf{c}$ kódszó, és tegyük fel, hogy $\boldsymbol{\varepsilon}^T = 0000100$, vagyis az 5. bit és csak ez a bit az üzenet átvitele során megsérül. Ekkor a vétel helyén a $\mathbf{v}^T = 0100001$ bitsorozatot kapjuk, és ismét könnyű számolás mutatja, hogy $\mathbf{Hv} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ (az egyes komponensek összeadását modulo 2 végezzük), ami mint bináris szám éppen 5-öt ad, és éppen ez a hiba helye. Megváltoztatva a vett üzenetben az 5. bitet, a 0100101 bitsorozatot kapjuk, egyezésben az elküldött bitsorozattal.

Nyitott még, hogy egy adott k-bites üzenethez hogyan tudjuk könnyen meghatározni az n-bites kódolt üzenetet. Legyen $b_1 \dots b_k$ az üzenet. A kiszámítandó n-bites $\mathbf{c}^T$-ben a 2-hatványnak megfelelő indexekhez tegyük a kiszámítandó biteket, vagyis legyen $\mathbf{c}$-ben a 2^t indexhez tartozó, egyelőre ismeretlen bit p_t, és a többi helyre helyezzük el eredeti sorrendben a $\mathbf{b}$ vektor bitjeit. $\mathbf{H}$-val szorozva ezt a vektort, egy egyenletrendszert kapunk, mégpedig olyat, hogy minden egyenletben pontosan egy ismeretlen szerepel, így azt könnyen ki tudjuk fejezni. A korábbi $r = 3$ esetben ez azt jelenti, hogy $n = 7$, $k = 4$, az üzenet $\mathbf{b}^T = b_1 b_2 b_3 b_4$, három ellenőrző bit lesz, és ezeket a $2^0 = 1$-, $2^1 = 2$- és $2^2 = 4$-indexű helyekre rakjuk, vagyis $c_1 = p_0$, $c_2 = p_1$, $c_3 = b_1$, $c_4 = p_2$, $c_5 = b_2$, $c_6 = b_3$ és $c_7 = b_4$. Konkrétan legyen az üzenet $\mathbf{b}^T = 0101$. Ekkor $\mathbf{c}^T = p_0 p_1 0 p_2 101$, és a $\mathbf{Hc}$ szorzat, amelynek az értéke $\mathbf{0}$,

$$p_0 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + p_1 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + p_2 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + 0 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Átrendezés és kissé másként való írás után ebből azt kapjuk, hogy teljesülnie kell a

$$\begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} = 0\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 1\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + 0\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 1\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

mátrixegyenletnek, azaz $p_0 = 0$, $p_1 = 1$ és $p_2 = 0$, ahonnan $\mathbf{c}^T = 0100101$ (nem véletlenül a korábban már használt kódszót kaptuk). Ha az egyszerűbb írásmód kedvéért **H** oszlopait átrendezzük olyan sorrendben, hogy a bal szélén álljon az egységmátrix, amelyet a 2-hatványhoz tartozó indexek jelölnek ki, és ettől jobbra helyezkedik el **H** többi oszlopa az eredeti sorrendben, akkor

$$\begin{pmatrix} p_0 \\ \vdots \\ p_{r-1} \end{pmatrix} = \sum_{b_j=1} h'_{j+r},$$

ahol $\mathbf{h}'_i$ az átrendezett mátrix i-edik oszlopa. Ismét az előbbi példával $\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ az átrendezett mátrix, és a $\mathbf{b}^T = b_1b_2b_3b_4$ üzenethez tartozó paritásbitek

$$\begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} = b_1\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + b_2\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + b_3\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + b_4\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} b_1 \oplus b_2 \oplus b_4 \\ b_1 \oplus b_3 \oplus b_4 \\ b_2 \oplus b_3 \oplus b_4 \end{pmatrix}.$$

Az ellenőrzést és a javítást már láttuk: megszorozzuk **H**-t a beérkezett n-nessel jobbról, és a **Hv** által mint bináris számmal meghatározott helyen lévő bitet az ellenkezőjére változtatjuk, ha a szorzat értéke nem nulla. Ez az eljárás azonban ismét helytelen eredményre vezet, ha a hibák száma nagyobb, mint egy. Házi feladat annak meggondolása, hogy ha két hiba van, akkor egy, az előbbi két helytől különböző harmadik helyen, azaz egy hibátlan bitet javítunk, míg ha három hiba van, akkor előfordul, hogy a szorzat értéke $\mathbf{0}$, vagyis azt hisszük, hogy nem volt hiba, míg ha a szorzat nem nulla, akkor biztosan egy negyedik helyen „javítunk". Mindenesetre az esetleges (néha hibás) javítás után a kódszóról leválasztva a paritásbiteket, visszakapjuk az eredeti üzenetet (feltéve, hogy legfeljebb egy hiba volt, és így helyesen dekódoltunk). Ismét a korábbi példával, ha a vett bitsorozat, amint láttuk, 0100001, akkor javítás után a 0100101 kódszót kaptuk, és leválasztva a paritásbiteket, amelyek ebben a sorozatban az 1., 2. és 4. helyen állnak, kapjuk a 0101 üzenetet. Ha viszont eredetileg ismét ez volt az üzenet, de az átvitel során a 3. és 7. bit sérül, akkor $\mathbf{v}^T = 0110100$, ezt **H**-val szorozva $\mathbf{Hv} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, ezért átfordítjuk **v**-ben a 4. bitet, ekkor azt kapjuk, hogy 0111100, és kihámozva az üzenetbiteket azt gondoljuk, hogy az eredeti üzenet 1100, ami hibás eredmény. Konklúzióként azt mondhatjuk, hogy a Hamming-kód is viszonylag kis hibavalószínűség esetén alkalmazható.

A Hamming-kódhoz az eredeti üzenetek hossza olyan k érték kell, hogy legyen, amelyhez van olyan pozitív egész r, amellyel $k = 2^r - r - 1$ (ilyen például $4, 11, 26, 57$, stb.). Ez nem feltétlenül szükséges: ha k nem ilyen érték, akkor az üzenetet megfelelő számú nullával kiegészítve, kódolás után ezeket a nullákat elhagyhatjuk, míg dekódolás előtt ismét beírjuk őket, és dekódolás után megint eldobjuk.

Eddig két olyan kódot ismertettünk, amelyek egy hiba esetén helyesen javítottak, de két hibát nem. Vannak az előbbieknél bonyolultabb kódok, amelyek több hiba esetén is helyesen javítanak. A továbbiakban részletesebben foglalkozunk az itt elmondottakkal.

2. A kódtér geometriája

2.1. Definíció

Legyen S nem üres véges halmaz, és $n \in \mathbb{N}^+$. Ekkor az S^n **u** és **v** elemének **Hamming-távolság**a $d(\mathbf{u},\mathbf{v}) = |\{n > i \in \mathbb{N} | u_i \neq v_i\}|$, és ha C az S^n legalább két elemből álló részhalmaza, akkor $d(C) = \min_{\substack{\mathbf{u}\in C \\ \mathbf{u}\neq\mathbf{v}\in C}} \{d(\mathbf{u},\mathbf{v})\}$ **a** C **(minimális) távolsága**.

Amennyiben $\mathcal{S}$ additív Abel-csoport a 0 neutrális elemmel, akkor $w(\mathbf{u}) = |\{n > i \in \mathbb{N} | u_i \neq 0\}|$ az **u Hamming-súlya**, és ha még a $C \subseteq S^n$ halmazra $C \setminus \{\mathbf{0}\} \neq \emptyset$, úgy $w(C) = \min_{\mathbf{0}\neq\mathbf{u}\in C} \{w(\mathbf{u})\}$ **a** C **(minimális) súlya**, ahol $\mathbf{0} = \underbrace{0 \ldots 0}_{n}$.

Δ

A definíció alapján $|C| \leq 1$ esetén C távolsága, $C \subseteq \{\mathbf{0}\}$-nál C súlya definiálatlan.

2.2. Tétel

Legyen $S \neq \emptyset$ véges halmaz, $n \in \mathbb{N}^+$, $C \subseteq S^n$. Ekkor

- a Hamming-távolság metrika az S^n halmazon;
- ha $|C| \geq 2$, akkor $d(C) \in \mathbb{N}$, és van olyan $(\mathbf{u},\mathbf{v}) \in C \times (C \setminus \{\mathbf{u}\})$, hogy $d(\mathbf{u},\mathbf{v}) = d(C)$;

ha S Abel-csoport a 0 neutrális elemmel, $\mathbf{0}$ a csupa 0-ból álló vektor, és tetszőleges $\mathbf{u} \in S^n$, $\mathbf{v} \in S^n$, elemekkel $\mathbf{u} - \mathbf{v} = u_1 - v_1, \ldots, u_n - v_n$, akkor

- $d(\mathbf{u},\mathbf{v}) = w(\mathbf{u} - \mathbf{v})$ és $w(\mathbf{u}) = d(\mathbf{u},\mathbf{0})$;
- ha a legalább kételemű $C \subseteq S^n$ olyan, hogy $C - C \subseteq C$ is teljesül, akkor $d(C) = w(C)$;
- ha $C \setminus \{\mathbf{0}\} \neq \emptyset$, akkor $w(C) \in \mathbb{N}$, és létezik C-nek olyan **u** eleme, amelyre $w(\mathbf{u}) = w(C)$.

Δ

Bizonyítás:

1. $d(\mathbf{u},\mathbf{v})$ minden S^n-beli rendezett párra értelmezett, értéke mint egy véges halmaz számossága nemnegatív egész, vagyis egyben nemnegatív valós szám, és egy adott **u**, **v** párhoz pontosan egy ilyen számérték tartozik, ezért d egy $S^n \times S^n \to \mathbb{R}_0^+$ leképezés ($\mathbb{R}_0^+$ a nemnegatív valós számok halmaza), továbbá $d(\mathbf{u},\mathbf{v})$ pontosan akkor 0, ha minden fellépő i indexre u_i és v_i azonos, azaz ha $\mathbf{u} = \mathbf{v}$. A szimmetria nyilvánvaló, hiszen a nem-egyenlőség szimmetrikus tulajdonság, ezért még a háromszög-egyenlőtlenséget kell megvizsgálni. Ha **z** is S^n eleme, akkor $u_i = z_i$ és $z_i = v_i$ esetén $u_i = v_i$, ami megfordítva azt jelenti, hogy ha egy adott i-re $u_i \neq v_i$, akkor vagy u_i nem egyezik z_i-vel, vagy z_i és v_i különbözik, így egy olyan i index, amely szerepel $d(\mathbf{u},\mathbf{v})$ meghatározásában, eleme a $d(\mathbf{u},\mathbf{z})$-t és $d(\mathbf{z},\mathbf{v})$-t meghatározó indexhalmaz legalább egyikének, tehát $d(\mathbf{u},\mathbf{v}) \leq d(\mathbf{u},\mathbf{z}) + d(\mathbf{z},\mathbf{v})$.

2. $d(C)$ meghatározásában nem egyenlő **u** és **v** elemek szerepelnek, ezért a definícióban szereplő halmaz minden eleme pozitív egész szám, és a halmaz nem üres, ezért ez a halmaz a természetes számok halmazának nem üres részhalmaza, így van benne egy és csak egy legkisebb pozitív egész, de akkor ez valamely **u**, **v** pár távolsága.

3. Abel-csoportban $u_i = v_i$ és $u_i - v_i = 0$ egyszerre igaz, így az $u_i \neq v_i$-t és $u_i - v_i \neq 0$-t teljesítő i indexek azonosak, $d(\mathbf{u},\mathbf{v}) = w(\mathbf{u} - \mathbf{v})$, amiből $\mathbf{v} = \mathbf{0}$ helyettesítéssel $w(\mathbf{u}) = d(\mathbf{u},\mathbf{0})$, hiszen $\mathbf{0}$-ban minden i-re 0 áll, és tetszőleges u_i-re $u_i - 0 = u_i$.

4. Most legyen $C \subseteq S^n$ legalább kételemű, és $C - C \subseteq C$. Míg **u** és **v** végigfut minden C-beli különböző elempáron, azalatt $\mathbf{u} - \mathbf{v}$ egy-egy C-beli, $\mathbf{0}$-tól különböző elem lesz, ezért az adott $d(\mathbf{u},\mathbf{v})$ érték szerepel $w(C)$ meghatározásában is. De fordítva is igaz a dolog: ha **u** a C egy nem nulla eleme,

akkor $d(\mathbf{u},\mathbf{0})$ benne lesz a $d(C)$-t definiáló halmazban, ezért a két halmaz, de akkor a minimumuk is azonos.

5. Ez hasonló a $d(C)$-re vonatkozó kijelentés bizonyításához.

□

A súly definíciója alapján $w(-\mathbf{u}) = w(\mathbf{u})$, és $d(\mathbf{u},\mathbf{v}) \geq |d(\mathbf{u},\mathbf{w}) - d(\mathbf{w},\mathbf{v})|$ a háromszög-egyenlőtlenségből. Szintén a háromszög-egyenlőtlenség alapján

$$w(\mathbf{u}+\mathbf{v}) = w\big(\mathbf{u}-(-\mathbf{v})\big) = d(\mathbf{u},-\mathbf{v}) \leq d(\mathbf{u},\mathbf{0}) + d(\mathbf{0},-\mathbf{v})$$
$$= w(\mathbf{u}) + w(-\mathbf{v}) = w(\mathbf{u}) + w(\mathbf{v})$$

illetve

$$w(\mathbf{u}+\mathbf{v}) = w\big(\mathbf{u}-(-\mathbf{v})\big) = d(\mathbf{u},-\mathbf{v}) \geq |d(\mathbf{u},\mathbf{0}) - d(\mathbf{0},-\mathbf{v})|$$
$$= |w(\mathbf{u}) - w(-\mathbf{v})| = |w(\mathbf{u}) - w(\mathbf{v})|,$$

vagyis a súlyokra is teljesül a háromszög-egyenlőtlenség.

A továbbiakban általában $d(C)$ helyett d-t, $w(C)$ helyett w-t írunk.

2.3. Megjegyzés

1. Legyen S nem üres, véges halmaz és $n \in \mathbb{N}^+$. S-t **szimbólumhalmaz**nak, $C \subseteq S^n$-t **kód**nak nevezzük, $\mathbf{v} \in S^n$ egy S **fölötti** n**-hosszúságú szó**, és $\mathbf{u} \in C$ egy S **fölötti kódszó**. Ha $M = |C|$, $d(C) = d$ és $q = |S|$, akkor C egy $(n, M, d)_q$**-paraméterű kód**. A jelölésben q-t és d-t, egymástól függetlenül, el lehet hagyni.

2. A **hibakorlátozó kód**ok szinte mindig egyenletesek, azaz azonos hosszúságúak a kódszavak (ha nem így lenne, és hiba van az átvitel során, akkor esetleg már a kódszóhatárok sem ismerhetőek fel). A továbbiakban feltesszük, hogy nincs **szinkronhiba**, azaz a vétel során ugyanannyi szimbólum detektálható, mint amennyit elküldtünk, a vett szó hossza azonos az elküldött szó hosszával (ez nem mindig igaz, és vannak olyan kódok, amelyek képesek detektálni, és esetleg – legalábbis részben – javítani a szinkronhibát).

Δ

2.4. Definíció

Legyen S nem üres, véges halmaz, $n \in \mathbb{N}^+$ és $t \in \mathbb{R}_0^+$. Ekkor $G_t(\mathbf{u}) = \{\mathbf{v} \in S^n | d(\mathbf{u},\mathbf{v}) \leq t\}$, ahol $\mathbf{u} \in S^n$, az S^n**-beli u középpontú,** t **sugarú gömb**.

Δ

2.5. Tétel

Legyen $S \neq \emptyset$ véges halmaz, $n \in \mathbb{N}^+$**,** $C \subseteq S^n$, $|C| \geq 2$ és $t \in \mathbb{N}$. Ha $t < \frac{d}{2}$, akkor a C-beli középpontú, t-sugarú gömbök páronként diszjunktak, de $t \geq \frac{d}{2}$ esetén van olyan $\mathbf{u} \in C$, $\mathbf{u} \neq \mathbf{v} \in C$, hogy $G_t(\mathbf{u}) \cap G_t(\mathbf{v}) \neq \emptyset$.

Δ

Bizonyítás:

Ha $\mathbf{u} \in C$, $\mathbf{u} \neq \mathbf{v} \in C$, $t \in \mathbb{N}$, és az S^n-beli $\mathbf{x}$-re $\mathbf{x} \in G_t(\mathbf{u}) \cap G_t(\mathbf{v})$, akkor $d(\mathbf{u},\mathbf{x}) \leq t$ és $d(\mathbf{v},\mathbf{x}) \leq t$, azaz $2t = t + t \geq d(\mathbf{u},\mathbf{x}) + d(\mathbf{x},\mathbf{v}) \geq d(\mathbf{u},\mathbf{v}) \geq d$, tehát $t \geq \frac{d}{2}$, így $t < \frac{d}{2}$ esetén a C-beli középpontok köré írt gömbök páronként diszjunktak.

Nézzük a második állítást. Korábban beláttuk, hogy van olyan $\mathbf{u}$ és $\mathbf{v} \neq \mathbf{u}$ vektor C-ben, amelyekkel $d(\mathbf{u},\mathbf{v}) = d$. Ez azt jelenti, hogy $\mathbf{u}$ és $\mathbf{v}$ pontosan $d(\leq n)$ helyen tér el egymástól, mondjuk a $0 \leq i_1 < \cdots < i_d < n$-indexű komponensekben. Legyen $\mathbf{z} \in S^n$ $\mathbf{u}$-val azonos, kivéve az előbbi indexek közül $\left\lceil \frac{d}{2} \right\rceil$ helyet, ahol $\mathbf{v}$-vel egyenlő. Ekkor $d(\mathbf{u},\mathbf{z}) = \left\lceil \frac{d}{2} \right\rceil$ és $d(\mathbf{z},\mathbf{v}) = d - \left\lceil \frac{d}{2} \right\rceil = \left\lfloor \frac{d}{2} \right\rfloor$. $t \in \mathbb{N}$ és $t \geq \frac{d}{2}$, továbbá $\left\lfloor \frac{d}{2} \right\rfloor \leq \frac{d}{2} \leq \left\lceil \frac{d}{2} \right\rceil < \frac{d}{2} + 1$, így $t \geq \left\lceil \frac{d}{2} \right\rceil$, ezért $d(\mathbf{u},\mathbf{z}) = \left\lceil \frac{d}{2} \right\rceil \leq t$ és $d(\mathbf{z},\mathbf{v}) = \left\lfloor \frac{d}{2} \right\rfloor \leq t$, azaz $\mathbf{z} \in G_t(\mathbf{u})$ és $\mathbf{z} \in G_t(\mathbf{v})$, vagyis $\mathbf{z} \in G_t(\mathbf{u}) \cap G_t(\mathbf{v})$, ez a C-beli középpontú két gömb nem idegen.

□

2.6. Következmény

Legyen $S \neq \emptyset$ véges halmaz, $n \in \mathbb{N}^+$, $C \subseteq S^n$, $|C| \geq 2$, $\mathbf{u} \in C$ és $\mathbf{x} \in S^n$. Ha $d(\mathbf{u},\mathbf{x}) < \frac{d}{2}$, akkor minden $C \setminus \{\mathbf{u}\}$-beli $\mathbf{v}$ vektorra $d(\mathbf{u},\mathbf{x}) < d(\mathbf{v},\mathbf{x})$, míg $d(\mathbf{u},\mathbf{x}) \geq \frac{d}{2}$ esetén ez nem feltétlenül igaz.

Δ

A tétel lényege, hogy $\frac{d}{2}$ egy vízválasztó. Amennyiben egy kódszó az átvitel során ennél kevesebb helyen hibásodik meg, akkor a megérkezett szó a kódszavak közül az eredeti, elküldött kódszóhoz van legközelebb, attól tér el a legkevesebb helyen, viszont ha a hibák száma legalább ennyi, akkor ez nem feltétlenül igaz, sőt, biztosan van olyan kódszó és olyan hiba, amikor ez nem igaz.

Bizonyítás:

Legyen $\mathbf{v} \in C \setminus \{\mathbf{u}\}$, és $d(\mathbf{u},\mathbf{x}) < \frac{d}{2}$. Ekkor $\frac{d}{2} + d(\mathbf{x},\mathbf{v}) > d(\mathbf{u},\mathbf{x}) + d(\mathbf{x},\mathbf{v}) \geq d(\mathbf{u},\mathbf{v}) \geq d$-ből átrendezés után kapjuk, hogy $d(\mathbf{x},\mathbf{v}) > d - \frac{d}{2} = \frac{d}{2} > d(\mathbf{u},\mathbf{x})$. Ha viszont $\mathbf{u}$, $\mathbf{v}$ és $\mathbf{x} = \mathbf{z}$ az előző tétel bizonyításában szereplő három elem, úgy $d(\mathbf{u},\mathbf{x}) = \left\lceil \frac{d}{2} \right\rceil \geq \frac{d}{2} \geq \left\lfloor \frac{d}{2} \right\rfloor = d(\mathbf{x},\mathbf{v})$.

□

Hiba jelzésére alkalmas blokk-kódot könnyű szerkeszteni: ehhez elegendő, ha C valódi része S^n-nek, hiszen ha vételnél egy $S^n \setminus C$ elemet találunk, biztosak lehetünk benne, hogy hiba történt az átvitel során. Tovább visszük a gondolatot: partícionáljuk S^n-t, és legyen C olyan, hogy minden osztállyal legfeljebb egy közös pontja van. Ezt úgy használhatjuk hibajavításra, hogy amennyiben a vett jel egy olyan osztályban van, amelyben található kódszó, akkor úgy tekintjük, mintha ez a kódszó lett volna az üzenet, ellenkező esetben jelezzük, hogy hibás volt az átvitel. Természetesen a jelzés elmarad, ha a továbbítás során úgy változott meg a közlemény, hogy az eredmény is eleme C-nek, illetve javító kód esetén maga is egy kódszó, hiszen ekkor a hiba rejtve marad; hasonlóan hibajavítás esetén helytelenül korrigálunk, ha a vett szó nem abba az osztályba esik, amelyben az eredeti található, de olyanba, amelyben van reprezentáns. A probléma mindkét módszernél az S^n halmaz megfelelő felosztása, és javítás esetén a reprezentánsok megfelelő kiválasztása. Ez utóbbi a **dekódolás** problémája.

2.7. Definíció

Legyen A és S nem üres véges halmaz, $|S| = q$, $n \in \mathbb{N}^+$, és $\varphi: A \to S^n$ injektív. A φ A^+-ra való homomorf kiterjesztése által meghatározott betűnkénti kód **blokk-kód**.

Δ

Rögtön látható, hogy a fenti C kód egy $(n, M)_q$-paraméterű kód, ahol $M = |A|$. Egyébként a blokk-kódolás mellett létezik más kódolási eljárás is, ezzel azonban nem foglalkozunk.

Most egy speciális dekódolási sémát ismertetünk.

2.8. Definíció

Legyen $S \neq \emptyset$ véges halmaz, $n \in \mathbb{N}^+$ és $C \subseteq S^n$. $f: S^n \to C$ a **döntési függvény** vagy **döntési séma**, és f **minimális távolságú dekódolás**, ha minden $\mathbf{v} \in S^n$-re $d\big(\mathbf{v}, f(\mathbf{v})\big) = \min\limits_{\mathbf{u} \in C}\{d(\mathbf{u}, \mathbf{v})\}$.

Δ

A hibajavítás minimális távolságú dekódolás esetén tehát úgy történik, hogy amikor beérkezik n szimbólum, akkor megkeressük azt a (illetve egy olyan) kódszót, amely a legkevesebb helyen tér el a vett n-estől. Ezt vagy úgy tesszük, hogy a vétel helyén csak a kódszavakat tároljuk, és a beérkezett szót mindegyik kódszóval összehasonlítva kikeressük a(z egyik) legközelebb fekvő kódszót, vagy tároljuk az összes lehetséges szót, és mindegyikhez a hozzá legközelebb lévő (egyik) kódszót, vagyis a döntési függvényt, és ez esetben csupán a táblázatban kell kikeresni a beérkezett szót, és a hozzá tartozó kódszó megadja a dekódolást. Az előbbi esetben kisebb tárra, de hosszabb számolásra van szükség, míg a második esetben fordított a helyzet, vagyis most is a számítástechnikában szokásos tárméret - futási idő cserearány problémájával állunk szemben.

A blokk-kódolás esetén a minimális távolságú dekódolás szinte kizárólagos, jóllehet nem minden esetben eredményezi a legkisebb hibavalószínűséget.

2.9. Definíció

Legyen $t \in \mathbb{N}$. Egy kód t**-hiba jelző**, ha tetszőleges üzenetben előforduló minden legfeljebb t számú hibát képes jelezni, és t**-hiba javító**, ha tetszőleges üzenetben előforduló minden legfeljebb t számú hibát képes javítani. A kód **pontosan** t**-hiba jelző**, amennyiben t-hiba jelző, de van olyan $t+1$ hiba, amelyet nem jelez, és **pontosan** t**-hiba javító**, ha t-hiba javító, de van olyan $t+1$ hiba, amelyet nem javít, vagy hibásan javít.

Δ

A definícióban lényeges, hogy ha egy kód pontosan t-hiba jelző, az nem jelenti azt, hogy t-nél több hibát nem képes jelezni, csupán azt, hogy van legalább egy ilyen $t+1$ hibát tartalmazó hibaminta. Ha visszagondolunk a bevezetőben említett paritásbites kódra, tehát ahol egy n-bites bináris szót úgy toldottunk meg egy bittel, hogy a keletkezett $n+1$-bites szóban az 1-esek száma páros legyen, akkor tudjuk, hogy ez a kód minden olyan esetben jelez, ha a hibák száma páratlan, de soha nem jelez, ha páros számú helyen történt hiba, vagyis ez a kód 1-hiba jelző, jóllehet bármely olyan esetben jelzi, hogy hiba történt, ha például a hibák száma három. Olyan pontosan t-hiba jelző kódra is lehetne példát mutatni, amelyben van olyan $t+1$ hibát tartalmazó hibaminta, amelyet képes a rendszer jelezni.

Az előbbi megállapítások igazak a hibajavításra is.

2.10. Tétel

Egy (n, M, d)-kód akkor és csak akkor t-hiba jelző, ha $t < d$, és akkor és csak akkor pontosan t-hiba jelző, ha $t = d - 1$. Minimális távolságú dekódolással a kód akkor és csak akkor t-hiba javító, ha $t < \frac{d}{2}$, és akkor és csak akkor pontosan t-hiba javító, ha $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Δ

Bizonyítás:

Minden d-távolságú kódban van olyan $\mathbf{u}$, $\mathbf{v}$ pár, amelyre $d(\mathbf{u}, \mathbf{v}) = d$. Ha egy ilyen $\mathbf{u}$ üzenetben a d hiba úgy lép fel, hogy $\mathbf{u}$ átmegy $\mathbf{v}$-be, akkor a hibát nem tudjuk jelezni; viszont $\mathbf{u}$-ban bárhogy lép is fel d-nél kevesebb (de lagalább 1) hiba, a keletkező elem nem lehet kódszó, mivel két kódszó között legalább d pozícióban különbség van.

Korábban láttuk, hogy $t < \frac{d}{2}$ esetén a vett szó az eredeti kódszóhoz van legközelebb, minden más kódszó távolabb esik a vett szótól, ezért minimális távolságú dekódolással helyesen döntünk, a dekódolás helyes. Mivel abban az esetben, ha t egész szám, $t < \frac{d}{2}$ ekvivalens a $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ relációval, ezért ez egyben azt is jelenti, hogy minimális távolságú dekódolással minden olyan esetben helyesen javítunk, amikor a hibák száma nem nagyobb, mint $\left\lfloor \frac{d-1}{2} \right\rfloor$. Ha viszont $t \geq \frac{d}{2}$, akkor van két nem idegen, kódszóközéppontú gömb. Legyen $\mathbf{u}$ és $\mathbf{v}$ két olyan kódszó, amelyek távolsága éppen d, és $\mathbf{x}$ az a szó, amely $\mathbf{u}$-tól $\left\lfloor \frac{d}{2} \right\rfloor$, $\mathbf{v}$-től pedig $\left\lceil \frac{d}{2} \right\rceil$ távolságra van. Tudjuk, hogy ekkor minden más kódszótól is legalább $\left\lceil \frac{d}{2} \right\rceil$ távolságra fekszik $\mathbf{x}$. Legyen f a minimális távolságú dekódolás dekódoló függvénye. Ha az előbbi két távolság nem azonos, akkor nyilván $f(\mathbf{x}) = \mathbf{u}$, ellenkező esetben $f(\mathbf{x})$ bármely olyan kódszó lehet, amely $\mathbf{x}$-től $\frac{d}{2}$ távolságra van, tehát lehet például ismét $\mathbf{u}$. Ekkor abban az esetben, ha $\mathbf{v}$-t küldjük, és a beérkezett szó $\mathbf{x}$, akkor a hibák száma $\left\lceil \frac{d}{2} \right\rceil = \left\lfloor \frac{d-1}{2} \right\rfloor + 1$, és ezt a vett szót hibásan javítjuk, hiszen nem $\mathbf{v}$-re, hanem $\mathbf{u}$-ra döntünk, ami azt jelenti, hogy egy d-távolságú kód esetén minimális távolságú dekódolással minden, legfeljebb $\left\lfloor \frac{d-1}{2} \right\rfloor$ hiba javítható, de van olyan $\left\lfloor \frac{d-1}{2} \right\rfloor + 1$ hiba, amelyet rosszul javítunk, így a minimális távolságú dekódolással a d-távolságú kód pontosan $\left\lfloor \frac{d-1}{2} \right\rfloor$-hiba javító.

□

Végül általánosítjuk a hibajelzés - hibajavítás feladatát. Két általánosításról lesz szó.

Legyen C egy (n, M, d)-paraméterű kód, és t, valamint a t-nél nem kisebb s olyan nemnegatív egész számok, hogy $t + s = d - 1$. Ekkor megadható olyan döntési függvény, amely minden t-nél nem több hibát javít, és s-nél nem több hibát jelez. Legyen ugyanis a $\mathbf{v}$ szóra $f(\mathbf{v}) = \mathbf{u}$, ahol $\mathbf{u}$ kódszó, akkor és csak akkor, ha $d(\mathbf{u}, \mathbf{v}) \leq t$. Mivel $2t = t + t \leq t + s = d - 1 < d$, ezért $t < \frac{d}{2}$, tehát a kódszavak körüli t-sugarú gömbök diszjunktak, így egy $\mathbf{v}$-hez legfeljebb egy kódszót rendel f. Ha $d(\mathbf{u}, \mathbf{v}) = t'$, és $\mathbf{u} \neq \mathbf{u}' \in C$, akkor $d - 1 < d \leq d(\mathbf{u}, \mathbf{u}') \leq d(\mathbf{u}, \mathbf{v}) + d(\mathbf{v}, \mathbf{u}') = t' + d(\mathbf{v}, \mathbf{u}')$, és innen kapjuk, hogy $d(\mathbf{v}, \mathbf{u}') > d - 1 - t'$. $t' \leq t$ esetén $d(\mathbf{v}, \mathbf{u}') > d - 1 - t' \geq d - 1 - t = s \geq t \geq t' = d(\mathbf{u}, \mathbf{v})$, így azon szavakra, amelyeket javít a rendszer, a dekódolás minimális távolságú. Ha viszont $t < t' \leq s$, akkor $d(\mathbf{v}, \mathbf{u}') > d - 1 - t' \geq d - 1 - s = t$, vagyis $\mathbf{v}$ valamennyi kódszótól t-nél nagyobb távolságra van, így a vett szót nem javítjuk, de jelezhetjük a hibát.

Az előbbi séma két szélső esete, ha $s = t$, illetve ha $t = 0$. Az első esetben visszajutunk a tiszta minimális távolságú dekódoláshoz, míg a második eset a hibajelző kód, ekkor ugyanis nem javítunk, csak jelezzük a hibát.

A másik módosításhoz legyen $2t + r = d - 1$, ahol t és r nemnegatív egész számok, $\mathbf{u}$ egy kódszó, és $\mathbf{v}$ egy olyan szó, amely $\mathbf{u}$-ból $t' + r'$ hibával áll elő, ahol $t' \leq t$ és $r' \leq r$. Tegyük fel, hogy az r' hibának ismerjük a helyét (például ezeken a pozíciókon olyan jel van, amely nem eleme az input-ábécének). Legyen $\mathbf{u}'$ tetszőleges, az $\mathbf{u}$-tól különböző kódszó, és $\tilde{\mathbf{u}}$, $\tilde{\mathbf{v}}$ és $\tilde{\mathbf{u}}'$ olyan, $n - r'$ komponensű szavak, amelyeket rendre $\mathbf{u}$-ból, $\mathbf{v}$-ből és $\mathbf{u}'$-ből kapunk, ha az ismert hibáknak megfelelő r' pozíciót elhagyjuk. Ekkor

$$d - 1 < d \leq d(\mathbf{u}, \mathbf{u}') \leq d(\tilde{\mathbf{u}}, \tilde{\mathbf{u}}') + r' \leq d(\tilde{\mathbf{u}}, \tilde{\mathbf{v}}) + d(\tilde{\mathbf{v}}, \tilde{\mathbf{u}}') + r'$$
$$= t' + r' + d(\tilde{\mathbf{v}}, \tilde{\mathbf{u}}') \leq t + r + d(\tilde{\mathbf{v}}, \tilde{\mathbf{u}}'),$$

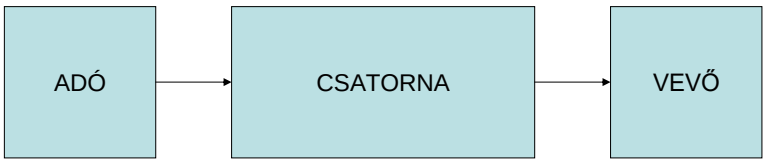
majd ebből $d(\tilde{\mathbf{v}}, \tilde{\mathbf{u}}') > d - 1 - t - r = 2t + r - t - r = t \geq t' = d(\tilde{\mathbf{u}}, \tilde{\mathbf{v}})$, tehát az ismert hibák helyét lehagyva, minimális távolságú dekódolással helyesen javítunk.

Most ismét megnézzük a szélső eseteket. $r = 0$ esetén ismét a jól ismert minimális távolságú dekódolást kapjuk, míg ha $t = 0$, akkor a javítható hibák száma $d - 1$. Ez azt jelenti, hogy egy és csak egy olyan kódszó van, amely a beérkezett szótól pontosan a megjelölt r' helyen különbözik, hiszen bármely más kódszótól még legalább további $d - r' \geq d - r = d - (d - 1) = 1$ helyen van eltérés.

A 2.8. definíció után felvázoltuk, hogy hogyan történhet általános esetben a minimális távolságú dekódolás. Ha például $n = 50$, és a kód bináris, akkor $|S^n| = 2^{50}$, vagyis a másodikként említett dekódolási eljárással ennyi szót és a hozzá tartozó kódszót kellene tárolnunk (egyenként 50-bites adatokként). Ha viszont csak a kódszavakat tároljuk, és mondjuk $M = 2^{40}$, akkor a vett szót 2^{40} különböző kódszóval kell összehasonlítani, hogy kiválasszuk a vett szóhoz legközelebbi kódszót. Látható, hogy egyik módszer sem túlságosan kedvező (az egyik a tárigény, a másik a futási idő szempontjából nem polinomiális algoritmus). A dolgon úgy tudunk segíteni, ha valamilyen egyéb módszerrel tudunk következtetni a vett szó alapján az elküldött kódszóra, vagyis ha valamilyen módon ki tudjuk számolni a kódszót a beérkezett hibás szóból. Ehhez a kódba valamilyen matematikai struktúrát építünk.

3. A kódolás valószínűségi alapjai

A **kommunikációs modell**t mutatja tömören az alábbi 1. ábra.



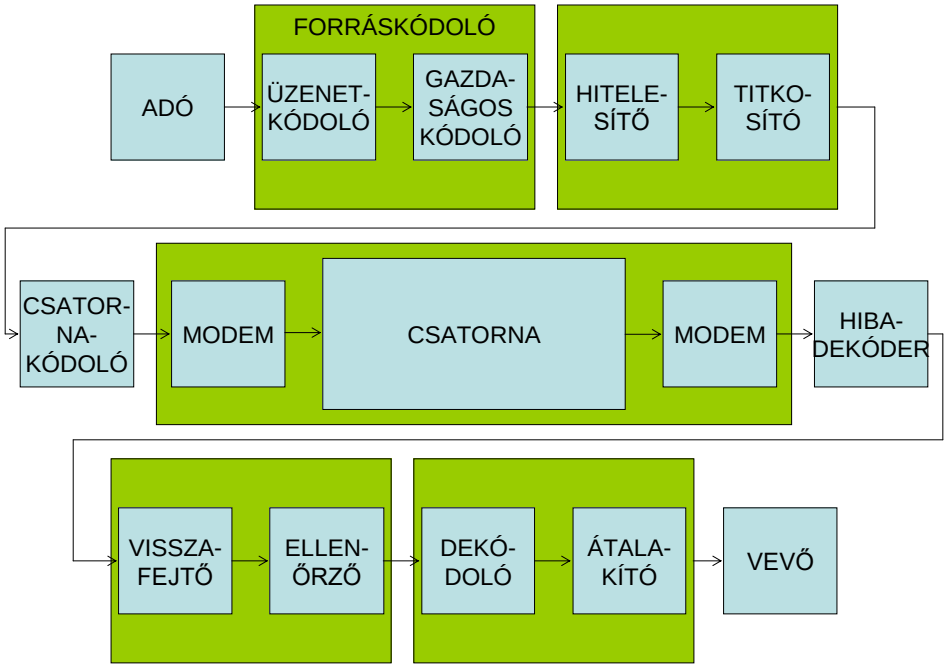
1. ábra

A kommunikáció során információt viszünk át az adótól a vevőhöz. Az információt adatok hordozzák, így valójában a csatornán az adatokat továbbítjuk a bemenettől a kimenet felé. Az információ átvitele térben és időben történik, bár közülük az egyik rendszerint domináns. Mivel a hibakorlátozás szempontjából elvileg közömbös, hogy adattárolásról vagy adatátvitelről van szó, ezért bármelyikről is szólunk, az a másikra is érvényes.

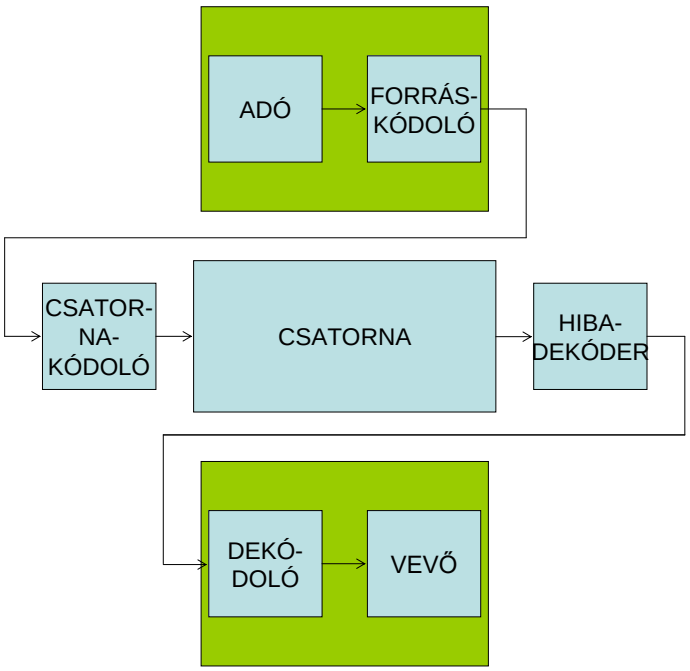
Az átvitel során négy probléma merül fel:

- a műszaki megvalósítás
- gazdaságossági kérdések
- az átvitel során fellépő hibák korlátozása
- titkosság - sértetlenség - hitelesség.

A fenti négy feladat megoldása külön - külön történik (bár nem biztos, hogy így a legjobb, de így lehet könnyen megvalósítani), amint a 2. ábra mutatja. Az előbbi modellt tömörebben, a hibakorlátozás feladatát kiemelve a 3. ábra mutatja.



2. ábra



3. ábra

A problémák megoldásához az adatokat kódolni kell. A **kódolás** során az üzeneteknek az átvitelre alkalmasabb jelsorozatot, adatot feleltetünk meg. A kódolástól elvárjuk, hogy injektív legyen, különben nem lenne lehetséges a **dekódolás**. Ha az átvitel során megengedünk egy adott nagyságú hibát, akkor az injektivitásnál gyengébb feltétel is elegendő.

Az előző fejezetben leírt feltételnek megfelelően feltesszük, hogy a kódjaink egyenletesek, vagyis a kódszavak hossza azonos, valamint hogy nincs szinkronhiba, tehát a vett szó hossza azonos az elküldött szó hosszával**.**

Legyen $I = \{u_i | q \geq i \in \mathbb{N}^+\}$ a csatorna **bemeneti ábécé**je (a továbbiakban mindig feltesszük, hogy a csatorna **diszkrét**), és legyen $O = \{v_i | q' \geq i \in \mathbb{N}^+\}$ a **kimeneti ábécé**. Feltesszük (mert feltehetjük), hogy $I \subseteq O$ (mert ha nem így lenne, akkor tekinthetnénk $O' = I \cup O$-t), így $q' \geq q$, ahol mind q, mind q' pozitív egész szám. Ha adott a kódszavak hossza, n, akkor a kódszavak halmaza, C, I^n egy részhalmaza. A csatorna kimenetén nem pontosan ugyanazt a jelsorozatot kapjuk, mint amit a bemenetére adtunk, és az eltérés általában nem determinisztikus, így a kimeneti és bemeneti jelsorozatok kapcsolatát alkalmas valószínűségi eloszlásokkal adhatjuk meg. A különböző $l \in \mathbb{N}^+$-okhoz tartozó $P(\eta_1 = v_{j_1}, \dots, \eta_l = v_{j_l} | \xi_1 = u_{i_1}, \dots, \xi_l = u_{i_l})$ feltételes valószínűségek, ahol $u_{i_k} \in I$ és $v_{j_k} \in O$, meghatározzák a csatornát. Ha mindig teljesül a

$$P(\eta_1 = v_{i_1}, \dots, \eta_l = v_{i_l} | \xi_1 = u_{j_1}, \dots, \xi_l = u_{j_l}) = \prod_{k=1}^{l} P(\eta_k = v_{i_k} | \xi_k = u_{j_k})$$

feltétel, akkor a csatorna **emlékezet nélküli**, és ilyenkor a $q \geq j \in \mathbb{N}^+$ és $q' \geq i \in \mathbb{N}^+$ indexekkel $C_{i,j} = P(v_i | u_j)$ a **csatornamátrix**.

Legyen $\mathbf{u} \in C$. Ha **u**-t elküldjük, akkor a **csatornazaj**ok következtében egy **u**-tól különböző $\mathbf{v} \in O^n$ érkezik a kimenetre. Ekkor dönteni kell, hogy mi lehetett az eredeti üzenet. Ez egy **döntési függvény**, vagy **döntési séma**, egy $f: O^n \to C \cup \{*\}$ leképezés, ahol $* \notin C$. Ha valamely $\mathbf{v} \in O^n$-re $f(\mathbf{v}) = \mathbf{u} \in C$, akkor ez azt jelenti, hogy úgy véljük, **u** volt az elküldött üzenet. Ha viszont $f(\mathbf{v}) = *$, akkor csak

annyit teszünk, hogy jelezzük, valami hiba történt az átvitel során, de nem tudjuk (vagy nem akarjuk) eldönteni, hogy mi volt az eredeti üzenet. Nyilván akkor helyes a döntésünk, ha valóban $f(\mathbf{v}) = \mathbf{u}$-t küldték, különben **döntési hiba** keletkezik. Egy $\mathbf{u} \in C$ kódszó küldése esetén a döntési hiba $P(hiba|\boldsymbol{\xi} = \mathbf{u}) = \sum_{\mathbf{v} \notin f^{-1}(\mathbf{u})} P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u})$, és a döntési hiba várható értéke

$$P(hiba) = \sum_{\mathbf{u} \in C} P(hiba|\boldsymbol{\xi} = \mathbf{u}) P(\boldsymbol{\xi} = \mathbf{u}) = \sum_{\mathbf{u} \in C} \sum_{\mathbf{v} \notin f^{-1}(\mathbf{u})} P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u})\, P(\boldsymbol{\xi} = \mathbf{u}).$$

A cél ennek a hibának a minimálása (f a változó!). $P(hiba)$ függ a bemeneti eloszlástól is, így nem lehet egy, csak a csatornától függő optimális döntési függvényt megadni. Megpróbálhatnánk egy maximális hibát előírni, vagyis hogy egy adott $\varepsilon \in \mathbb{R}^+$-ra legyen $P(hiba|\boldsymbol{\xi} = \mathbf{u}) < \varepsilon$ minden kódszó esetén. Sajnos nincs egzakt módszer arra, hogy a megadott feltételt kielégítő f függvényt megtaláljuk.

Nézzük a döntési hibát a kimenet oldaláról. Ekkor $P(hiba|\boldsymbol{\eta} = \mathbf{v}) = 1 - P(\boldsymbol{\xi} = f(\mathbf{v})|\boldsymbol{\eta} = \mathbf{v})$, és $P(hiba) = 1 - \sum_{\mathbf{v} \in O^n} P(\boldsymbol{\xi} = f(\mathbf{v})|\boldsymbol{\eta} = \mathbf{v}) P(\boldsymbol{\eta} = \mathbf{v})$, ami $\sum_{\mathbf{v} \in O^n} P(\boldsymbol{\xi} = f(\mathbf{v})|\boldsymbol{\eta} = \mathbf{v}) P(\boldsymbol{\eta} = \mathbf{v})$ maximális értékénél minimális. Az összeg minden tagja nemnegatív, így akkor maximális, ha külön-külön minden tagja maximális. Mivel $P(\boldsymbol{\eta} = \mathbf{v}) \geq 0$, ezért ismét akkor kapjuk a maximumot, ha $P(\boldsymbol{\xi} = f(\mathbf{v})|\boldsymbol{\eta} = \mathbf{v})$ maximális (bár $P(\boldsymbol{\eta} = \mathbf{v}) = 0$ esetén közömbös az előbbi érték). A változó most is az f függvény, vagyis úgy kell az $f(\mathbf{v})$ értéket megválasztani, hogy a feltételes valószínűség maximális legyen, tehát legyen $P(\boldsymbol{\xi} = f(\mathbf{v})|\boldsymbol{\eta} = \mathbf{v}) = \max_{\mathbf{u} \in C}\{P(\boldsymbol{\xi} = \mathbf{u}|\boldsymbol{\eta} = \mathbf{v})\}$. Ehhez ismerni kellene a $P(\boldsymbol{\xi} = \mathbf{u}|\boldsymbol{\eta} = \mathbf{v})$ feltételes valószínűségeket, ám nem ezek, hanem a $P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u})$ valószínűségek adottak. Ha $P(\boldsymbol{\eta} = \mathbf{v}) \neq 0$, akkor $P(\boldsymbol{\xi} = \mathbf{u}|\boldsymbol{\eta} = \mathbf{v}) = \frac{P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u}) P(\boldsymbol{\xi} = \mathbf{u})}{P(\boldsymbol{\eta} = \mathbf{v})}$, ahol $\mathbf{v}$, tehát a $P(\boldsymbol{\eta} = \mathbf{v})$ valószínűség rögzített, és így $P(\boldsymbol{\xi} = \mathbf{u}|\boldsymbol{\eta} = \mathbf{v})$ maximuma ismét függ a $P(\boldsymbol{\xi} = \mathbf{u})$ bemeneti eloszlástól (ez egyébként nyilvánvaló, hiszen ugyanazt a hibavalószínűséget határoztuk meg, mint korábban).

Ha a döntési függvényt a $P(\boldsymbol{\xi} = f(\mathbf{v})|\boldsymbol{\eta} = \mathbf{v}) = \max_{\mathbf{u} \in C}\{P(\boldsymbol{\xi} = \mathbf{u}|\boldsymbol{\eta} = \mathbf{v})\}$ feltétellel határozzuk meg, akkor ezt a döntési függvényt **ideális megfigyelő**nek nevezzük. Az előbbiek alapján az ideális megfigyelő esetén a döntési hiba várható értéke minimális.

Most éljünk azzal a megkötéssel, hogy a bemeneti eloszlás egyenletes. Ha $|C| = M$, akkor az előbbi megkötéssel minden $\mathbf{u} \in C$ kódszó esetén $P(\boldsymbol{\xi} = \mathbf{u}) = \frac{1}{M}$, és

$$P(\boldsymbol{\xi} = \mathbf{u}|\boldsymbol{\eta} = \mathbf{v}) = \frac{P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u}) P(\boldsymbol{\xi} = \mathbf{u})}{P(\boldsymbol{\eta} = \mathbf{v})} = \frac{1}{MP(\boldsymbol{\eta} = \mathbf{v})} P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u}).$$

Itt $\frac{1}{MP(\boldsymbol{\eta}=\mathbf{v})}$ független $\mathbf{u}$-tól, így

$$\max_{\mathbf{u} \in C} P(\boldsymbol{\xi} = \mathbf{u}|\boldsymbol{\eta} = \mathbf{v}) = \frac{1}{MP(\boldsymbol{\eta} = \mathbf{v})} \max_{\mathbf{u} \in C}\{P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u})\}$$

tehát $f(\mathbf{v}) = \hat{\mathbf{u}}$, ahol $P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \hat{\mathbf{u}}) = \max_{\mathbf{u} \in C}\{P(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u})\}$. Az ily módon meghatározott döntési függvény a **maximum likelihood döntési séma**.

Nézzünk egy példát. Legyen $I = \{0,1\} = O$, a csatorna emlékezet nélküli, és a csatornamátrix legyen $\mathbf{C} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$, ahol p egy 1-nél nem nagyobb nemnegatív valós szám. Ez a **bináris szimmetrikus csatorna**, rövidítve a **BSC** (**B***inary* **S***ymmetric* **C***hannel*). Legyen továbbá a bemeneti eloszlás $P(\xi = 0) = q$ és $P(\xi = 1) = 1 - q$, ahol q is 1-nél nem nagyobb nemnegatív valós szám. Ekkor

$$P(\eta = 0) = P(\eta = 0|\xi = 0)P(\xi = 0) + P(\eta = 0|\xi = 1)P(\xi = 1) = (1-p)q + p(1-q)$$
$$P(\eta = 1) = P(\eta = 1|\xi = 0)P(\xi = 0) + P(\eta = 1|\xi = 1)P(\xi = 1) = pq + (1-p)(1-q),$$

és ezt a két eredményt felhasználva meg tudjuk határozni a fordított feltételes valószínűségeket a Bayes-tétel alkalmazásával. Ekkor az alábbi eredményeket kapjuk.

$$P(\xi=0|\eta=0)=\frac{P(\eta=0|\xi=0)P(\xi=0)}{P(\eta=0)}=\frac{(1-p)q}{(1-p)q+p(1-q)}$$
$$P(\xi=1|\eta=0)=\frac{P(\eta=0|\xi=1)P(\xi=1)}{P(\eta=0)}=\frac{p(1-q)}{(1-p)q+p(1-q)},$$

és így $f(0)=\begin{cases}0,\text{ha } q>p\\1,\text{ha } q<p\end{cases}$ (és ha $p=q$, akkor mindegy),

$$P(\xi=0|\eta=1)=\frac{P(\eta=1|\xi=0)P(\xi=0)}{P(\eta=1)}=\frac{pq}{pq+(1-p)(1-q)}$$
$$P(\xi=1|\eta=1)=\frac{P(\eta=1|\xi=1)P(\xi=1)}{P(\eta=1)}=\frac{(1-p)(1-q)}{pq+(1-p)(1-q)},$$

vagyis most $f(1)=\begin{cases}0,\text{ha } p>1-q\\1,\text{ha } p<1-q\end{cases}$ (és ismét mindegy, ha $p=1-q$). Az így meghatározott f függvény az ideális megfigyelő. Ha feltesszük, hogy $q=\frac{1}{2}$ és $p<\frac{1}{2}$, akkor $f(0)=0$ és $f(1)=1$. Ugyanezt kapjuk a $q=\frac{1}{2}$ feltétel esetén a $\max\limits_{u\in\{0,1\}}\{P(\eta=v|\xi=u)\}$ feltételből is:

$$P(\eta=0|\xi=0)=1-p\wedge P(\eta=0|\xi=1)=p\wedge p<\frac{1}{2}<1-p\Rightarrow f(0)=0$$
$$P(\eta=1|\xi=0)=p\wedge P(\eta=1|\xi=1)=1-p\wedge p<\frac{1}{2}<1-p\Rightarrow f(1)=1.$$

Az utóbbi döntési függvény a maximum likelihood döntési függvény. Ekkor a döntési hiba

$$P^{(1)}(hiba)=P(\eta=1|\xi=0)P(\xi=0)+P(\eta=0|\xi=1)P(\xi=1)=pq+p(1-q)=p.$$

Most legyen a csatorna az előbbi és $n=3$, továbbá $C=\{000,111\}$. Legyen a döntési függvény $f(\mathbf{v})=\left\lfloor\frac{v_1+v_2+v_3}{2}\right\rfloor$, vagyis legyen $f(000)=f(001)=f(010)=f(100)=0$, és hasonlóképpen legyen $f(111)=f(110)=f(101)=f(011)=1$ (arra a jelre döntünk, amely többször fordul elő a vett szóban, ez a **többségi döntés**. Mivel páratlan hosszúságú a szó, és két különböző jel van, így valamelyik mindig többségben lesz). Ekkor a döntési hiba

$$P^{(3)}(hiba)=\binom{3}{2}p^2(1-p)+\binom{3}{3}p^3=3p^2-2p^3=3p^2\left(1-\frac{2}{3}p\right),$$

hiszen akkor döntünk rosszul, ha az átvitel során három összetartozó bitből legalább kettő meghibásodik. Összehasonlítva ezt az előbbi esettel, $\frac{P^{(3)}(hiba)}{P^{(1)}(hiba)}=3p\left(1-\frac{2}{3}p\right)$. A függvény maximuma $p=\frac{3}{4}$-nél van, így $p<\frac{1}{2}$ esetén az arány kisebb, mint $p=\frac{1}{2}$-nél, ahol az értéke 1, vagyis $p<\frac{1}{2}$ esetén a háromszorozásnál a döntési hiba kisebb lesz. Ha például $p=10^{-3}$ (ez egy elég zajos csatorna), akkor az előbbi arány $\frac{P^{(3)}(hiba)}{P^{(1)}(hiba)}=3\cdot10^{-3}\left(1-\frac{2}{3}\cdot10^{-3}\right)\approx3\cdot10^{-3}\approx\frac{1}{333}$, vagyis a javulás kb. 333-szoros.

Most legyen $|I|=q(\geq2)$, $O=I$, és a csatornamátrix $C_{i,i}=1-p$, és $i\neq j$-re $C_{i,j}=\frac{p}{q-1}$ (ez a csatorna az **emlékezet nélküli diszkrét szimmetrikus csatorna**, **az MDSC**, azaz a **M***emoryless* **D***iscrete* **S***ymmetric* **C***hannel*). Ekkor

$$P(\boldsymbol{\eta}=\mathbf{v}|\boldsymbol{\xi}=\mathbf{u}) = \prod_{k=1}^{l} P\left(\eta_k = v_{i_k}\middle|\xi_k = u_{j_k}\right)$$
$$= \prod_{u_{j_k}\neq v_{i_k}} P\left(\eta_k = v_{i_k}\middle|\xi_k = u_{j_k}\right)\cdot \prod_{u_{j_k}= v_{i_k}} P\left(\eta_k = v_{i_k}\middle|\xi_k = u_{j_k}\right)$$
$$= \prod_{u_{j_k}\neq v_{i_k}} \frac{p}{q-1}\cdot \prod_{u_{j_k}= v_{i_k}} (1-p) = \left(\frac{p}{q-1}\right)^d (1-p)^{n-d} = (1-p)^n \left(\frac{\frac{p}{q-1}}{1-p}\right)^d,$$

ahol n a kódszavak hossza, és $d = d(\mathbf{u},\mathbf{v})$ az $\mathbf{u}$ és $\mathbf{v}$ azonos pozícióban lévő, eltérő komponenseinek száma, az $\mathbf{u}$ és $\mathbf{v}$ Hamming-távolsága. Ha $\frac{p}{q-1} < 1-p$, azaz, ha $0 < p < 1-\frac{1}{q}$, akkor a fenti valószínűség akkor maximális, ha $d(\mathbf{u},\mathbf{v})$ minimális, vagyis ha $d(f(\mathbf{v}),\mathbf{v}) = \min_{\mathbf{u}\in C}\{d(\mathbf{u},\mathbf{v})\}$. Az így meghatározott döntési függvény a **minimális távolságú dekódolás** (lásd a 12. oldalon a 2.8. definíciót). MDSC esetén tehát a minimális távolságú dekódolás a maximum likelihood döntési függvény.

Visszatérve a háromszoros ismétléshez, nyilván három helyett az ismétlések száma bármely $n \in \mathbb{N}^+$-ra $2n+1$ is lehet. Annak a valószínűsége, hogy egy $2n+1 \geq k \in \mathbb{N}$-re az átvitel során k hiba lép fel, $P(\kappa = k) = \binom{2n+1}{k} p^k (1-p)^{(2n+1)-k}$. Ez binomiális eloszlás, és így a hibák számának várható értéke $E(\kappa) = (2n+1)p$. Ha $p < \frac{1}{2}$, akkor $E(\kappa) = (2n+1)p < n + \frac{1}{2} < n+1$, a hibás jegyek várható száma kisebb, mint a nem hibás jegyek várható száma, a döntés várhatóan helyes lesz. Mi ennek az ára? Ehhez bevezetjük az alábbi fogalmat.

3.1. Definíció

Legyen C egy $(n, M)_q$-paraméterű kód. Ekkor $\mathcal{R}_q = \frac{1}{n}\log_q M$ a **kódsebesség**.

Δ

$\log_q M$ azt adja meg, hogy mekkora minimális szóhosszal lehet q különböző szimbólum felhasználásával M különböző szót megadni, így a kódsebesség azt mutatja, hogy a minimálisan szükséges hosszhoz képest mekkora a kódszavak hossza. Nyilván igaz, hogy $0 \leq \mathcal{R}_q \leq 1$, feltéve, hogy a kód legalább egy szót tartalmaz. A fentebb ismertetett ismétléses kód esetén az volt a helyzet, hogy az ismétlések számának növelésével a döntési hiba nullához tartott, de ezzel együtt a kódsebesség is tart a nullához, vagyis végül hibátlanul visszük át a semmit. Általában, ha n tart a végtelenhez, miközben M nem változik, vagyis ugyanannyiféle üzenetet egyre hosszabb kódokkal akarunk átvinni a csatornán, akkor a kódsebesség, $\mathcal{R}_q$, tart a nullához, vagyis hiába tart a döntési hiba a nullához, ám az átvitt üzenetek száma is tart a nullához. **Shannon** szerint ez nem szükségszerű.

Az **entrópia** információelméleti fogalmát Shannon határozta meg. Korábban **Heartley** vizsgálta matematikai szempontból az információt, és úgy találta, hogy ha n különböző üzenet lehetséges, akkor egy-egy **üzenet információtartalma**, az **egyedi információmennyiség** $I = \log n$. E szerint a kifejezés szerint azonban a különböző üzenetek azonos mennyiségű információt, új ismeretet közölnek a fogadóval. Ezzel szemben Shannon úgy gondolta, hogy egy üzenet annál több információt szolgáltat, minél váratlanabb, minél kevésbé lehet rá számítani, azaz minél kisebb a valószínűsége. Ha X egy véges eseménytér, az üzenetek halmaza, és az $x_i \in X$ üzenet p_i valószínűséggel fordul elő, akkor tehát Shannon szerint az x_i üzenet $I(p_i)$ információt szolgáltat, ahol I egyelőre ismeretlen függvény. A teljes **üzenethalmaz átlagos információtartalma** az egyes üzenetek egyedi információtartalmának várható értéke, $H(p_{n-1},\dots,p_0) = \sum_{i=0}^{n-1} p_i I(p_i)$, ahol n a különböző üzenetek száma, és H az **entrópiafüggvény**. Mivel egyelőre I ismeretlen, ezért H-t sem ismerjük. H meghatározásához bizonyos feltételeket kell megfogalmazni. Egy lehetséges axiomatikus bevezetés az alábbi kikötéseket tartalmazza:

1. $(p_{n-1}, \dots, p_0) \in]0,1[^n \subseteq \mathbb{R}^n$ véges diszkrét valószínűségi eloszlás;
2. $H(p_{n-1}, \dots, p_0)$ a változóinak szimmetrikus függvénye, azaz ha π az $\{i \in \mathbb{N} | i < n\}$ halmaz tetszőleges permutációja, akkor $H(p_{n-1}, \dots, p_0) = H\left(p_{\pi(n-1)}, \dots, p_{\pi(0)}\right)$;
3. $H(tp_{n-1}, (1-t)p_{n-1} \dots, p_0) = H(p_{n-1}, \dots, p_0) + p_{n-1}H(t, 1-t)$, ha $t \in]0,1[\subseteq \mathbb{R}$;
4. $H(t, 1-t)$ t-nek folytonos függvénye, ha $t \in]0,1[\subseteq \mathbb{R}$;
5. $H\left(\frac{1}{2}, \frac{1}{2}\right) > 0$.

A fenti feltételeknek pontosan egy folytonos függvény, $H(p_{n-1}, \dots, p_0) = -\sum_{i=0}^{n-1} p_i \log p_i$ felel meg, és ebből leolvasva $I(p_i) = -\log p_i$. Ha minden üzenet valószínűsége azonos, tehát bármelyik $\frac{1}{n}$ valószínűséggel fordul elő, akkor valóban igaz, hogy az egyedi üzenetek által közvetített információ mértéke $I = \log n$. Általános esetben viszont az egyes üzenetek bekövetkezése különböző valószínűséggel történik, tehát általában $I(p_i) \neq \log n$. A valós értékű logaritmusfüggvény csak a pozitív valós számokra értelmezett, és ha x a pozitív valós számokon keresztül tart a 0-hoz, akkor a logaritmusfüggvény értéke abszolút értékben a ∞-hez tart, így $|x \log x| \to 0 \cdot \infty$. De $\lim_{x \to 0+0} (x \log x)$ létezik, és 0-val egyenlő, ezért az entrópiafüggvényt kiterjeszthetjük arra az esetre is, amikor egy vagy több valószínűség értéke 0, azzal, hogy ekkor $p_i \log p_i = 0$.

Láthatóan $H(p_{n-1}, \dots, p_0) \geq 0$, és a függvény értéke akkor és csak akkor 0, ha egy kivételével valamennyi valószínűség 0 (és ekkor a nem nulla valószínűség 1, hiszen a valószínűségek összege 1).

Az előbbi felírásban nem adtuk meg konkrétan a logaritmus alapját, ám erre nincs is szükség. Ha ugyanis egy alapról áttérünk egy másikra, az csupán a mértékegység megváltozását jelenti (hasonlóan mondjuk a méterhez és lábhoz), hiszen $\log_a u = \log_a b \cdot \log_b u$. Magát a logaritmus r alapját $H\left(\frac{1}{2}, \frac{1}{2}\right) = c$ határozza meg, ugyanis $c = H\left(\frac{1}{2}, \frac{1}{2}\right) = -\left(\frac{1}{2}\log_r \frac{1}{2} + \frac{1}{2}\log_r \frac{1}{2}\right) = \log_r 2$-ből $r = 2^{\frac{1}{c}} > 1$. Az alap szokásos értéke az információelméletben 2, és ekkor az entrópia egysége a bit. Ezt az elnevezést **John W. Tukey** vezette be a **binary digit** rövidítéseként. Tekintettel arra, hogy ugyanez a neve egy kettes számrendszerben felírt szám egy-egy számjegyének, ezért megkülönböztetésül az információelméleti egységet szokás **binary unit**-ként, a **binary unit** rövidítéseként említeni.

Ha a p_i valószínűségek az X eseményhalmaz elemei előfordulásainak a valószínűségei, akkor $H(p_{n-1}, \dots, p_0)$ tulajdonképpen az X tér entrópiája, ezért ezt az értéket $H(X)$-szel is jelölhetjük.

Csupán az érdekesség, és bizonyos patriotikus büszkeség miatt jegyezzük meg, hogy Shannonnak **Neumann János** javasolta az entrópia elnevezést, lévén, hogy a kifejezés matematikailag hasonló alakú, mint a korábbi fizikai entrópia. Az elnevezést a formális hasonlóságon kívül bizonyos tartalmi azonosságok is alátámasztják, bár igen komoly eltérések is kimutathatóak a két entrópiafogalom között, amiért többen károsnak tartják az azonos megnevezést. Shannonnak más „magyar kapcsolata" is volt: foglalkozott sakkautomatával, és ezzel kapcsolatban megemlítette **Kempelen Farkas** nevét, valamint a kommunikációról szólva **Gábor Dénes**t nevezi meg egyik úttörőként.

A fenti H-függvény a **Shannon-féle entrópiafüggvény**. Léteznek általánosabb kifejezések is az entrópiára. Egyik a $H_\alpha(p_{n-1}, \dots, p_0) = \frac{1}{1-\alpha}\log \sum_{i=0}^{n-1} p_i^\alpha$ **Rényi-féle entrópia**, ahol $1 > \alpha \in \mathbb{R}_0^+$. Ez a kifejezés határértékként tartalmazza a Shannon-féle entrópiát, ha α balról tart 1-hez.

A $H(p_{n-1}, \dots, p_0)$ függvénynek az értelmezési tartományában pontosan egy maximuma van a $(p_{n-1}, \dots, p_0) = \left(\frac{1}{n}, \dots, \frac{1}{n}\right)$ helyen, és ekkor az értéke $\log n$, ami éppen 1, ha a logaritmus alapszáma is n. Ez az entrópia intuitív értelmezése alapján világos, hiszen átlagosan akkor jutunk a legtöbb információhoz, akkor lehet a legkevésbé megjósolni a soron következő üzenetet, ha lényegében véve semmit sem tudunk az egyes üzenetekről, bármelyik esemény azonos valószínűséggel következhet be. A pontos bizonyításhoz tegyük fel, hogy $n \in \mathbb{N}^+$, $n > i \in \mathbb{N}$-re $0 \leq a_i \in \mathbb{R}$ és $0 < b_i \in \mathbb{R}$, $a = \sum_{i=0}^{n-1} a_i$, $b = \sum_{i=0}^{n-1} b_i$ és $1 < r \in \mathbb{R}$. Ekkor, kihasználva, hogy az r-alapú logaritmusfüggvény az értelmezési tartományának minden pontjában alulról szigorúan konkáv,

$$\sum_{i=0}^{n-1} a_i \log_r \frac{b_i}{a_i} = a \sum_{i=0}^{n-1} \frac{a_i}{a} \log_r \frac{b_i}{a_i} \leq a \log_r \sum_{i=0}^{n-1} \frac{a_i}{a} \frac{b_i}{a_i} = a \log_r \frac{\sum_{i=0}^{n-1} b_i}{a} = a \log_r \frac{b}{a},$$

és pontosan akkor van egyenlőség, ha minden i-re $\frac{a_i}{b_i} = \frac{a}{b}$. Most legyen $a_i = p_i$ és $b_i = 1$, ekkor $a = 1$ és $b = n$, és az előbbi eredményből kapjuk, hogy $-\sum_{i=0}^{n-1} p_i \log_r p_i \leq \log_r n$, és pontosan akkor éri el az entrópia a maximumát, amikor valamennyi valószínűség azonos értékű.

A továbbiakban szükségünk lesz az entrópiafogalom kiterjesztésére. Legyen két véges valószínűségi szkémánk, az egyik az X, a másik az Y eseménytéren, az előbbiben m, az utóbbiban n elemi eseménnyel. Legyen $p_i^{(X)}$ az $x_i \in X$ és $p_j^{(Y)}$ az $y_j \in Y$ esemény előfordulásának valószínűsége, $p_{i,j}$ az x_i és y_j esemény együttes bekövetkezésének valószínűsége, míg $p_{i|j}$ az $x_i \in X$ esemény előfordulásának valószínűsége, feltéve, hogy $y_j \in Y$ bekövetkezett. Most az alábbi entrópiákat vezethetjük be:

a) $H(X,Y) = -\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} p_{i,j} \log p_{i,j}$ az **együttes entrópia**;
b) $H(X|Y) = E\big(H\big(X\big|y_j\big)\big|n > j \in \mathbb{N}\big) = \sum_{j=0}^{n-1} p_j^{(Y)} H\big(X\big|y_j\big)$ az Y**-ra vonatkozó feltételes entrópia**, és hasonló az X-re vonatkozó $H(Y|X)$ feltételes entrópia. A definíciókat alkalmazva $H\big(X\big|y_j\big) = -\sum_{i=0}^{m-1} p_{i|j} \log p_{i|j}$, majd ezt felhasználva megkapjuk $H(X|Y)$-t, nevezetesen $H(X|Y) = -\sum_{j=0}^{n-1} p_j^{(Y)} \sum_{i=0}^{m-1} p_{i|j} \log p_{i|j} = -\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log p_{i|j}$.

Mivel a fent bevezetett fogalmak lényegében véve azonosak a korábbi entrópiafogalommal (annyi eltéréssel, hogy a feltételes entrópia egy átlagos entrópia), ezért a fenti függvények értéke is nemnegatív. Belátható továbbá, hogy

1. $H(X|Y) \leq H(X)$;
2. $H(X) + H(Y|X) = H(X,Y) = H(Y) + H(X|Y)$.

Valóban, a logaritmusfüggvény 1-nél nagyobb alap esetén szigorúan konkáv, így az ellentettje szigorúan konvex, tehát

$$\begin{aligned} H(X) - H(X|Y) &= -\sum_{i=0}^{m-1} p_i^{(X)} \log p_i^{(X)} + \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log p_{i|j} \\ &= -\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} p_{i,j} \log p_i^{(X)} + \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log \frac{p_{i,j}}{p_j^{(Y)}} \\ &= -\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log \frac{p_i^{(X)} p_j^{(Y)}}{p_{i,j}} \geq \log \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log \frac{p_i^{(X)} p_j^{(Y)}}{p_{i,j}} = \log 1 = 0, \end{aligned}$$

ami igazolja az első állítást, míg a másodikhoz

$$\begin{aligned} H(X) + H(Y|X) &= -\sum_{i=0}^{m-1} p_i^{(X)} \log p_i^{(X)} - \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log p_{j|i} \\ &= -\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} p_{i,j} \log p_i^{(X)} - \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log p_{j|i} \\ &= -\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log p_i^{(X)} \frac{p_{i,j}}{p_i^{(X)}} = -\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} p_{i,j} \log p_{i,j} = H(X,Y). \end{aligned}$$

Az első egyenlőtlenség azt fejezi ki, hogy ha az X üzenethalmazról már van valamilyen *a priori* ismeretünk, akkor legfeljebb annyi új információhoz jutunk, mint az előbbi ismeretek nélkül. A második egyenlőség viszont azt jelenti, hogy az együttes üzenethalmaz átlagos információtartalmát például úgy kapjuk meg, hogy meghatározzuk önmagában az X forrás információtartalmát, és ehhez még hozzávesszük azt az információmennyiséget, amelyet már az X ismeretében az Y forrásból nyerhetünk. A két pont összevetéséből az is látszik, hogy az együttes entrópia nem lehet nagyobb, mint a két külön-külön számolt entrópia összege, vagyis $H(X,Y) \leq H(X) + H(Y)$.

Végezetül még egy fontos fogalmat definiálunk, az $I(X,Y) = H(X) - H(X|Y)$ **kölcsönös információt**. A fentebbi 2. összefüggésből azonnal leolvasható, hogy az $I(X,Y) = H(Y) - H(Y|X)$, valamint az $I(X,Y) = H(X) + H(Y) - H(X,Y)$ összefüggés is teljesül. A kölcsönös információ azt fejezi ki, hogy Y-t megfigyelve még mennyi bizonytalanság marad X vonatkozásában. Figyelembe véve a $H(X|Y) \leq H(X)$ egyenlőtlenséget, látjuk, hogy a kölcsönös információ értéke is mindig nemnegatív, és a két valószínűségi mező entrópiájának minimumát nem haladja meg. A kölcsönös információ értéke 0, ha X és Y függetlenek, hiszen ekkor $H(X|Y) = H(X)$, és $I(X,Y) = H(X)$, ha Y és X között (legalábbis 1 valószínűséggel) determinisztikus függvénykapcsolat van.

Az itt megfogalmazott entrópia független valószínűségi változókra érvényes. Az entrópia általánosabb esetre is megadható, de ezzel a továbbiakban nem foglalkozunk.

A **csatorna kapacitása** nem más, mint a csatorna bemenetén és kimenetén lévő valószínűségi mező kölcsönös információjának maximuma a bemenetére adott eloszlás függvényében, vagyis matematikailag felírva $\mathcal{C} = \max_{P(X)}\{I(X,Y)\}$. Itt arról van szó, hogy a csatorna kimenetén megjelenő jelsorozat a bemenetre adott jelsorozattól és a csatornától függ. Minél erősebb az eltérés, annál kevésbé lehet rekonstruálni a kimeneten megfigyelt jelsorozatból az elküldött kódszót. Az azonban, hogy milyen mértékű a torzulás, attól is függ, hogy hogyan választjuk meg a csatorna bemenetére adott jelsorozatokat. Ezt fejezi ki a csatornakapacitás.

Shannon azt állítja, hogy bizonyos csatornák esetén a csatorna kapacitásánál kisebb bármely sebességgel tetszőleges kis hibavalószínűséggel átvihető az információ, vagyis lehet olyan kódot konstruálni, amellyel az előbb említett módon lehet kommunikálni (a *kisebb* megkötés akkor igaz, ha a kölcsönös információ mérésénél is az alkalmazott szimbólumok száma a logaritmus alapja, különben egy megfelelő, az alkalmazott alaptól függő konstanssal való szorzás után igaz a *kisebb* feltétel). Ismeretes a tétel két megfordítása is. A *gyenge megfordítás* szerint a csatorna kapacitását meghaladó sebesség esetén a döntési hiba akármilyen kódolás esetén is nagyobb lesz egy pozitív korlátnál, míg az *erős megfordítás* szerint a kód hosszának növekedésével a döntési hiba valószínűsége 1-hez tart (a gyenge megfordítás nem következik az erős megfordításból, a két tétel önálló, továbbá most is igaz a logaritmus alapjára vonatkozó korábbi megjegyzés).

Bizonyítás nélkül a tételek az alábbiak, feltéve, hogy q szimbólummal kódolunk.

1. **A zajos csatorna kódolási tétele**. Ha $\mathcal{C} > \mathcal{R}_q \in \mathbb{R}^+$, akkor van olyan $C_n: \left(n, \left\lceil q^{\mathcal{R}_q n}\right\rceil\right)_q$ kódsorozat és döntési függvények olyan sorozata, hogy $P_n^{(max)}(hiba) \to 0$, ha $n \to \infty$.

Ezt a tételt néhány csatornatípusra, többek között az emlékezet nélküli csatornákra igazolták.

2. **Gyenge megfordítás**. $\mathcal{C} < \mathcal{R}_q \in \mathbb{R}^+$ esetén bármely $C_n: \left(n, \left\lceil q^{\mathcal{R}_q n}\right\rceil\right)_q$ kódsorozat és tetszőleges döntési függvény mellett van olyan $\varepsilon \in \mathbb{R}^+$, hogy minden $n \in \mathbb{N}^+$-ra $P_n(hiba) > \varepsilon$.

3. **Erős megfordítás**. Ha $\mathcal{C} < \mathcal{R}_q \in \mathbb{R}^+$, akkor bármely $C_n: \left(n, \left\lceil q^{\mathcal{R}_q n}\right\rceil\right)_q$ kódsorozat, és a döntési függvények tetszőleges sorozata esetén $\lim_{n\to\infty} P_n(hiba) = 1$.

A megfordítási tételek lényege, hogy a csatornakapacitásnál nagyobb sebességgel nem lehet hibátlanul dekódolni, sőt, minél hosszabbak a kódszavak, annál biztosabb, hogy hibásan dekódolunk.

Shannon tétele elvi jelentőségű. A tétel szerint létező kódot még senkinek nem sikerült konstruálnia, ami nem okoz túl nagy problémát, ugyanis egy ilyen kód hossza és mérete használhatatlanul nagy lenne. A tétel jelentősége, hogy megmutatja, hogyan lehet egyszerre csökkenteni a dekódolási hibát a kódsebesség lényeges csökkenése nélkül: több üzenetet egyszerre kell, nagyobb hosszúságú kódszavakba kódolni, így nő a kód mérete is, ellensúlyozva a kódsebesség csökkenését.

Az entrópia fogalmának segítségével például az alábbi csatornatípusokat definiálhatjuk:

- **Veszteségmentes csatorna**
  a kimenet teljesen meghatározza a bemenetet, vagyis az alábbi feltételek bármelyike teljesül:

  a) O particionálható úgy, hogy az osztályok száma megegyezik a bemeneti ábécé méretével, és $P(\eta \in O_i | \xi = x_i) = 1$;
  b) $\forall(y \in O): P(\eta = y) \neq 0 \Rightarrow (\exists(x \in I): P(\eta = y | \xi = x) = 1)$;
  c) $H(X|Y) = 0$.

Ekkor a csatorna kapacitása $\mathcal{C} = \log|I|$.

- **Determinisztikus csatorna**
  a bemenet teljesen meghatározza a kimenetet, ami ekvivalens az alábbiak bármelyikével:

  a) $\forall(x \in I)\exists(y \in O): P(\eta = y | \xi = x) = 1$;
  b) $H(Y|X) = 0$.

Most a csatorna kapacitása $\mathcal{C} = \log|\{y \in O | \exists(x \in I): P(\eta = y | \xi = x) = 1\}|$.

- **Zajmentes csatorna**
  ha egyszerre veszteségmentes és determinisztikus, vagyis ha

$$\exists(\varphi: I \to O): \big(\mathrm{Im}(\varphi) = O \wedge (\forall(x \in I): P(\eta = \varphi(x) | \xi = x) = 1)\big).$$

A csatorna kapacitása megegyezik a veszteségmentes csatorna kapacitásával.

- **Haszontalan csatorna**
  ha Y teljesen független X-től, azaz ha a következő két feltétel valamelyike igaz:

  a) $\forall(y \in O)\forall(x_i \in I)\forall\big(x_j \in I\big): P(\eta = y | \xi = x_i) = P\big(\eta = y \big| \xi = x_j\big)$;
  b) $H(X|Y) = H(X)$.

A haszontalan csatorna kapacitása $\mathcal{C} = 0$, hiszen most $I(X, Y) = 0$.

Más szempontból a csatorna lehet

- **sorszimmetrikus**
  ha a csatornamátrix sorai egymás permutációi;

- **oszlopszimmetrikus**
  ha a csatornamátrix oszlopai egymás permutációi;

- **szimmetrikus**
  ha egyszerre sor- és oszlopszimmetrikus.

Könnyen belátható az alábbi tétel.

3.2. Tétel

Sorszimmetrikus csatornamátrixnál egyenletes bemeneti eloszláshoz egyenletes kimeneti eloszlás tartozik. Oszlopszimmetrikus csatornamátrix esetén $H(Y|X)$ nem függ a bemeneti eloszlástól.

Δ

Most legyen adott egy Cs_1 csatorna a q_1-elemű I_1 bemeneti, az O_1 kimeneti szimbólumhalmazzal és a $P_1(\boldsymbol{\eta} = \mathbf{v}|\boldsymbol{\xi} = \mathbf{u})$ feltételes valószínűségekkel, ahol $\mathbf{u} \in C_1 \subseteq I_1^{n_1}$ és $\mathbf{v} \in O_1^{n_1}$, és hasonlóan adott egy 2-vel indexelt csatorna és kód. A két kód **ekvivalens**, ha $\mathcal{R}_1 = \mathcal{R}_2$, és minden f_1 döntési függvényhez van olyan $\varphi_1 \colon C_1 \to C_2$ injekció és f_2 döntési függvény, hogy minden $\mathbf{u} \in C_1$ esetén $P_1(hiba|\boldsymbol{\xi} = \mathbf{u}) = P_2\big(hiba\big|\boldsymbol{\xi} = \varphi_1(\mathbf{u})\big)$, és a másik irányban is megadható hasonló tulajdonságokkal rendelkező injektív leképezés. Hasonlóan, (C_1, f_1) ekvivalens (C_2, f_2)-vel, ha a kódsebességek azonosak, és megadható a két kód között egy bijekció, hogy az egymáshoz rendelt kódszavakra a döntési hiba értéke megegyezik. Ha mindkét irányban létezik injektív leképezés, akkor létezik a két kód között bijektív megfeleltetés is, tehát $M_1 = M = M_2$, és a két kód sebessége pontosan akkor azonos, ha

$$\frac{1}{n_1 \log_2 q_1} \log_2 M = \frac{1}{n_1} \log_{q_1} M_1 = \mathcal{R}_1 = \mathcal{R}_2 = \frac{1}{n_2} \log_{q_2} M_2 = \frac{1}{n_2 \log_2 q_2} \log_2 M,$$

azaz akkor és csak akkor, ha $q_1^{n_1} = q_2^{n_2}$.

Speciális esetként tegyük fel, hogy $q_1^{n_1} = q_2^{n_2}$ és $\psi \colon O_1^{n_1} \to O_2^{n_2}$ bijektív leképezés, amelynek C_1-re való φ megszorítása bijektíven képezi le C_1-et C_2-re, és amelynél minden $(\mathbf{u}, \mathbf{v}) \in C_1 \times O_1^{n_1}$ párra $P_1(\boldsymbol{\eta}_1 = \mathbf{v}|\boldsymbol{\xi}_1 = \mathbf{u}) = P_2\big(\boldsymbol{\eta}_2 = \psi(\mathbf{v})\big|\boldsymbol{\xi}_2 = \varphi(\mathbf{u})\big)$. Belátjuk, hogy az előbbi feltételekkel bármely f_1 döntési sémához megadható olyan f_2 döntési séma, hogy a két kód ekvivalens.

Mivel $q_1^{n_1} = q_2^{n_2}$ és $\varphi \colon C_1 \to C_2$ bijektív, ezért a két kódsebesség megegyezik. ψ bijekció, így létezik az inverze, ψ^{-1}. Legyen $\mathbf{v}^{(2)} \in O_2^{n_2}$-re $f_2\big(\mathbf{v}^{(2)}\big) = \varphi\left(f_1\left(\psi^{-1}\big(\mathbf{v}^{(2)}\big)\right)\right)$, ekkor f_2 egy döntési séma az $O_2^{n_2}$ halmazon. Egy tetszőleges $\big(\mathbf{u}^{(2)}, \mathbf{v}^{(2)}\big) \in C_2 \times O_2^{n_2}$-re

$$\begin{aligned}
\mathbf{v}^{(2)} \in f_2^{-1}\big(\mathbf{u}^{(2)}\big) &\Leftrightarrow \mathbf{u}^{(2)} = f_2\big(\mathbf{v}^{(2)}\big) = \varphi\left(f_1\left(\psi^{-1}\big(\mathbf{v}^{(2)}\big)\right)\right) \\
&\Leftrightarrow \varphi^{-1}\big(\mathbf{u}^{(2)}\big) = f_1\left(\psi^{-1}\big(\mathbf{v}^{(2)}\big)\right) \\
&\Leftrightarrow \mathbf{v}^{(1)} = \psi^{-1}\big(\mathbf{v}^{(2)}\big) \in f_1^{-1}\left(\varphi^{-1}\big(\mathbf{u}^{(2)}\big)\right) = f_1^{-1}\big(\mathbf{u}^{(1)}\big),
\end{aligned}$$

ahol $\mathbf{u}^{(1)} = \varphi^{-1}\big(\mathbf{u}^{(2)}\big) \in C_1$ és $\mathbf{v}^{(1)} = \psi^{-1}\big(\mathbf{v}^{(2)}\big) \in O_1^{n_1}$. A döntési hiba egy $\mathbf{u}^{(2)}$ üzenet esetén

$$\begin{aligned}
P_2\left(hiba\middle|\boldsymbol{\xi}_2 = \varphi\big(\mathbf{u}^{(1)}\big)\right) &= P_2\big(hiba\big|\boldsymbol{\xi}_2 = \mathbf{u}^{(2)}\big) \\
&= \sum_{\mathbf{v}^{(2)} \notin f_2^{-1}\left(\mathbf{u}^{(2)}\right)} P_2\big(\boldsymbol{\eta}_2 = \mathbf{v}^{(2)}\big|\boldsymbol{\xi}_2 = \mathbf{u}^{(2)}\big) \\
&= \sum_{\mathbf{v}^{(1)} \notin f_1^{-1}\left(\mathbf{u}^{(1)}\right)} P_2\left(\boldsymbol{\eta}_2 = \psi\big(\mathbf{v}^{(1)}\big)\middle|\boldsymbol{\xi}_2 = \varphi\big(\mathbf{u}^{(1)}\big)\right) \\
&= \sum_{\mathbf{v}^{(1)} \notin f_1^{-1}\left(\mathbf{u}^{(1)}\right)} P_1\big(\boldsymbol{\eta}_1 = \mathbf{v}^{(1)}\big|\boldsymbol{\xi}_1 = \mathbf{u}^{(1)}\big) = P_1\big(hiba\big|\boldsymbol{\xi}_1 = \mathbf{u}^{(1)}\big),
\end{aligned}$$

így a két kód bármely egymásnak megfelelő eleme esetén azonos a döntési hiba, a két kód ekvivalens.

Most tegyük fel, hogy $I_1 = I_2 = I = O = O_1 = O_2$, $n_2 = n$, $Cs_1 = Cs = Cs_2$ egy MDSC, végül f_1 a minimális távolságú dekódolás. Ha ψ az O^n önmagába való **távolságtartó leképezés**e (vagyis $d(\mathbf{u},\mathbf{v}) = d\big(\psi(\mathbf{u}),\psi(\mathbf{v})\big)$ az O^n bármely két $\mathbf{u}$ és $\mathbf{v}$ elemére), amelynek C_1-re való φ megszorítása a C_1-et C_2-re képezi le, akkor a két kód ekvivalens, feltéve, hogy f_2 is a minimális távolságú dekódolás. Ekkor ugyanis $n_1 = n$, és ha $\psi(\mathbf{u}_1) = \psi(\mathbf{u}_2)$, akkor $d(\mathbf{u}_1,\mathbf{u}_2) = d\big(\psi(\mathbf{u}_1),\psi(\mathbf{u}_2)\big) = 0$, tehát $\mathbf{u}_1 = \mathbf{u}_2$, a leképezés injektív, és mivel φ ráképezés, tehát szürjektív, így bijektív, továbbá

$$P_2\big(\boldsymbol{\eta}_2 = \psi(\mathbf{v})\big|\boldsymbol{\xi}_2 = \varphi(\mathbf{u})\big) = \left(\frac{p}{q-1}\right)^{d(\varphi(\mathbf{u}),\psi(\mathbf{v}))}(1-p)^{n-d(\varphi(\mathbf{u}),\psi(\mathbf{v}))}$$
$$= \left(\frac{p}{q-1}\right)^{d(\mathbf{u},\mathbf{v})}(1-p)^{n-d(\mathbf{u},\mathbf{v})} = P_1(\boldsymbol{\eta}_1 = \mathbf{v}|\boldsymbol{\xi}_1 = \mathbf{u})$$

bármely $\mathbf{u} \in C_1$, $\mathbf{v} \in O^n$ pár esetén, amiből következik a hibavalószínűségek egyenlősége is. (Megjegyezzük, hogy ψ a teljes O^n halmazon bijektív, hiszen láttuk, hogy távolságtartó leképezés injektív, és egy véges halmaz önmagába való injektív leképezése egyben szürjektív is.)

ψ akkor és csak akkor távolságtartó, ha $\psi(u_1 \dots u_n) = \sigma_1\big(u_{\pi^{-1}(1)}\big) \dots \sigma_n\big(u_{\pi^{-1}(n)}\big)$, ahol π az indexhalmaz permutációja, míg a σ_i-k az O halmaz permutációi. Az könnyen belátható, hogy sem π, sem a σ_i-k nem változtatnak a távolságon. Nézzük a másik irányt, legyen tehát ψ az O^n önmagába való távolságtartó leképezése, és legyen $\mathbf{u}^{(0)}$ egy tetszőleges, rögzített eleme O^n-nek, valamint minden $n \geq i \in \mathbb{N}^+$ indexre legyen $\mathbf{u}^{(i)}$ egy-egy olyan O^n-beli elem, amely az i-edik és csak az i-edik pozícióban különbözik (de különbözik!) $\mathbf{u}^{(0)}$-tól. A továbbiakban bármely $\mathbf{u} \in O^n$-re legyen $\psi(\mathbf{u}) = \mathbf{v}$. Ekkor $d\big(\mathbf{v}^{(0)},\mathbf{v}^{(i)}\big) = 1$, vagyis $\mathbf{v}^{(0)}$ és $\mathbf{v}^{(i)}$ is pontosan egy helyen, mondjuk a k_i-edik pozícióban különbözik. Ha $i \neq j$, akkor $k_i \neq k_j$, ugyanis ellenkező esetben $1 \geq d\big(\mathbf{v}^{(i)},\mathbf{v}^{(j)}\big) = d\big(\mathbf{u}^{(i)},\mathbf{u}^{(j)}\big) = 2$ lenne, ami nyilvánvaló képtelenség. Ez azt jelenti, hogy a $\pi\colon i \mapsto k_i$ szabály az indexhalmaz egy permutációja. Most legyen $\tilde{\mathbf{u}}^{(i)}$ olyan vektor, amely $\mathbf{u}^{(0)}$-tól pontosan egy helyen, az i-edik pozícióban különbözik, továbbá amely különbözik $\mathbf{u}^{(i)}$-től. Ekkor $\tilde{\mathbf{v}}^{(i)}$ is egyetlen helyen különbözik $\mathbf{v}^{(0)}$-tól, mondjuk $\tilde{k}_i$-ben. Ha $\tilde{k}_i \neq k_i$, akkor $d\big(\mathbf{u}^{(i)},\tilde{\mathbf{u}}^{(i)}\big) = 1$, de $d\big(\mathbf{v}^{(i)},\tilde{\mathbf{v}}^{(i)}\big) = 2$, ami ellentmondás, így $\tilde{k}_i = k_i$. Ugyanakkor $v_{k_i}^{(i)} = \tilde{v}_{k_i}^{(i)}$ esetén $d\big(\mathbf{v}^{(i)},\tilde{\mathbf{v}}^{(i)}\big) = 0$, tehát $v_{k_i}^{(i)} \neq \tilde{v}_{k_i}^{(i)}$, így $\sigma_{k_i}\colon u_i^{(i)} \mapsto v_{k_i}^{(i)}$ O egy-egy permutációja.

Most tegyük fel, hogy ha $d\big(\mathbf{u}^{(0)},\mathbf{u}\big) \leq k < n$, akkor $\psi(u_1 \dots u_n) = \sigma_1\big(u_{\pi^{-1}(1)}\big) \dots \sigma_n\big(u_{\pi^{-1}(n)}\big)$, és legyen $\mathbf{u} \in O^n$ olyan, amelyre $d\big(\mathbf{u}^{(0)},\mathbf{u}\big) = k+1$. Az egyszerűség kedvéért feltehetjük, hogy a két vektor az első $k+1$ pozícióban különbözik. Legyen $\mathbf{u}'$ az a vektor, amely az első k pozícióban $\mathbf{u}$-val, a többi helyen $\mathbf{u}^{(0)}$-val azonos, és így $d\big(\mathbf{u}^{(0)},\mathbf{u}'\big) = k$ és $d(\mathbf{u}',\mathbf{u}) = 1$, míg $\mathbf{u}''$ olyan, amely csak a $k+1$-edik helyen tér el $\mathbf{u}^{(0)}$-tól, és itt $\mathbf{u}$-val egyezik. $\mathbf{u}''$-re $d\big(\mathbf{u}^{(0)},\mathbf{u}''\big) = 1$ és $d(\mathbf{u}'',\mathbf{u}) = k$, továbbá $d(\mathbf{u}',\mathbf{u}'') = k+1$. A távolságtartás miatt $d\big(\mathbf{v}^{(0)},\mathbf{v}\big) = k+1$. De $d(\mathbf{v},\mathbf{v}') = d(\mathbf{u},\mathbf{u}') = 1$, vagyis $\mathbf{v}'$ és $\mathbf{v}$ egy helyen különbözik. Ha ez egy olyan pozíció, ahol $\mathbf{v}^{(0)}$ és $\mathbf{v}'$ eltér, akkor $\mathbf{v}$ és $\mathbf{v}^{(0)}$ legfeljebb csak k helyen tér el, ami nem lehet. Ha ez az egy eltérő pozíció nem ott van, ahol $\mathbf{v}^{(0)}$ és $\mathbf{v}''$ különbözik, akkor $d(\mathbf{v},\mathbf{v}'') = k+2$, ami ismét lehetetlen. Végül abban az esetben, ha az előbbi pozíciók megegyeznek, de nem azonos a két érték, akkor $d(\mathbf{v},\mathbf{v}'') = k+1$, míg $d(\mathbf{u},\mathbf{u}'') = k$, így ez sem lehet, tehát $\mathbf{u}$ képét is meghatározták a π és σ_i permutációk.

Általában csak akkor mondanak két kódot ekvivalensnek, ha a fenti módon felelnek meg egymásnak, vagyis ha az egyik a másikból a komponensek, valamint az egyes pozíciókon a szimbólumhalmaz permutációjával áll elő. Ennek speciális esete, amikor a szimbólumhalmaz test, és az egyes pozíciókon alkalmazott permutációk a test valamely nem nulla elemével való szorzások. Ebben az esetben a két kódot **skalárekvivalens**nek mondják.

Ha a csatorna MDSC, és a bemeneti eloszlás egyenletes, akkor a hibák várható száma n-hosszúságú kódszóban np, ahol p annak a valószínűsége, hogy a kimeneten megjelenő szimbólum különbözik a bemenetre adott jeltől, vagyis annak, hogy egy jel az átvitel során megváltozott. Minimális távolságú

dekódolásnál a javítható hibák száma a 2.10. Tétel szerint arányos a kód távolságával, így ahhoz, hogy a várhatóan fellépő valamennyi hibát ki tudjuk javítani minimális távolságú dekódolással, szükséges, hogy d arányosan nőjön n-nel (mint láttuk, nagy kódsebesség és kis döntési hiba nagy kódszóhosszúsággal érhető el), vagyis biztosítani kell, hogy $np \sim d$ teljesüljön, azaz hogy $\delta = \frac{d}{n} \sim p$ legyen. Sajnos a legtöbb kódcsalád nem teljesíti ezt a feltételt, általában $\delta \to 0$, ha $n \to \infty$.

4. Lineáris kódok

4.1. Jelölés

Legyen $n \in \mathbb{N}^+$. $\mathbb{F}_q^n$-et mint $\mathbb{F}_q$ fölötti n-dimenziós lineáris teret $V_q^{(n)}$, ennek elemeit és a komponensekből álló oszlopvektort $\mathbf{u}$, a megfelelő sorvektort $\boldsymbol{u}^T$ jelöli. $n \geq k \in \mathbb{N}$-re $W_q^{(n,k)}$ a $V_q^{(n)}$ (egy) k-dimenziós altere.

Δ

4.2. Definíció

Ha $\mathcal{S}$ Abel-csoport, és $\mathcal{C} \leq \mathcal{S}^n$ a komponensenkénti $\mathcal{S}$-beli művelettel, akkor C **csoportkód**. Ha $\mathcal{S}^n$ egyben egy test feletti vektortér, és $\mathcal{C}$ ennek k-dimenziós altere, akkor a kód **lineáris**. Az előbbi lineáris kód jele $[n, k, d]_q$, ahol d és q egymástól függetlenül elhagyható.

Δ

A C kód nyilván pontosan akkor csoportkód, ha $\mathcal{S}$ additív Abel-csoport és $C - C \subseteq C$, továbbá a korábbi és a mostani definíciókból látható, hogy egy $[n, k]_q$ kódban $M = q^k$.

4.3. Tétel

Ha $n \in \mathbb{N}^+$, és $C \subseteq V_q^{(n)}$ legalább 1-dimenziós altér, akkor $d(C) = w(C)$.

Δ

Bizonyítás:

$k \geq 1$ és $q \geq 2$, így $|C| = q^k \geq q \geq 2$, ahol k az altér dimenziója. Lineáris tér additív Abel-csoport az összeadással, és altér zárt a kivonásra, ezért $\mathcal{S} = \mathbb{F}_q$-val $\mathbb{F}_q^n$ és C megfelel a 2.1. Definíció és 2.2. Tétel előírásainak.

□

4.4. Definíció

Legyen $n \in \mathbb{N}^+$, $\mathbf{a} \in V_q^{(n)}$ és $\mathbf{b} \in V_q^{(n)}$. $(\mathbf{a}, \mathbf{b}) = \mathbf{a}^T\mathbf{b} = \sum_{i=0}^{n-1} a_i b_i$ az $\mathbf{a}$ és $\mathbf{b}$ **skalárszorzata**, és $\mathbf{a}$, $\mathbf{b}$ **ortogonális**, ha $(\mathbf{a}, \mathbf{b}) = 0$. $W_q^{(n,k)^\perp} = \left\{\mathbf{x} \in V_q^{(n)} \middle| \forall \left(\mathbf{v} \in W_q^{(n,k)}\right) : (\mathbf{v}, \mathbf{x}) = 0\right\}$ a $W_q^{(n,k)}$ **ortogonális altere**.

Δ

4.5. Tétel

$W_q^{(n,k)^\perp}$ a $V_q^{(n)}$ $n-k$-dimenziós altere, és $\left(W_q^{(n,k)^\perp}\right)^\perp = W_q^{(n,k)}$. $W_q^{(n,k)}$ és $W_q^{(n,k)^\perp}$ metszete általában nem csupán a nullvektort tartalmazza, így a két altér direkt összege általában nem $V_q^{(n)}$.

□

Bizonyítás:

$W_q^{(n,k)^\perp} \subseteq V_q^{(n)}$ a definíció következménye. Amennyiben $\mathbf{x} \in W_q^{(n,k)^\perp}$, $\mathbf{y} \in W_q^{(n,k)^\perp}$, $a \in \mathbb{F}_q$ és $b \in \mathbb{F}_q$, akkor bármely $W_q^{(n,k)}$-beli $\mathbf{u}$-val

$$(\mathbf{u}, a\mathbf{x}+b\mathbf{y}) = \sum_{i=0}^{n-1} u_i(ax_i+by_i) = a\sum_{i=0}^{n-1} u_i x_i + b\sum_{i=0}^{n-1} u_i y_i = a(\mathbf{u},\mathbf{x}) + b(\mathbf{u},\mathbf{y}) = 0,$$

$W_q^{(n,k)^\perp}$ altere $V_q^{(n)}$-nek. Ha $k=0$, azaz az altér csupán a nullvektorból áll, akkor az ortogonális altér a teljes tér, hiszen a nullvektorra minden vektor merőleges, ekkor az ortogonális altér dimenziója valóban $n-k$. Nézzük a $k>0$ esetet. Legyen $\mathbf{x}$ az ortogonális altér egy eleme, és $\mathbf{u}^{(0)}, \dots, \mathbf{u}^{(k-1)}$ a $W_q^{(n,k)}$ egy bázisa. Ekkor $\sum_{t=0}^{n-1} u_t^{(j)} x_t = 0$ a szóbajövő j értékekre, azaz $\mathbf{x}$ megoldása az $\mathbf{Ux}=\mathbf{0}$ egyenletnek, ahol $\mathbf{U}$ az együttható-mátrix: a $k>i\in\mathbb{N}$, $n>j\in\mathbb{N}$ indexekre $U_{i,j}=u_j^{(i)}$. A mátrix sorai a lineárisan független $\mathbf{u}^{(i)}$ vektorok, így a mátrix rangja k, de akkor az n-méretű $\mathbf{x}$-ben pontosan $n-k$ komponens választható szabadon, a megoldások $n-k$-dimenziós teret alkotnak.

Ha $\mathbf{u}$ olyan eleme az altérnek, hogy $\sum_{i=0}^{n-1} u_i^2 = 0$, akkor $\mathbf{u}$ önmagára ortogonális. Ha $q=2^m$, akkor $e=-e$-ből $e^2=-e$, és ha $q\equiv 1\ (4)$, akkor $\left(u^{\frac{q-1}{4}}\right)^2 = -e$, ahol u a test egy primitív eleme, így az előbbi esetben $ee0\dots0$, míg a második esetben $a=u^{\frac{q-1}{4}}$-gyel $ea0\dots0$ nem nulla önortogonális vektor, vagyis ilyen q-k esetén minden legalább kétdimenziós térben van nem nulla önortogonális vektor. Most legyen $q\equiv -1\ (4)$. Az $x^2=a$ egyenletnek, ahol $a=u^l$, akkor és csak akkor van egy $b=u^k$ megoldása, ha $2k\equiv l\ (q-1)$, vagyis pontosan akkor, ha l páros, így a nem nulla elemeknek pontosan a fele négyzetelem a testben (ez láthatóan minden páratlan q esetén igaz), vagyis az ilyen elemek száma $\frac{q-1}{2}$. Figyelembe véve, hogy $0^2=0$, $\left|\{e+x^2 | x\in\mathbb{F}_q\}\right| = \left|\{-y^2 | y\in\mathbb{F}_q\}\right| = \frac{q+1}{2}$. A két halmaz együttesen $q+1$ elemből áll, de $\mathbb{F}_q$-nak csupán q különböző eleme van, ezért van legalább egy közös elem, mondjuk $e+a^2$ és $-b^2$, így $e+a^2=-b^2$, azaz $e+a^2+b^2=0$, és az $eab0\dots0$ vektor önortogonális.

Az eredeti altér minden vektora merőleges az ortogonális altér valamennyi vektorára, tehát $W_q^{(n,k)} \subseteq \left(W_q^{(n,k)^\perp}\right)^\perp$. Ám a két tér dimenziója és így a két tér is azonos, tehát $\left(W_q^{(n,k)^\perp}\right)^\perp = W_q^{(n,k)}$.

□

4.6. Definíció

Legyen $n\in\mathbb{N}^+$, $n\geq k\in\mathbb{N}$ és $W_q^{(n,k)}$ egy $[n,k]_q$-kód. A $W_q^{(n,k)}$ lineáris tér egy bázisának elemeiből mint sorvektorokból álló $\mathbf{G}$ mátrix **a kód generátormátrixa**, a $W_q^{(n,k)^\perp}$ ortogonális tér bázisvektoraihoz tartozó sorvektorokból mint sorokból álló $\mathbf{H}$ mátrix **a kód (paritás)ellenőrző mátrixa**.

Δ

4.7. Tétel

Egy $[n,k]_q$-paraméterű kód generátormátrixa egy $\mathbb{F}_q$ fölötti, $k\times n$ méretű, k-rangú mátrix, míg a kód ellenőrző mátrixa $\mathbb{F}_q$ fölötti, $(n-k)\times n$ méretű, $n-k$-rangú mátrix.

Az $\mathbb{F}_q$ fölötti $k\times n$ méretű, k-rangú $\mathbf{G}$ és $(n-k)\times n$ méretű, $n-k$-rangú $\mathbf{H}$ mátrix akkor és csak akkor generátor- és ellenőrző mátrixa ugyanazon $[n,k]_q$-paraméterű kódnak, ha $\mathbf{HG}^T=\mathbf{0}$, továbbá $\mathbf{v}\in V_q^{(n)}$ akkor és csak akkor eleme a kódnak, ha $\mathbf{Hv}=\mathbf{0}$.

Δ

Bizonyítás:

$W_q^{(n,k)}$-nak mint az $\mathbb{F}_q$ fölötti n-komponensű vektorokból álló tér k-dimenziós alterének minden eleme szintén $\mathbb{F}_q$ fölötti n-komponensű vektor, a bázis k vektort tartalmaz, és ezek lineárisan függetlenek, így kiadódik a $\mathbf{G}$ méretére, rangjára és elemeire vonatkozó állítás.

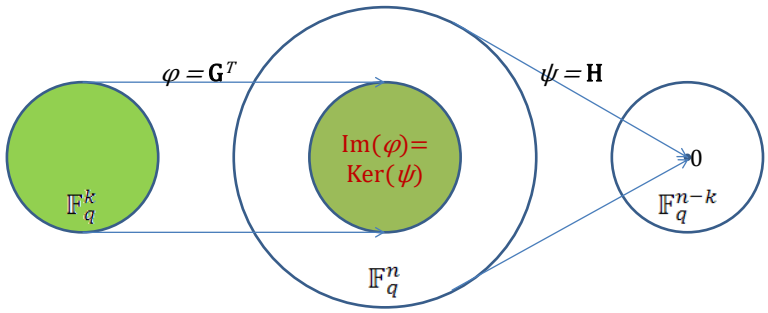
H sorai $V_q^{(n)}$-beli vektorokhoz tartozó sorvektorok, így $\mathbb{F}_q$ fölötti n-esek, továbbá az ortogonális altér dimenziója $n-k$, tehát **H** $\mathbb{F}_q$ elemeiből álló $(n-k)\times n$-es mátrix, és sorai mint bázisvektorok lineárisan függetlenek, a rang $n-k$. **G** sorai az altér elemei, **H** sorai az ortogonális altérhez tartoznak, így **H** bármely sorát a **G** tetszőleges sorával szorozva nullát kapunk, **H** és $\mathbf{G}^T$ szorzata nulla.

Fordítva, ha **G** sorai n-komponensűek, akkor elemei $V_q^{(n)}$-nek, és mivel a mátrix rangja azonos a sorok számával, ezért a sorok lineárisan függetlenek, és így az n-dimenziós tér egy k-dimenziós alterét feszítik ki. Hasonlóan kapjuk, hogy **H** sorai a $V_q^{(n)}$ egy $n-k$-dimenziós alterének bázisát alkotják. Végül $\mathbf{HG}^T=$-ból következik, hogy a két mátrix sorai, vagyis a két altér bázisának vektorai merőlegesek egymásra, amiből következik, hogy **G** sorainak bármely lineáris kombinációja merőleges **H** sorainak tetszőleges lineáris kombinációjára, tehát a **G** illetve **H** által meghatározott altér merőleges egymásra, és a két dimenzió összege n, így a két altér egymás ortogonális komplementere, amiből következik, hogy **G** és **H** egy $[n,k]_q$-paraméterű kód generátor- és ellenőrző mátrixa.

Legyen $\mathbf{v}\in W_q^{(n,k)}$, akkor az ortogonális altér minden eleme, de így **H** minden sora merőleges **v**-re, minden ilyen szorzat, és emiatt **Hv** is **0** lesz. Fordítva, ha **Hv** nulla, akkor **v** a **H** minden sorára mint $W_q^{(n,k)^\perp}$-beli vektorra ortogonális, de akkor $W_q^{(n,k)^\perp}$ minden vektorára is merőleges, hiszen ezek a mátrix sorainak lineáris kombinációi, **v** ortogonális a teljes $W_q^{(n,k)^\perp}$ altérre, azaz $\mathbf{v}\in W_q^{(n,k)}$.

□

A **G** illetve a **H** mátrix ismeretében egy $[n,k]_q$ kódot tekinthetünk a következő módon is. A kódolandó üzenetek az $\mathbb{F}_q$ fölötti k-dimenziós tér elemei, amelyeket a szintén $\mathbb{F}_q$ fölötti n-dimenziós tér elemeivel kódolunk, vagyis a kódolás egy $\varphi\colon \mathbb{F}_q^k\to\mathbb{F}_q^n$ leképezés, és a leképezést a $\varphi\colon \mathbf{u}^T\mapsto\mathbf{u}^T\mathbf{G}$ megfeleltetés adja, ahol **u** az $\mathbb{F}_q^k$ tetszőleges eleme. Ekkor $C=\mathrm{Im}(\varphi)=\mathrm{Im}(\mathbf{G})$ a kód. Ugyanakkor azt is mondhatjuk, hogy a kód az $\mathbb{F}_q$ fölötti n-dimenziós tér azon és csak azon elemeiből áll, amelyeket a $\psi\colon\mathbf{v}\mapsto\mathbf{Hv}$ megfeletetés az $n-k$-dimenziós tér nullelemére képez, vagyis amelyek benne vannak a leképezés magjában, tehát $C=\mathrm{Ker}(\psi)=\mathrm{Ker}(\mathbf{H})$. Az első leképezésnek injektívnek kell lennie, hiszen csak ilyen leképezéssel kapunk kódolást, és ez teljesül, hiszen **G** sorai lineárisan függetlenek. Ugyanakkor a második leképezés szürjektíven képezi le $\mathbb{F}_q^n$-t $\mathbb{F}_q^{n-k}$-ra, mivel **H** sorai lineárisan függetlenek, így generálják az $n-k$-dimenziós teret. Az előbb mondottakat szemlélteti az alábbi 4. ábra.



4. ábra

Az ábrából leolvasható az az egyébként nyilvánvaló tény, hogy $\mathbb{F}_q^k\cong\mathcal{C}\leq\mathbb{F}_q^n$, és hogy $\mathbf{HG}^T=\mathbf{0}$.

Felhívjuk a figyelmet rá, hogy egy kódnak több különböző generátormátrixa és több különböző ellenőrző-mátrixa lehet, hiszen egy lineáris tér bázisa korántsem egyértelmű. Sőt, még az sem igaz, hogy egy adott generátormátrixhoz egy és csak egy ellenőrző mátrix tartozik, mivel a kód bármely generátormátrixára és tetszőleges ellenőrző mátrixára igaz a tétel. Végül a tételből az is kiolvasható, hogy egy kódot egyértelműen meghatározza valamely generátor- vagy ellenőrző mátrixa, és akkor ez a mátrix meghatározza a kód valamennyi generátor- és ellenőrző mátrixát. Kérdés, hogy hogyan lehet adott generátormátrixhoz meghatározni egy ellenőrző mátrixot, vagy fordítva.

4.8. Definíció

Az $[n,k]$-paraméterű kód generátormátrixa **standard alakú**, ha $\mathbf{G}=(\mathbf{I}_k\ \mathbf{P})$ vagy $\mathbf{G}=(\mathbf{P}\ \mathbf{I}_k)$ alakú. Hasonlóan definiáljuk a standard alakú ellenőrző mátrixot is.

Δ

4.9. Tétel

Ha $\mathbf{H}=(\mathbf{I}_{n-k}\ \mathbf{P})$ az $[n,k]_q$-paraméterű kód ellenőrző mátrixa, akkor $\mathbf{G}=(-\mathbf{P}^T\ \mathbf{I}_k)$ a kód egy generátormátrixa. Fordítva, ha $\mathbf{G}=(\mathbf{I}_k\ \mathbf{P})$ egy lineáris kód generátormátrixa, akkor $\mathbf{H}=(-\mathbf{P}^T\ \mathbf{I}_{n-k})$ egy lehetséges ellenőrző mátrix.

Δ

Bizonyítás:

$(\mathbf{I}_{n-k}\ \mathbf{P})(-\mathbf{P}^T\ \mathbf{I}_k)^T=(\mathbf{I}_{n-k}\ \mathbf{P})\begin{pmatrix}-\mathbf{P}\\ \mathbf{I}_k\end{pmatrix}=-\mathbf{P}+\mathbf{P}=\mathbf{0}$. A másik állítás bizonyítása hasonló.

□

Az előző tétel alapján könnyen meghatározhatunk egy adott generátormátrixhoz egy ellenőrző mátrixot, vagy fordítva. Tegyük fel, hogy adott egy $[n,k]_q$ kód ellenőrző-mátrixa, $\mathbf{H}$. Mivel a mátrix sorainak száma $n-k$, és a rangja ugyanekkora, ezért van a mátrixban $n-k$ lineárisan független oszlop, és így egy $n-k$-méretű reguláris részmátrix. Most $\mathbf{H}$-t jobbról megszorozva egy alkalmas $\mathbf{\Pi}$ permutációs mátrixszal, a reguláris részmátrix a mátrix első $n-k$ oszlopába vihető, és ha ez a részmátrix $\mathbf{M}$, akkor $\mathbf{H}'=\mathbf{M}^{-1}\mathbf{H}\mathbf{\Pi}=(\mathbf{I}_{n-k}\ \mathbf{P})$ lesz, és $\mathbf{G}'=(-\mathbf{P}^T\ \mathbf{I}_k)$ a $\mathbf{H}'$ által meghatározott kód egy generátormátrixa. Most legyen $\mathbf{G}=\mathbf{G}'\mathbf{\Pi}^T$. Permutációs mátrix inverze egyenlő a mátrix transzponáltjával, így $\mathbf{G}'=\mathbf{G}\mathbf{\Pi}$. Ekkor $\mathbf{0}=\mathbf{H}'\mathbf{G}'^T=(\mathbf{M}^{-1}\mathbf{H}\mathbf{\Pi})(\mathbf{G}\mathbf{\Pi})^T=\mathbf{M}^{-1}\mathbf{H}\mathbf{\Pi}\mathbf{\Pi}^T\mathbf{G}^T=\mathbf{M}^{-1}(\mathbf{H}\mathbf{G}^T)$, és mivel $\mathbf{M}^{-1}$ reguláris, ezért $\mathbf{M}^{-1}(\mathbf{H}\mathbf{G}^T)=\mathbf{0}$ akkor és csak akkor, amennyiben $\mathbf{H}\mathbf{G}^T=\mathbf{0}$, vagyis $\mathbf{G}$ a kód generátormátrixa.

Az előzőek szerint egy ellenőrző mátrixból úgy tudunk meghatározni egy generátormátrixot, hogy a sorokon végzett reguláris műveletekkel (például Gauss-eliminációval), valamint az oszlopok sorrendjének változtatásával úgy alakítjuk át $\mathbf{H}$-t, hogy a bal szélén egységmátrix álljon. Ebből a mátrixból meghatározzuk $\mathbf{G}'$-t, és az így kapott mátrix oszlopait a $\mathbf{H}$ oszlopain végrehajtott cserékkel ellenkező sorrendben és irányban permutálva megkapjuk a keresett generátormátrixot.

Legyen például $\mathbb{F}_q=\mathbb{Z}_5$ és $\mathbf{H}=\begin{pmatrix}2&1&0&3&1&4&2\\1&3&0&1&0&2&0\\2&1&0&1&4&4&1\\3&3&1&4&2&1&3\end{pmatrix}$. Ebből csak a sorokon végzett invertálható átalakításokkal kapjuk a $\mathbf{H}''=\mathbf{M}^{-1}\mathbf{H}=\begin{pmatrix}4&3&3&3\\3&3&2&4\\2&4&1&0\\2&2&2&0\end{pmatrix}\begin{pmatrix}2&1&0&3&1&4&2\\1&3&0&1&0&2&0\\2&1&0&1&4&4&1\\3&3&1&4&2&1&3\end{pmatrix}=\begin{pmatrix}1&0&3&0&2&2&0\\0&1&4&0&4&0&0\\0&0&0&1&1&0&0\\0&0&0&0&0&0&1\end{pmatrix}$ mátrixot. Ez utóbbi mátrix oszlopait a $\pi=(3,5,6,7,4)$ ciklusnak megfelelő permutációval felcserélve a

$$\mathbf{H}'=\mathbf{H}''\mathbf{\Pi}=\begin{pmatrix}1&0&3&0&2&2&0\\0&1&4&0&4&0&0\\0&0&0&1&1&0&0\\0&0&0&0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&0&0&1&0&0\\0&0&1&0&0&0&0\\0&0&0&0&0&1&0\\0&0&0&0&0&0&1\\0&0&0&1&0&0&0\end{pmatrix}=\begin{pmatrix}1&0&0&0&3&2&2\\0&1&0&0&4&4&0\\0&0&1&0&0&1&0\\0&0&0&1&0&0&0\end{pmatrix}=(\mathbf{I}_4\ \mathbf{P})$$

mátrixot kapjuk, ahol $\mathbf{P} = \begin{pmatrix} 3 & 2 & 2 \\ 4 & 4 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Ebből $\mathbf{G}' = (-\mathbf{P}^T\ \mathbf{I}_3) = \begin{pmatrix} 2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 4 & 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$, és végül

$$\mathbf{G} = \mathbf{G}'\mathbf{\Pi}^T = \begin{pmatrix} 2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 4 & 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 4 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

4.10. Definíció

Az S fölötti $(n, M)_q$ kód **szisztematikus** vagy **szeparábilis a** $0 \leq i_1 < \cdots < i_l < n$ **indexekre**, ha $l = \lceil \log_q M \rceil$, és a kódban ezen az l pozíción álló l-esek páronként különbözőek. A kód **szisztematikus**, ha vagy az első, vagy az utolsó l pozícióra nézve szeparábilis.

Δ

Ha egy kód szisztematikus valamely pozíciókra, akkor az ezen pozíción álló l-esek tekinthetőek az üzenetnek, így hibajavítás után a dekódolás a többi pozíción lévő jegyek elhagyását jelenti.

Valamely indexekre szeparábilis kód ekvivalens egy szisztematikus kóddal, hiszen oszlopcserékkel a $0 \leq i_1 < \cdots < i_l < n$-indexű oszlopok átvihetőek a $0,1, \ldots, l-1$-indexű oszlopokba.

4.11. Tétel

Minden lineáris kód ekvivalens egy szisztematikus kóddal.

Δ

Bizonyítás:

Tekintsük a kód $\mathbf{G}$ generátormátrixát. $\mathbf{G}$-nek k sora van, és a sorai lineárisan függetlenek, így van k lineárisan független oszlopa is. Ha ezek az oszlopok a $0 \leq i_0 < \cdots < i_{k-1} < n$ indexekhez tartoznak, akkor, miközben előállítjuk a kódot, azaz vesszük a generátormátrix sorainak valamennyi lineáris kombinációját, a kijelölt oszlopokhoz tartozó részmátrix előállítja a k-dimenziós tér valamennyi vektorát egyszer és csakis egyszer, vagyis a kód szeparábilis az előbb megadott indexekre, és akkor a korábbi megjegyzés alapján a kód szisztematikussá tehető az oszlopok megfelelő permutációjával.

□

Az alábbi tétel szerint egy kód ellenőrző mátrixa szoros kapcsolatban áll a távolságával.

4.12. Tétel

Legyen $\mathbf{H}$ a d-távolságú $[n, k]$ kód ellenőrző mátrixa, ahol $k \geq 1$. Ekkor $\mathbf{H}$-nak van d lineárisan összefüggő oszlopa, de bármely ennél kevesebb oszlopa lineárisan független.

Δ

Bizonyítás:

A $V_q^{(n)}$-beli $\mathbf{c}$ akkor és csak akkor eleme $W_q^{(n,k)}$-nak, ha $\mathbf{Hc} = \mathbf{0}$. Legyen a $\mathbf{0} \neq \mathbf{c} \in V_q^{(n)}$ vektor súlya $(n \geq) t \in \mathbb{N}$, $0 \leq i_1 < \cdots < i_t < n$ azok az indexek, amelyekre $c_l \neq 0$, és $\mathbf{h}_{(i)}$ a $\mathbf{H}$ i-edik oszlopa. $\mathbf{0} = \mathbf{Hc} = \sum_{j=1}^{t} c_{i_j} \mathbf{h}_{(i_j)}$ pontosan akkor teljesül, ha a megadott c_{i_j}-k egy kódszó nem nulla komponensei. Lineáris kód súlya és távolsága azonos, vagyis a kód súlya is d, így a kódhoz tartozó bármely nem nulla vektor legalább d nem nulla komponenst tartalmaz, $\mathbf{Hc}$ csak úgy lehet $\mathbf{0}$, ha $t \geq d$. Ez azt jelenti,

hogy d-nél kevesebb (de legalább egy) nem nulla komponensű vektor esetén $\mathbf{Hc} \neq \mathbf{0}$, d-nél kevesebb oszlop lineárisan független. Másrészt mindig van olyan $\mathbf{c}$ kódszó, amelynek a súlya pontosan d, és akkor $\mathbf{H}$-ban a $\mathbf{c}$ nem nulla komponenseihez tartozó indexek által meghatározott oszlopok lineárisan összefüggenek, van $\mathbf{H}$-ban d lineárisan összefüggő oszlop.

□

4.13. Definíció

A C lineáris kód **duális**a $C^{\perp}$. C **önortogonális**, ha $C \subseteq C^{\perp}$, és **önduális**, ha $C = C^{\perp}$.

Δ

4.14. Tétel

Legyen $\mathbf{G}$ és $\mathbf{H}$ az $[n,k]$-paraméterű C kód generátor- és ellenőrző mátrixa. Ekkor $\mathbf{G}^D = \mathbf{H}$ és $\mathbf{H}^D = \mathbf{G}$ a duális kód generátor- és ellenőrző mátrixa. C pontosan akkor önortogonális, ha $\mathbf{G}\mathbf{G}^T = \mathbf{0}$, és akkor és csak akkor önduális, ha önortogonális, és $n = 2k$. Önortogonális kód bármely lineáris részkódja önortogonális.

Δ

Bizonyítás:

$\mathbf{G}$ sorai a kód mint altér egy bázisának elemei, és $\mathbf{H}$ sorai ezen altér ortogonális alterének egy bázisa. Ortogonális altér ortogonális altere az eredeti altér, így igaz az első állítás.

$\mathbf{G}\mathbf{G}^T = \mathbf{0}$ akkor és csak akkor, ha a generátormátrix sorai, azaz a kód mint altér egy bázisának elemei páronként merőlegesek egymásra. Ekkor az altér bármely két vektora merőleges egymásra, vagyis az altér bármely vektora merőleges az altér összes vektorára, amiből következik, hogy C minden eleme benne van az ortogonális kiegészítőben is. Ez viszont azt jelenti, hogy $\mathbf{G}\mathbf{G}^T = \mathbf{0}$ pontosan akkor igaz, ha teljesül a $C \subseteq C^{\perp}$ tartalmazás, vagyis ha a kód önortogonális.

$C = C^{\perp}$-ből következik, hogy egyrészt $C \subseteq C^{\perp}$, tehát a kód önortogonális, másrészt, hogy $k = n - k$, tehát hogy $n = 2k$. Ha viszont $C \subseteq C^{\perp}$, és $n = 2k$, akkor egyben az is igaz, hogy $C = C^{\perp}$, vagyis a kód önduális.

Az utolsó állítás abból következik, hogy ha $\mathbf{G}$ sorai merőlegesek egymásra, akkor a kód bármely generátormátrixának sorai is páronként ortogonálisak, ez a sorok bármely részhalmazára is igaz, és ez a részhalmaz az eredeti kód egy lineáris részkódját határozza meg, továbbá a lineáris részkód bármely bázisa kiegészíthető az eredeti tér egy bázisává, tehát valamely generátormátrixává.

□

Önortogonális például a $\mathbf{G} = \begin{pmatrix} 1\,0\,1\,0\,1\,0\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \end{pmatrix}$ mátrix által generált $[7,3]_2$-paraméterű kód, és egy $[8,4]_2$-paraméterű önduális kódot generál a $\mathbf{G} = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0 \\ 0\,1\,1\,0\,0\,1\,1\,0 \\ 0\,0\,0\,1\,1\,1\,1\,0 \end{pmatrix}$ mátrix.

Amennyiben egy kód generátormátrixának valamely oszlopa csak nullát tartalmaz, akkor nyilván a kód valamennyi szavában ezen a pozíción 0 áll. Ellenkező esetben igaz a következő tétel.

4.15. Tétel

Ha az $[n,k]_q$-paraméterű C kód valamely kódszavának j-edik pozícióján, ahol $n > j \in \mathbb{N}$, 0-tól különböző elem áll, akkor a kódszavak ezen pozícióján $\mathbb{F}_q$ minden eleme pontosan q^{k-1}-szer fordul elő, és az ezen oszlop elemeiből álló vektor súlya $(q-1)q^{k-1}$.

Δ

Bizonyítás:

Tekintsük a kód azon kódszavainak halmazát, amelyekben a j-edik pozíción 0 áll. Egy ilyen kódszó bármely konstansszorosában, és két ilyen kódszó összegében is 0 áll ezen a pozíción, tehát ezek a kódszavak a kód egy lineáris alterét alkotják. Amennyiben a kód valamennyi kódszavában ezen a helyen 0 van, akkor ez az altér azonos magával a kóddal, ellenkező esetben annak egy valódi altere. Nézzük az utóbbi esetet. A lineáris kód az összeadással additív Abel-csoport, és ennek az előbbi altér elemei egy részcsoportját képezik. Az eredeti tér két eleme akkor és csak akkor esik az altér szerinti ugyanazon mellékosztályba, ha a két kódszó különbsége benne van a részcsoportban, azaz ha a különbségvektorban a j-edik pozíción 0 áll. Ez viszont pontosan akkor teljesül, ha a kiválasztott két vektorban a megadott pozíción a test azonos eleme van, vagyis azt kaptuk, hogy a kód azon és csak azon elemei vannak azonos mellékosztályban, amelyeknek a j-edik komponense azonos. Egy csoport valamely részcsoportja szerinti valamennyi mellékosztályban ugyanannyi elem van, ezért már csak a mellékosztályok számát kell meghatározni. Legyen az eredetileg tekintett $\mathbf{u}$ szóban, amelyben tehát a j-edik pozíción álló elem nem 0, ez a nem nulla elem $0 \neq a \in \mathbb{F}_q$. Mivel a kód lineáris, ezért kódszó bármely konstansszorosa is kódszó, így ha b a test egy eleme, akkor a $\mathbf{v} = ba^{-1}\mathbf{u}$ kódszóban a j-edik pozíción b lesz, vagyis a test minden eleme előfordul a j-edik pozíción, így a mellékosztályok száma q. A kódszavak száma q^k, ezért egy-egy mellékosztályban pontosan q^{k-1} elem van, tehát a test minden eleme pontosan q^{k-1}-szer fordul elő a j-edik pozíción kódszavak között. Végül a súlyra vonatkozó állítást úgy kapjuk, hogy az oszlopban a 0 q^{k-1}-szer található, az összes többi vektorban ezen a helyen nem 0 áll, tehát az oszlop súlya $q^k - q^{k-1} = (q-1)q^{k-1}$.

□

Az $(n, M)_q$-paraméterű C kód kódsebessége $\mathcal{R} = \frac{1}{n}\log_q M$. $[n,k]_q$-kódban $M = q^k$, és ezt alkalmazva kapjuk egy lineáris kód kódsebességét.

4.16. Tétel

Az $[n,k]_q$-paraméterű C lineáris kód kódsebessége $\mathcal{R} = \frac{k}{n}$.

Δ

Most tekintsük az n-dimenziós bináris lineáris teret, és definiáljunk egy új műveletet: ha $\mathbf{u}$ és $\mathbf{v}$ a $\mathbb{Z}_2^n$ két eleme, akkor legyen $(\mathbf{u} \cap \mathbf{v})_i = u_i v_i$. Ekkor

$$d(\mathbf{u},\mathbf{v}) = w(\mathbf{u}-\mathbf{v}) = w(\mathbf{u}+\mathbf{v}) = \sum_{i=0}^{n-1}\big((u_i+v_i) \bmod 2\big) = \sum_{i=0}^{n-1}(u_i+v_i-2u_iv_i)$$
$$= \sum_{i=0}^{n-1}u_i + \sum_{i=0}^{n-1}v_i - 2\sum_{i=0}^{n-1}u_iv_i = w(\mathbf{u}) + w(\mathbf{v}) - 2w(\mathbf{u}\cap\mathbf{v}).$$

Ha ebben a térben két vektor, $\mathbf{u}$ és $\mathbf{v}$ ortogonális, akkor $0 = (\mathbf{u},\mathbf{v}) = \bigoplus_{i=0}^{n-1}u_iv_i = \sum_{i=0}^{n-1}u_iv_i \bmod 2$, így $\sum_{i=0}^{n-1}u_iv_i$ páros. Ha $\mathbf{u}$ önortogonális, azaz $\mathbf{u} = \mathbf{v}$, akkor tehát $\sum_{i=0}^{n-1}u_i^2 = \sum_{i=0}^{n-1}u_i = w(\mathbf{u})$ páros (mert $0^2 = 0$ és $1^2 = 1$), így egy önortogonális bináris kód bármely kódszavának súlya, és akkor bármely két kódszavának távolsága is, páros.

Bizonyos bináris kódoknál fontos az alábbi

4.17. Tétel

Ha a $\mathbf{G}$ generátormátrixszal megadott C bináris kód önortogonális, és $\mathbf{G}$ valamennyi sorának súlya osztható néggyel, akkor a kód valamennyi kódszavának súlya osztható 4-gyel.

Δ

Bizonyítás:
Bináris kódban a nem nulla együtthatókkal vett lineáris kombináció összeadás, így bármely lineáris kombináció megkapható összeadással, ezért elegendő azt bizonyítani, hogy ha két vektor súlya osztható néggyel, akkor hasonló igaz az összegükre is. Legyen a két vektor $\mathbf{u}$ és $\mathbf{v}$. A tétel előtt beláttuk, hogy $w(\mathbf{u}+\mathbf{v}) = w(\mathbf{u}) + w(\mathbf{v}) - 2\sum_{i=0}^{n-1} u_i v_i$, és ha C önortogonális, akkor $\sum_{i=0}^{n-1} u_i v_i$ páros szám. Ekkor viszont az előbbi egyenlőség jobb oldalán minden tag, és így a bal oldal is, osztható néggyel.
□

Korábban azt mondtuk, hogy a dekódolás egyszerűsítése érdekében alkalmazunk olyan kódokat, amelyeknek a szerkezete bizonyos strukturális összefüggéssel rendelkezik. A lineáris kódok ilyenek, ezért azt reméljük, hogy valamilyen jól használható, viszonylag egyszerű és gyors algoritmussal végezhető a dekódolás. Az alábbiakban megmutatjuk, hogy ez valóban így van.

Tekinsünk egy $[n,k,d]_q$-paraméterű C kódot, és legyen $\mathbf{u}$ ennek egy eleme. Tegyük fel, hogy az $\mathbf{u}$-t elküldve, a vétel helyére egy $\mathbf{v} \in \mathbb{F}_q^n$ vektor érkezik. Mivel $\mathbb{F}_q^n$ lineáris tér, ezért $\mathbf{v}$-t felírhatjuk $\mathbf{v} = \mathbf{u} + \boldsymbol{\varepsilon}$ alakban, ahol $\boldsymbol{\varepsilon}$ szintén $\mathbb{F}_q^n$ egy eleme. $\boldsymbol{\varepsilon}$ a **hibavektor**, ugyanis pontosan $\boldsymbol{\varepsilon}$ nem nulla elemei mutatják, hogy mely pozícióban és az adott pozícióban milyen hiba történt az átvitel során.

A korábbiakban $\mathbf{H}$-t csupán arra használtuk, hogy ellenőrizzük, vajon $\mathbf{v}$ eleme-e a kódnak: mint tudjuk, $\mathbf{v} \in C$ akkor és csak akkor igaz, ha $\mathbf{Hv} = \mathbf{0}$. Valójában az utóbbi szorzat ennél több információt rejt. Legyen $\mathbf{s} = \mathbf{Hv}$. $\mathbf{s}$ a $\mathbf{v}$ szóhoz tartozó **szindróma**. A szindróma az $\mathbb{F}_q$ fölötti $n-k$-dimenziós tér egy eleme, hiszen $\mathbf{s}$ a $\mathbf{H}$ oszlopainak lineáris kombinációja, és $\mathbf{H}$ rangja $n-k$. Ha $\mathbf{v}$-t javítani akarjuk, akkor ismernünk kell $\boldsymbol{\varepsilon}$-t. Mivel $\boldsymbol{\varepsilon}$ az n-dimenziós tér bármely eleme lehet, azaz q^n különböző hibavektor van, és a szindrómák száma ennél kevesebb, csupán q^{n-k} (feltéve, hogy valódi kódról van szó, azaz k legalább 1), a szindróma ismeretében nem várhatjuk el, hogy minden esetben helyesen javítunk. Ezt egyébként egyetlen kódtól sem remélhetjük, hiszen ha a vétel helyére egy, a küldöttől eltérő kódszó érkezik, akkor arról elég kevéssé meggyőzően lehetne állítani, hogy hibás. A szindróma ismeretében azonban bizonyos következtetést le tudunk vonni a hibára vonatkozóan:

$$\mathbf{s} = \mathbf{Hv} = \mathbf{H}(\mathbf{u}+\boldsymbol{\varepsilon}) = \mathbf{Hu} + \mathbf{H}\boldsymbol{\varepsilon} = \mathbf{0} + \mathbf{H}\boldsymbol{\varepsilon} = \mathbf{H}\boldsymbol{\varepsilon},$$

vagyis a szindróma értéke a hibától függ. Másrészről

$$\mathbf{H}\boldsymbol{\varepsilon}_1 = \mathbf{s}_1 = \mathbf{s}_2 = \mathbf{H}\boldsymbol{\varepsilon}_2 \Leftrightarrow \mathbf{0} = \mathbf{s}_1 - \mathbf{s}_2 = \mathbf{H}\boldsymbol{\varepsilon}_1 - \mathbf{H}\boldsymbol{\varepsilon}_2 = \mathbf{H}(\boldsymbol{\varepsilon}_1 - \boldsymbol{\varepsilon}_2) \Leftrightarrow \boldsymbol{\varepsilon}_1 - \boldsymbol{\varepsilon}_2 \in C,$$

tehát két hibavektor szindrómája akkor és csak akkor azonos, ha a különbségük kódszó. Mivel a kód egy altér, és az altér az összeadással részcsoport, ezért az előző megállapítás azt jelenti, hogy két hibavektor szindrómája pontosan akkor azonos, ha a két szó a C mint additív részcsoport szerinti azonos mellékosztályban van. Ezek szerint a szindróma alapján két hibavektort akkor és csak akkor tudunk megkülönböztetni, ha különböző mellékosztályban vannak, vagy másként, azonos mellékosztályban lévő hibavektorok között a szindróma alapján nem tudunk különbséget tenni. Mindez azt jelenti, hogy azonos mellékosztályban lévő hibavektorok közül egyet és csak egyet tekinthetünk reprezentánsnak, azaz minden olyan esetben, amikor a vett szó alapján számított szindróma $\mathbf{s}$, akkor az $\mathbf{s}$ által meghatározott mellékosztály reprezentánsát tekintjük **javítható hibamintá**nak, vagy másként **mellékosztályvezető**nek, vagyis feltesszük, hogy ez volt a hiba, és ezzel a vélt hibával korrigáljuk a vett szót, a mellékosztályba tartozó többi hibavektor viszont **nem javítható hibaminta**. Ennél többet nem is várhatunk. Ha a vett szó $\mathbf{v}$, akkor ez a q^k különböző kódszó bármelyikéből származhatott, vagyis $\mathbf{v}$ q^k különböző $\boldsymbol{\varepsilon}$ hibavektorral, hibamintával jöhetett létre, de a döntési függvény ezek közül egyre és csak egyre dönthet. Mivel a lehetséges hibaminták száma q^n, ezért átlagban $\frac{q^n}{q^k} = q^{n-k}$ lehet a javítható hibaminták száma, éppen annyi, ahány különböző szindróma van.

A következő kérdés, hogy milyen alapon válasszuk ki az egy mellékosztályba tartozó q^k különböző hibamintából az egyetlen javítható hibamintát. Legyen ez a mellékosztályhoz tartozó vektorok közül (egy) minimális súlyú, vagyis egy tetszőleges $\boldsymbol{\varepsilon}$ hibavektor esetén az $\boldsymbol{\varepsilon}$-t tartalmazó, $\mathbf{s}$ szindrómájú C szerinti mellékosztály $\boldsymbol{\varepsilon}^{(s)}$-sel jelölt reprezentánsa

$$\boldsymbol{\varepsilon}^{(s)} \in \boldsymbol{\varepsilon} + C = \{\boldsymbol{\varepsilon}' \in \mathbb{F}_q^n | \mathbf{H}\boldsymbol{\varepsilon}' = \mathbf{s} = \mathbf{H}\boldsymbol{\varepsilon}\} \wedge w\{\boldsymbol{\varepsilon}^{(s)}\} = \min_{\boldsymbol{\varepsilon}' \in \boldsymbol{\varepsilon}+C} \{w\{\boldsymbol{\varepsilon}'\}\}.$$

Ekkor az f döntési függvény olyan, hogy tetszőleges $\mathbf{v} \in \mathbb{F}_q^n$-re $f(\mathbf{v}) = \mathbf{v} - \boldsymbol{\varepsilon}^{(s)}$, ahol $\mathbf{s} = \mathbf{H}\mathbf{v}$. Ha $\mathbf{u}$ az üzenet, akkor, amint azt már láttuk, $\mathbf{H}\boldsymbol{\varepsilon}^{(s)} = \mathbf{s} = \mathbf{H}\mathbf{v} = \mathbf{H}\boldsymbol{\varepsilon}$, vagyis a tényleges hibaminta a javításra felhasznált hibamintával azonos mellékosztályban van. Ekkor viszont

$$\begin{aligned} d\big(\mathbf{v}, f(\mathbf{v})\big) &= d\big(\mathbf{v}, \mathbf{v} - \boldsymbol{\varepsilon}^{(s)}\big) = w\left(\mathbf{v} - \left(\mathbf{v} - \boldsymbol{\varepsilon}^{(s)}\right)\right) = w\big(\boldsymbol{\varepsilon}^{(s)}\big) = \min_{\boldsymbol{\varepsilon} \in \boldsymbol{\varepsilon}^{(s)}+C} \{w(\boldsymbol{\varepsilon})\} \\ &= \min_{\mathbf{u} \in C}\big\{w\big(\boldsymbol{\varepsilon}^{(s)} + \mathbf{u}\big)\big\} = \min_{\mathbf{u} \in C}\{w(\mathbf{v} - f(\mathbf{v}) + \mathbf{u})\} = \min_{\mathbf{u} \in C}\big\{w\big(\mathbf{v} - (f(\mathbf{v}) - \mathbf{u})\big)\big\} \\ &= \min_{\mathbf{u}' \in C}\{w(\mathbf{v} - \mathbf{u}')\} = \min_{\mathbf{u}' \in C}\{d(\mathbf{v}, \mathbf{u}')\}, \end{aligned}$$

tehát a fenti módon választott mellékosztály-vezetőkkel f minimális távolságú dekódolást valósít meg.

Amint látjuk, lineáris kódok esetén a minimális távolságú dekódoláshoz elegendő minden szindrómához tárolni a hozzá tartozó hibamintát. Általános esetben a minimális távolságú dekódoláshoz a lehetséges q^n szó mindegyikéhez tárolni kell a döntési függvény értékét, vagyis egy q^n-méretű tömböt kell tárolni. Ezzel szemben az ismertetett **szindróma-dekódolás**nál a szükséges tárméret csupán q^{n-k}, ami lényegesen kisebb az előző értéknél, és ennek ára mindössze egy mátrixszorzás.

Most legyen $\boldsymbol{\varepsilon}$ tetszőleges, $\frac{d}{2}$-nél kisebb súlyú hibaminta, és $\boldsymbol{\varepsilon}'$ az $\boldsymbol{\varepsilon}$-nal azonos mellékosztályban lévő, $\boldsymbol{\varepsilon}$-től különböző hibaminta. Ekkor $\mathbf{0} = \boldsymbol{\varepsilon} - \boldsymbol{\varepsilon}' \in C$, így a súlyokra vonatkozó háromszög-egyenlőtlenséggel $d \le w(\boldsymbol{\varepsilon} - \boldsymbol{\varepsilon}') \le w(\boldsymbol{\varepsilon}) + w(\boldsymbol{\varepsilon}') < \frac{d}{2} + w(\boldsymbol{\varepsilon}')$, és innen $w(\boldsymbol{\varepsilon}') > d - \frac{d}{2} = \frac{d}{2} > w(\boldsymbol{\varepsilon})$, vagyis egy mellékosztályban legfeljebb egy $\frac{d}{2}$-nél kisebb súlyú hibaminta lehet, az ilyen hibaminták mindegyike mellékosztályvezető, tehát a szindróma-dekódolással minden $\frac{d}{2}$-nél kevesebb hiba javítható, a kód a szindrómadekódolással legalább $\left\lfloor \frac{d-1}{2} \right\rfloor$-hiba javító. Legyen ugyanakkor $\mathbf{u}$ egy d-súlyú kódszó. $\mathbf{u}$ felírható $\mathbf{u} = \mathbf{u}^{(1)} - \mathbf{u}^{(2)}$ alakban úgy, hogy $\mathbf{u}^{(1)}$ megegyezik $\mathbf{u}$-val, kivéve valamely $\left\lfloor \frac{d}{2} \right\rfloor$ olyan pozíciót, ahol $\mathbf{u}$ nem nulla, és ezeken a helyeken $\mathbf{u}^{(1)}$-ben 0 áll, míg $\mathbf{u}^{(2)}$ éppen ezeken a helyeken azonos $-\mathbf{u}$-val, és minden más helyen 0. Ekkor $w\big(\mathbf{u}^{(1)}\big) = \left\lceil \frac{d}{2} \right\rceil = \left\lfloor \frac{d-1}{2} \right\rfloor + 1$, $w\big(\mathbf{u}^{(2)}\big) = \left\lfloor \frac{d}{2} \right\rfloor$, és $\mathbf{u}^{(1)}$, $\mathbf{u}^{(2)}$ azonos mellékosztályban van (hiszen a különbségük kódszó), vagyis kettejük mint hibaminták közül legfeljebb az egyik javítható, így biztosan lesz olyan, legfeljebb $\left\lceil \frac{d}{2} \right\rceil = \left\lfloor \frac{d-1}{2} \right\rfloor + 1$ súlyú hibaminta, amely nem javítható, így a kód pontosan $\left\lfloor \frac{d-1}{2} \right\rfloor$-hiba javító (ez nyilván nem meglepő, hiszen a szindróma-dekódolás minimális távolságú dekódolás, és d-távolságú kód minimális távolságú dekódolással pontosan $\left\lfloor \frac{d-1}{2} \right\rfloor$-hiba javító).

5. Ciklikus kódok

Emlékeztetünk rá, hogy ha a és $c \neq 0$ valós számok, akkor $a \bmod c = a - c\left\lfloor\frac{a}{c}\right\rfloor$, ami abban az esetben, ha a egész szám és c pozitív egész szám, azt jelenti, hogy $a \bmod c$ az a osztási maradéka a c-vel való osztáskor, azaz $c > a \bmod c \in \mathbb{N}$ és $a \bmod c \equiv a\ (c)$. Most legyen $\mathcal{R}$ egységelemes kommutatív gyűrű, és f valamint h $\mathcal{R}$ fölötti polinomok, ahol h főegyütthatója egység $\mathcal{R}$-ben. Ekkor f maradékosan osztható h-val úgy, hogy a maradék vagy 0, vagy a fokszáma kisebb h fokszámánál, és ez a maradék egyértelműen meghatározott. Jelölje ezt az egyértelműen meghatározott osztási maradékot $f \bmod h$. Legyen most b egy további valós szám, és g az $R[x]$ egy eleme. A definíciók alapján könnyű látni, hogy valós számokra igaz az $(a+b) \bmod c = \big((a \bmod c) + (b \bmod c)\big) \bmod c$ egyenlőség, ám $\mathbb{R}$-ben általában nem teljesül, hogy $(a+b) \bmod c = (a \bmod c) + (b \bmod c)$ (például legyen $\frac{c}{2} < a = b < c$), míg polinomgyűrűben az $(f+g) \bmod h = (f \bmod h) + (g \bmod h)$ összefüggés mindig érvényes, ugyanis polinomok összegének fokszáma nem nagyobb a tagok fokszámai maximumánál.

Most legyen f legfeljebb n-edfokú, és h m-edfokú. Nulla-együtthatós tagoktól eltekintve f egyértelműen írható az $f = f^{[0]} + x^m f^{[1]}$ alakban, ahol $\delta\big(f^{[0]}\big) < m$. Az előbbiek alapján, figyelembe véve, hogy ha az osztandó fokszáma kisebb az osztó fokszámánál, akkor a maradék megegyezik az osztandóval, $f \bmod h = f^{[0]} + \big(x^m f^{[1]} \bmod h\big)$, illetve, ha $f = \sum_{i=0}^{n} a_i x^i$ és $n \geq m-1$, akkor

$$f \bmod h = f^{[0]} + \big(x^m f^{[1]} \bmod h\big) = f^{[0]} + \left(x^m \sum_{i=0}^{n-m} a_{i+m}\big(x^i \bmod h\big) \bmod h\right).$$

Ha $m = n$ és h főpolinom, akkor ebből egyszerűen $f \bmod h = f - a_n h$, ahol a_n az f főegyütthatója (ez lehet 0 is, hiszen csak azt tettük fel, hogy f legfeljebb n-edfokú).

5.1. Definíció

A C$\subseteq S^n$ kód **ciklikus**, ha $\mathbf{u}^T = u_0 \dots u_{n-2}u_{n-1} \in C$ esetén $\mathbf{u}^T_{\rightarrow} = u_{n-1}u_0 \dots u_{n-2} \in C$. Az $l \in \mathbb{Z}$ hellyel való ciklikus jobbra léptetéssel kapott vektort $\mathbf{u}_{\underrightarrow{(l)}}$ jelöli.

Δ

Nyilván igaz, hogy $\mathbf{u}_{\underrightarrow{(l+1)}} = \left(\mathbf{u}_{\underrightarrow{(l)}}\right)_{\rightarrow}$, továbbá $\mathbf{u}_{\underrightarrow{(l)}} = \mathbf{u}_{\underrightarrow{(l \bmod n)}}$.

A definícióban nem kötöttük ki, ám a továbbiakban feltesszük, hogy a ciklikus kód lineáris is. Ekkor a ciklikus kódok tárgyalását segíti, ha a kódszavakat polinomként kezeljük.

5.2. Definíció

Legyen $n \in \mathbb{N}^+$, $\mathbf{u} \in V_q^{(n)}$, $u = \sum_{i=0}^{n-1} u_i x^i$, és $S^{(n)} = \left\{u \in \mathbb{F}_q[x] \middle| \mathbf{u} \in V_q^{(n)}\right\}$. Ha C egy $[n,k]_q$-paraméterű ciklikus kód, akkor $S^{[C]} = \left\{u \in \mathbb{F}_q[x] \middle| \mathbf{u} \in C\right\}$ **a kódpolinomok halmaza**, és $u \in S^{[C]}$ **az u kódszóhoz tartozó kódpolinom**.

Δ

Közvetlenül látható, hogy bármely két kódszóra és testbeli elemre $a\mathbf{g}$-hez illetve $\mathbf{g}^{(1)} + \mathbf{g}^{(2)}$-höz tartozó kódpolinom ag és $g^{(1)} + g^{(2)}$.

5.3. Tétel

Ha $n \in \mathbb{N}^+$ és $\mathbf{u} \in V_q^{(n)}$, akkor $u_{\rightarrow} = xu \bmod (x^n - e)$.

Δ

Bizonyítás:
$u = \sum_{i=0}^{n-1} u_i x^i$-ből $xu \bmod (x^n - e) = u_{n-1}x^0 + \sum_{i=1}^{n-1} u_{i-1}x^i = \sum_{i=0}^{n-1} u_{(i-1) \bmod n} x^i = u_{\rightarrow}$.

□

A fentiekből könnyen kapjuk, hogy $u_{\underrightarrow{(l)}} = x^{l \bmod n} u \bmod (x^n - e) = x^l u \bmod (x^n - e)$, tekintetbe véve, hogy $\mathbf{u}_{\underrightarrow{(l)}} = \mathbf{u}_{\underrightarrow{(l \bmod n)}}$ és $f(g \bmod h) = fg \bmod h$.

5.4. Tétel

Legyen $n \in \mathbb{N}^+$ és $n \geq k \in \mathbb{N}^+$. Az $[n,k]_q$-paraméterű C ciklikus kódhoz van $S^{[C]}$-ben olyan egyértelműen meghatározott $n-k$-adfokú g főpolinom, hogy $S^{[C]} = \{ag | a \in \mathbb{F}_q[x] \wedge \delta(a) < k\}$, továbbá $S^{[C]}$ elemeinek ilyen felírása egyértelmű, és $g | x^n - e$. Fordítva, ha az $n-k$-adfokú g főpolinom osztója az $x^n - e$ polinomnak, akkor az $S = \{ag | a \in \mathbb{F}_q[x] \wedge \delta(a) < k\}$ halmaz egy $[n,k]_q$-paraméterű ciklikus kódhoz tartozó kódpolinomhalmaz.

Δ

Bizonyítás:

1. $k \in \mathbb{N}^+$, ezért C legalább egydimenziós, van benne nem nulla vektor és $S^{[C]}$-ben nem nulla polinom, tehát $\emptyset \neq A = \{\deg(f) | 0 \neq f \in S^{[C]}\} \subseteq \mathbb{N}$, így létezik és egyértelmű az A legkisebb eleme. Ha ez t, akkor van $S^{[C]}$-ben olyan p polinom, amelynek a foka t. p főegyütthatója nem nulla, ezért van inverze, és ezzel szorozva p-t, egy t-edfokú g főpolinomot nyerünk. $n > t \in \mathbb{N}$, hiszen a kódszavak n-komponensűek. Legyen $S = \{ag | a \in \mathbb{F}_q[x] \wedge \delta(a) < n - t\}$, belátjuk, hogy $t = n - k$ és $S = S^{[C]}$.

$g \in S^{[C]}$, tehát $\mathbf{g}^{(0)} = \mathbf{g} \in C$. A kód ciklikus, ezért iterációval kapjuk, hogy bármely $i \in \mathbb{N}$-re $\mathbf{g}^{(i)} = \mathbf{g}_{\underrightarrow{(i)}}$ is eleme a kódnak. Fentebb láttuk, hogy $g^{(i)} = g_{\underrightarrow{(i)}} = x^i g \bmod (x^n - e)$. Ha $i < n - t$, akkor $x^i g$ fokszáma alacsonyabb n-nél. Mivel egy n-nél alacsonyabbfokú polinomot egy n-edfokú polinommal osztva a hányados 0, és így a maradék megegyezik az osztandóval, ezért az előbbiek alapján kapjuk, hogy a megadott intervallumba eső i-k esetén $g^{(i)} = x^i g$. Az $\mathbb{F}_q$-beli $a_0, \dots, a_{n-t-1}$ elemekkel $\sum_{i=0}^{n-t-1} a_i \mathbf{g}^{(i)}$ is kódvektor, hiszen a kód lineáris, ezért

$$\sum_{i=0}^{n-t-1} a_i g^{(i)} = \sum_{i=0}^{n-t-1} a_i (x^i g) = \left(\sum_{i=0}^{n-t-1} a_i x^i \right) g = ag$$

is benne van $S^{[C]}$-ben, ahol $a = \sum_{i=0}^{n-t-1} a_i x^i \in \mathbb{F}_q[x]$ és $\delta(a) < n - t$, tehát $S \subseteq S^{[C]}$.

Most legyen $u \in S^{[C]}$. u egyértelműen írható $u = cg + r$ alakban, ahol $\delta(r) < \deg(g) = t$. Mivel u n-nél alacsonyabbfokú, míg r t-nél alacsonyabbfokú, és t kisebb, mint n, ezért $cg = u - r$ is n-nél alacsonyabbfokú polinom, vagyis $\delta(c) < n - t$. Ekkor $cg \in S^{[C]}$, és innen $r = u - cg \in S^{[C]}$, hiszen a kód lineáris, így két kódszó különbsége is kódszó. De az $S^{[C]}$-beli nem nulla polinomok legalább t-edfokúak, így r csak a nullpolinom lehet, tehát $u = cg$ és $u \in S^{[C]}$, azaz $S^{[C]} \subseteq S$. Figyelembe véve az előbb megállapított ellenkező irányú tartalmazást kapjuk, hogy $S = S^{[C]}$.

$g \neq 0$, így $a^{(1)} g = a^{(2)} g \Leftrightarrow a^{(1)} = a^{(2)}$, és ag pontosan akkor kódpolinom, ha $\delta(a) < n - t$, ezért kölcsönösen egyértelmű megfeleltetés létesíthető C és S elemei között. C-nek q^k, míg S-nek q^{n-t} eleme van, a két érték megegyezik, így $k = n - t$, azaz $t = n - k$, tehát g egy $n-k$-adfokú főpolinom.

2. $\mathbf{g}^{(k)} \in C$, tehát $x^k g \bmod (x^n - e) = g^{(k)} \in S^{[C]}$. Mivel g egy $n-k$-adfokú főpolinom, ezért $x^k g = (x^n - e) + r$, ahol $\delta(r) < n$. $r = g^{(k)} \in C$, így r, és akkor $x^n - e = x^k g - r$ is osztható g-vel.

3. Tekintsük az S-beli polinomokat. Ezek mindegyike n-nél alacsonyabbfokú, $\mathbb{F}_q$ feletti polinom, ezért mindegyikük egy-egy $\mathbb{F}_q$ feletti n-dimenzós vektort határoz meg. S-beli polinomok összege és $\mathbb{F}_q$-beli konstansszorosa is S-beli, így a megfelelő vektorok alteret alkotnak $V_q^{(n)}$-ben, és a számosság alapján az altér dimenziója k. Legyen $\sum_{i=0}^{n-1} f_i x^i = f \in S$. Ekkor $xf = f_{n-1} \cdot (x^n - e) + r$, és $\delta(r) < n$. Itt $g|f$, mivel f kódpolinom, továbbá $g|x^n - e$ a g választása folytán igaz, de ekkor $g|r$ is teljesül, és mivel a fokszám is megfelelő, ezért $f_{\rightarrow} = r \in S$, S egy ciklikus kód polinomhalmaza.

□

Ha $m \in \mathbb{N}^+$ kisebb, mint n, és az $[n,k]$-paraméterű ciklikus kódhoz tartozó g polinom osztója az $x^m - e$ polinomnak, akkor $x^m - e$ is kódpolinom. De az $x^m - e$-nek megfelelő kódszóban pontosan két nullától különböző komponens van, így a kód távolsága legfeljebb 2, a kód egyetlen hiba javítására sem alkalmas (pontosabban szólva van olyan egyetlen hiba, amelyet a kód nem képes javítani).

Mivel g osztója $x^n - e$-nek, és mindkét polinom főpolinom, ezért $h = \frac{x^n - e}{g}$ is főpolinom.

5.5. Definíció

Az $[n,k]$ ciklikus kódhoz tartozó, egyértelműen meghatározott g polinom a **kód generátorpolinomja**, és $h = \frac{x^n - e}{g}$ a **kód ellenőrző polinomja**.

Δ

Amint a generátorpolinom ismeretében valamennyi kódszó megkapható egy polinommal való szorzással, az ellenőrzéshez is elegendő az ellenőrző polinommal való szorzás.

5.6. Tétel

Legyen h egy $[n,k]_q$-praméterű C ciklikus kód ellenőrző polinomja. Ekkor $c \in \mathbb{F}_q[x]$ pontosan akkor kódszópolinom, ha $\delta(c) < n$ és $hc \bmod (x^n - e) = 0$.

Δ

Bizonyítás:

$[n,k]$-paraméterű ciklikus kód bármely c kódpolinomjára $\delta(c) < n$, legyen tehát $c \in \mathbb{F}_q[x]$-re $\delta(c) < n$. $hc \bmod (x^n - e) = 0$ akkor és csak akkor, ha $hc = a \cdot (x^n - e) = a(gh) = (ag)h$ egy a polinommal, vagyis pontosan akkor, ha $c = ag$, ahol $\delta(a) < k$, vagyis ha c kódpolinom.

□

Könnyű látni, hogy bármely n természetes számra $[n,0]_q$ és $[n,n]_q$ ciklikus. Az előbbi csak a nullvektort tartalmazza, míg az utóbbi a teljes tér, márpedig a nullvektor bármely lineáris kombinációja és ciklikus eltoltja önmaga, míg a teljes tér nyilván lineáris, és minden vektor eltoltja is eleme ugyanezen térnek. Az előbbi kódot akkor kapjuk, ha $g = x^n - e$, hiszen most ahhoz, hogy ag legfeljebb $n-1$-edfokú legyen, szükséges, hogy a maga a nullpolinom legyen. Ez a nullvektornak felel meg, ami minden lineáris kódnak eleme. Az utóbbi kódot a $g = e$ polinom generálja, és így minden legfeljebb $n-1$-edfokú polinom kódpolinom, ezek halmaza viszont izomorf az n-dimenziós térrel.

5.7. Tétel

Legyen C_1 és C_2 egy $[n, k_1]_q$- illetve $[n, k_2]_q$-paraméterű ciklikus kód rendre a g_1 és g_2 generátorpolinommal. Ekkor

a) $C_1 \subseteq C_2$ akkor és csak akkor, ha $g_2 | g_1$;
b) $C_1 \cap C_2$ ciklikus kód a $g = [g_1, g_2]$ generátorpolinommal;
c) $C = \{u_1 + u_2 | u_1 \in C_1 \wedge u_2 \in C_2\} = C_1 + C_2$ a $g = (g_1, g_2)$ által generált ciklikus kód.

Δ

Bizonyítás:

a) Ha $C_1 \subseteq C_2$, akkor $g_1 \in C_2$, tehát $g_2 | g_1$. Ha viszont $g_2 | g_1$ és $c \in C_1$, akkor $\delta(c) < n$, továbbá $g_2 | g_1 | c$, és így $c \in C_2$, tehát $C_1 \subseteq C_2$.

b) Mind g_1, mind g_2 osztója $x^n - e$-nek, ezért g is osztója $x^n - e$-nek, és főpolinom, vagyis g is egy n hosszúságú C ciklikus kód generátorpolinomja. $c \in C_1 \cap C_2$ akkor és csak akkor, ha $c \in C_1$ és $c \in C_2$, tehát $g_1 | c$ és $g_2 | c$, vagyis ha $g | c$, azaz ha $c \in C$.

c) g nyilván osztója $x^n - e$-nek, tehát g nem 0, és egy n hosszúságú szavakból álló C' ciklikus kódot generál.

Ha $u \in C_1 + C_2$, akkor $u = u_1 + u_2$, ahol $u_1 \in C_1$, és $u_2 \in C_2$. Ekkor $g | g_1 | u_1$ és $g | g_2 | u_2$, így $g | u_1 + u_2$, tehát $u \in C'$, azaz $C \subseteq C'$.

A másik irányhoz legyen $u \in C'$. Ekkor $\delta(u) < n$ és $u = ag$. $g = (g_1, g_2)$, így alkalmas t_1 és t_2 polinommal $g = t_1 g_1 + t_2 g_2$. Ha $u_1 = a t_1 g_1 \bmod (x^n - e)$ és $u_2 = a t_2 g_2 \bmod (x^n - e)$, akkor $g_1 | u_1$, tehát $u_1 \in C_1$, és hasonlóan, $u_2 \in C_2$. $\delta(u) < n$-ből következik $u \bmod (x^n - e) = u$, így

$$u = u \bmod (x^n - e) = ag \bmod (x^n - e) = (a t_1 g_1 + a t_2 g_2) \bmod (x^n - e)$$
$$= (a t_1 g_1 \bmod (x^n - e)) + (a t_2 g_2 \bmod (x^n - e)) = u_1 + u_2,$$

vagyis $u \in C$, tehát $C' \subseteq C$, azaz $C = C'$.

□

5.8. Definíció

Az $\mathbb{F}_q$ fölötti C ciklikus kód **maximális**, ha g és **minimális**, ha h irreducibilis $\mathbb{F}_q$ fölött.

Δ

Ha $n = 1$, akkor csak triviális ciklikus kód létezik. Ellenkező esetben, ha C maximális, akkor g irreducibilis, tehát g nem konstans, továbbá g az $x^n - e$ valódi osztója (hiszen ennek e gyöke, így nem irreducibilis), C tehát nem triviális kód. Legyen $C \subseteq C'$, ekkor $g' | g$, és mivel g irreducibilis, ezért $g' = g$ vagy $g' = e$, azaz $C' = C$ vagy $C' = \mathbb{F}_q^n$. Ez azt jelenti, hogy egy maximális kódot nem tartalmaz egyetlen, tőle különböző, nem triviális ciklikus kód sem. Ha viszont C minimális és $C' \subseteq C$, akkor $\frac{x^n - e}{h} = g \,\big|\, g' = \frac{x^n - e}{h'}$, vagyis $h' | h$, és ebből vagy $h' = e$ vagy $h' = h$, hiszen h felbonthatatlan. A második esetben $C' = C$, míg az elsőben $g = x^n - e$, azaz $C' = \{\mathbf{0}\}$. Most tehát egy minimális kód nem tartalmaz tőle különböző, nem triviális ciklikus kódot.

Ha n és q relatív prímek, akkor egy $\mathbb{F}_q$ fölötti minimális kód mint olyan gyűrű, ahol a szorzást modulo $(x^n - e)$ végezzük, testet alkot. Legyen ugyanis $c_1 = a_1 g$ és $c_2 = a_2 g$ olyan kódszó, amelyek szorzata 0, vagyis $(a_1 a_2) g^2 = (a_1 g)(a_2 g) = c \cdot (x^n - e) = c(gh) = (ch) g$, ekkor $(a_1 a_2) g = ch$. Mivel n és q relatív prímek, így $x^n - e$ gyökei egyszeresek, ami azt jelenti, hogy g és h relatív prímek, hiszen a szorzatuk $x^n - e$, így nem lehet közös gyökük. Ekkor az előbbi szorzatfelírás alapján h osztója $a_1 a_2$-nek, és mivel a feltétel szerint a kód minimális, azaz h felbonthatatlan, és akkor egyben prím is, h osztója a_1 és a_2 közül legalább az egyiknek, mondjuk a_1-nek, $a_1 = uh$. Innen viszont azt kapjuk, hogy $c_1 = a_1 g = (uh) g = u(gh) = u \cdot (x^n - e) = 0$, vagyis a gyűrű a most bevezetett modulo $(x^n - e)$ szorzással nullosztómentes, és mivel a gyűrű véges, tehát test. Másként mondva, $\mathbb{F}_q[x]$-nek az $x^n - e$

szerinti maradékosztálygyűrűjében a h által generált kód mint részgyűrű test. Érthető tehát, hogy a minimális kódot **irreducibilis**nek valamint **felbonthatatlan**nak is mondják.

Legyen g az $x^n - e$ polinom egy főpolinom osztója, és $gh = x^n - e$, ekkor persze h is főpolinom. Ha c a g által generált kód egyik eleme, akkor tehát $c = ag = a\frac{x^n-e}{h}$, és innen $\frac{c}{e-x^n} = \frac{-a}{h}$. Mivel $\delta(c) < n$, ezért az előbbi egyenlőség jobb oldala egy n szerint periodikus formális hatványsor, vagyis c-t előállíthatjuk úgy, hogy a $-a$ polinomot mint formális hatványsort osztjuk a h polinommal mint formális hatványsorral, és vesszük a hányados első *n* elemét.

Egy további generálást kapunk, ha tovább alakítjuk az előző egyenlőség jobb oldalát:

$$S = \sum_{i=0}^{\infty} s_i x^i = \frac{c}{e - x^n} = \frac{-a}{h} = \frac{-h_0^{-1}a}{(h_0^{-1}h^*)^*},$$

ahol $f^* = \sum_{i=0}^{n} f_{n-i}x^i$ az n-edfokú $f = \sum_{i=0}^{n} f_i x^i$ polinom duálisa, és S a korábban már említett periodikus formális hatványsor. A jobb oldali tört számlálója legfeljebb $k-1$-edfokú, ugyanakkor $h_0^{-1}h^*$ egy k-adfokú főpolinom, vagyis $h_0^{-1}h^*$ az S formális hatványsor karakterisztikus polinomja. Ebből következik, hogy tetszőlegesen megadva az $s_0, \dots, s_{k-1}$ elemeket, az $s_{i+k} = \sum_{j=0}^{k-1}\left(-h_0^{-1}h_{k-j}\right)s_{i+j}$ rekurzióval $n - k > i \in \mathbb{N}$-re megkapjuk az $s_k, \dots, s_{n-1}$ elemeket, és így a teljes kódszót.

Eddig a ciklikus kódok generálásának három módját láttuk: ha g az $[n,k]_q$ ciklikus kód generátorpolinomja, $a \in \mathbb{F}_q[x]$ és $\delta(a) < k$, akkor C

- az ag-alakú polinomok halmaza;
- a $\frac{-a}{h}$ alakú formális hatványsorok n-hosszúságú kezdőszeleteinek halmaza;
- a $h_0^{-1}h^*$ karakterisztikus polinom által generált homogén lineáris rekurzív sorozatok n-hosszúságú kezdőszeleteinek halmaza.

5.9. Példa

Legyen $n = 8$, $q = 5$. Az $x^8 - 1 \in \mathbb{Z}_5[x]$ polinom $\mathbb{Z}_5$ fölötti felbontása

$$\begin{aligned} x^8 - 1 &= (x^4 - 1)(x^4 + 1) = (x^2 - 1)(x^2 + 1)(x^4 + 1) = (x - 1)(x + 1)(x^2 - 4)(x^4 - 4) \\ &= (x - 1)(x + 1)(x - 2)(x + 2)(x^2 - 2)(x^2 + 2) \\ &= (x + 1)(x + 2)(x + 3)(x + 4)(x^2 + 2)(x^2 + 3), \end{aligned}$$

és a két utolsó faktor már irreducibilis $\mathbb{Z}_5$ fölött, ugyanis $(\pm 1)^2 = 1$ és $(\pm 2)^2 = 4$. Válasszuk például g-nek az első három faktor szorzatát, akkor g és h az alábbi:

$$g = (x - 2)(x + 2)(x + 1) = (x^2 + 1)(x + 1) = x^3 + x^2 + x + 1$$

$$h = (x - 1)(x^2 - 2)(x^2 + 2) = (x - 1)(x^4 + 1) = x^5 + 4x^4 + x + 4,$$

és g egy $[8,5]_5$-paraméterű ciklikus kódot generál.

Ha most $a = x^2 + 2$, akkor az $a \mapsto ag$ leképezéssel

$$c = (x^2 + 2)(x^3 + x^2 + x + 1) = x^5 + x^4 + 3x^3 + 3x^2 + 2x + 2,$$

azaz $\mathbf{c}^T = 22331100$.

Ugyanezzel az a polinommal, de az $a \mapsto \frac{-a}{h}(1 - x^8)$ szabállyal való kódoláshoz a $-a$ polinomot mint formális hatványsort osztjuk a h polinommal mint formális hatványsorral, és vesszük a hányados hatványsor első nyolc elemét. (Formális hatványsoroknál az osztó legalacsonyabb fokú nem nulla

együtthatós tagjával osztjuk az osztandó legalacsonyabb fokú tagját. Az eredmény csak akkor formális hatványsor, ha ennek a hányadosnak a kitevője nemnegatív, vagyis ha az osztó legkisebb fokú nem nulla tagjának foka legfeljebb akkora, mint az osztandóban a legkisebb fokú nem nulla együtthatós tag foka.)

$$\begin{array}{llllllll}
(3 & +4x^2) : (4 + x + 4x^4 + x^5) = 2 + 2x + 3x^2 + 3x^3 + x^4 + x^5 + 0x^6 + 0x^7 \\
\quad 3x + 4x^2 & + 2x^4 + 3x^5 \\
\qquad 2x^2 & + 2x^4 & + 3x^6 \\
\qquad\quad 2x^3 + 2x^4 & & + x^6 + 2x^7 \\
\qquad\qquad 4x^4 & & + x^6 & + 2x^8 \\
\qquad\qquad\quad 4x^5 + x^6 & & & + 3x^8 + 4x^9 \\
\qquad\qquad\qquad\qquad 3x^8 & & & + 4x^{10}
\end{array}$$

és ismét azt kaptuk, hogy $\mathbf{c}^T = 22331100$ (látjuk, hogy $3x^8 + 4x^{10} = x^8(3 + 4x^2) = x^8(-a)$ a maradék, vagyis innen kezdve az eddigi együtthatók periodikusan ismétlődnek).

Végül nézzük a homogén lineáris rekurzióval való generálást. Most legyen adott az üzenet: $\mathbf{u}^T = 22331$ (a $\mathbf{c}^T$ 5-hosszúságú kezdő szelete). Ekkor $c_0c_1c_2c_3c_4 = 22331$, és a rekurzió

$$\begin{aligned} c_{i+5} &= h_5c_i + h_4c_{i+1} + h_3c_{i+2} + h_2c_{i+3} + h_1c_{i+4} \\ &= c_i + 4c_{i+1} + c_{i+4}, \end{aligned}$$

így

$$\begin{aligned} c_5 &= 2 + 4 \cdot 2 + 1 = 1 \\ c_6 &= 2 + 4 \cdot 3 + 1 = 0 \\ c_7 &= 3 + 4 \cdot 3 + 0 = 0, \end{aligned}$$

vagyis most megint $\mathbf{c}^T = 22331100$.

Az $f = \sum_{i=0}^{n} b_i x^i$ főpolinom által generált $\mathbf{s}$ homogén lineáris rekurzív sorozat $\frac{\tau}{f^*}$-ként is felírható, ha $\tau = \sum_{i=0}^{n-1} t_i x^i$ a $t_i = \sum_{j=0}^{i} b_{n-i+j} s_j$ együtthatókkal. Most $f = h_0^{-1}h^* = x^5 + 4x^4 + x + 4$ és $s^{(0)} = c_0c_1c_2c_3c_4 = 22331$, így

$$\begin{aligned} t_0 &= 1 \cdot 2 && = 2 \\ t_1 &= 4 \cdot 2 + 1 \cdot 2 && = 0 \\ t_2 &= 0 \cdot 2 + 4 \cdot 2 + 1 \cdot 3 && = 1 \\ t_3 &= 0 \cdot 2 + 0 \cdot 2 + 4 \cdot 3 + 1 \cdot 3 && = 0 \\ t_4 &= 1 \cdot 2 + 0 \cdot 2 + 0 \cdot 3 + 4 \cdot 3 + 1 \cdot 1 && = 0, \end{aligned}$$

tehát az osztással történő generáláshoz a számláló $\tau = x^2 + 2$, ami megegyezik $-h_0^{-1}a$-val.

□

Térjünk vissza az $S = \frac{-h_0^{-1}a}{\left(h_0^{-1}h^*\right)^*}$ alakhoz. Legyen a C kód $[n,k]_q$-paraméterű és $n = q^r - 1$ egy pozitív egész r-rel. Mivel h osztója $x^n - e$-nek, ezért a 0 nem gyöke h-nak, így h akkor és csak akkor irreducibilis $\mathbb{F}_q$ fölött, ha h^* felbonthatatlan a megadott test fölött. Tegyük fel, hogy h egy r-edfokú primitív polinom $\mathbb{F}_q$ fölött (vagyis a gyöke primitív elem $\mathbb{F}_{q^r}$-ben). Ekkor $h_0^{-1}h^*$ is egy r-edfokú primitív polinom $\mathbb{F}_q$ fölött, és (ha $a \neq 0$) S egy $\mathbb{F}_q$ fölötti maximális periódusú sorozat, vagyis a minimális periódusa $q^r - 1 = n$. Maximális periódusú sorozat minimálpolinomja által generált minden nem nulla sorozat egyetlen ilyen sorozat eltoltja, és valamennyi ilyen sorozat egyetlen minimális periódusú szakaszának súlya azonos, nevezetesen $(q-1)q^{r-1}$. Ez viszont azt jelenti, hogy ha az $[n,k]_q$-paraméterű kódban, ahol $n = q^r - 1$, az ellenőrző polinom egy r-edfokú, $\mathbb{F}_q$ fölötti primitív polinom, akkor a megfelelő kód minden nem $\mathbf{0}$ kódszavának súlya $(q-1)q^{r-1}$, vagyis bármely két kódszó távolsága azonos,

és megegyezik a kód minimális távolságával. (Mivel primitív polinom irreducibilis, tehát legalább elsőfokú, és k azonos h fokával, ezért k nem 0, a kód legalább két szót tartalmaz, a kódnak van minimális távolsága.) Az ilyen kódokat definiálja a következő

5.10. Definíció

A C kód **egyenlő távolságú**, **ekvidisztáns** vagy **szimplex**, ha bármely két különböző kódszó távolsága d.

Δ

Legyen $n = 8 = 3^2 - 1$, ekkor a $\mathbb{Z}_3$ fölötti $x^8 - 1$ polinom $\mathbb{Z}_3$ fölött irreducibilis polinomokra való felbontása $x^8 - 1 = (x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$. Mivel $h = x^2 + x + 2$ irreducibilis, ezért a rendje csak 2, 4 vagy 8 lehet. De h nem osztója sem $x^2 - 1$-nek, sem $x^4 - 1$-nek, így h primitív polinom $\mathbb{Z}_3$ fölött. Ha h egy $[8, k]_3$-paraméterű C ciklikus kód ellenőrző polinomja, akkor $k = \deg(h) = 2$, és a C generátorpolinomja $g = \frac{x^8-1}{x^2+x+2} = x^6 + 2x^5 + 2x^4 + 2x^2 + x + 1$. A kód tartalmazza a nullvektort, valamint a g-nek megfelelő 11202210 vektort, és mivel C ciklikus, ezért az utóbbi vektor valamennyi eltoltját, azaz a kód elemei többek között a

00000000 20221011 21011202
11202210 02210112 10112022
12022101 22101120 01120221

szavak. Ha az utólsó szót ismét elléptetjük egy hellyel ciklikusan balra, akkor a kiinduló nem **0** kódszót kapjuk. De $M = q^k = 3^2 = 9$, és a fentiekben éppen kilenc, páronként különböző kódszót soroltunk fel, vagyis a teljes kódot megadtuk. A megkonstruált kód bármely nem nulla kódszava tehát egyetlen kódszó ciklikus eltoltja, így minden nem nulla kódszó súlya azonos, a kód egyenlő távolságú.

Egy ciklikus kód nem feltétlenül lineáris, ám a gyakorlatban szinte mindig az. Ekkor a kódhoz megadható a generátor- és ellenőrző mátrix. Legyen az $[n, k]$-paraméterű ciklikus kód generátor- és ellenőrző polinomja g és h. Tekintsük azt a $k \times n$-méretű $\mathbf{G}$ mátrixot, amelynek i-edik sora az $x^i g$ polinom által meghatározott $\mathbf{g}^{(i)^T} = \underbrace{0 \dots 0}_{i} g_0 \dots g_{n-k} \underbrace{0 \dots 0}_{k-1-i}$ sorvektor, míg $\mathbf{H}$ egy $(n-k) \times n$-méretű mátrix, amelynek i-edik sora $\mathbf{h}^{(i)^T} = \underbrace{0 \dots 0}_{i} (h_0^{-1}h_k) \dots (h_0^{-1}h_0) \underbrace{0 \dots 0}_{n-k-1-i}$, azaz az $x^i h_0^{-1} h^*$ polinomhoz tartozó kódszó (a h_0^{-1}-gyel való szorzás biztosítja, hogy $h_0^{-1}h^*$ főpolinom legyen).

5.11. Tétel

Legyen $g = \sum_{i=0}^{n-k} g_i x^i$ és $h = \sum_{i=0}^{k} h_i x^i$ egy C ciklikus kód generátor- és ellenőrző polinomja. Ha $n > j \in \mathbb{N}$ mellett a $k > i \in \mathbb{N}$ indexekre $G_{i,j} = g_{j-i}$ és $n - k > i \in \mathbb{N}$-re $H_{i,j} = h_0^{-1} h_{k-j+i}$, ahol $l > n - k$ és $l < 0$ esetén $g_l = 0$, $l < 0$ és $l > k$ esetén $h_l = 0$, akkor a $\mathbf{G}$ és a $\mathbf{H}$ mátrix a kód generátor- és ellenőrző mátrixa.

Δ

Bizonyítás:

Mivel $gh = x^n - e$, ezért $g_0 h_0 = -e \neq 0$, és ekkor $g_0 \neq 0 \neq h_0$. Az rögtön látható, hogy $\mathbf{G}$ i-edik sora az $x^i g$-hez tartozó sorvektor, míg $\mathbf{H}$-ban az i-edik sor az $x^i(h_0^{-1}h^*)$ polinom által meghatározott n-méretű sorvektor. A $\mathbf{G}$ első k oszlopából álló kvadratikus mátrix főátlójában $g_0 \neq 0$ áll, míg a főátló alatt mindenütt 0 van, tehát ez a kvadratikus részmátrix reguláris, a rangja k, és ekkor ez a rangja a teljes mátrixnak is, hiszen a mátrix sorainak száma k. Hasonlóan kapjuk, hogy $\mathbf{H}$ rangja $n - k$. Az $\mathbf{u}^T = u_0 \dots u_{k-1}$ üzenettel

$$\mathbf{u}^T\mathbf{G} = \sum_{i=0}^{k-1} u_i \mathbf{g}^{(i)^T} = \sum_{i=0}^{k-1} u_i x^i g = \left(\sum_{i=0}^{k-1} u_i x^i\right) g = ug,$$

ahol u egy legfeljebb $k-1$-edfokú polinom, tehát $\mathbf{u}^T\mathbf{G} \in C$, $\mathbf{G}$ generálja a kódot. Most belátjuk, hogy $\mathbf{H}\mathbf{G}^T = \mathbf{0}$. Ehhez azt kell megmutatni, hogy $\mathbf{G}$ és $\mathbf{H}$ bármely két sora merőleges, vagyis hogy bármely $n-k > r \in \mathbb{N}$ és $k > s \in \mathbb{N}$ esetén $\sum_{j=0}^{n-1} H_{r,j}G_{s,j} = 0$, illetve $h_0 \sum_{j=0}^{n-1} H_{r,j}G_{s,j} = 0$, hiszen $h_0 \neq 0$.

$$h_0 \sum_{j=0}^{n-1} H_{r,j}G_{s,j} = h_0 \sum_{j=0}^{n-1} h_0^{-1} h_{k+r-j} g_{j-s} = \sum_{j=s}^{k+r} h_{k+r-j} g_{j-s}$$
$$= \sum_{j=0}^{k-s+r} h_{k-s+r-j} g_j = (gh)_{k-s+r} = (x^n - e)_{k-s+r}.$$

Az r-re és s-re adott határokkal $1 \leq k-s+r \leq n-1$, és $x^n - e$-ben az ezen indexekhez tartozó együtthatók mindegyike 0, így $\sum_{j=0}^{n-1} H_{r,j}G_{s,j} = 0$, tehát $\mathbf{H}\mathbf{G}^T = \mathbf{0}$, $\mathbf{H}$ a kód ellenőrző mátrixa.

□

Nézzük az 5.9. példa generátorpolinomja által generált kód generátor- és ellenőrző mátrixát:

$$\mathbf{G} = \begin{pmatrix} 1&1&1&1&0&0&0&0 \\ 0&1&1&1&1&0&0&0 \\ 0&0&1&1&1&1&0&0 \\ 0&0&0&1&1&1&1&0 \\ 0&0&0&0&1&1&1&1 \end{pmatrix} \quad \mathbf{H} = \begin{pmatrix} 4&1&0&0&4&1&0&0 \\ 0&4&1&0&0&4&1&0 \\ 0&0&4&1&0&0&4&1 \end{pmatrix}.$$

Mint tudjuk, k-dimenziós lineáris kód generátormátrixában van k lineárisan független oszlop. Ha a kód ciklikus, akkor ennél több is igaz.

5.12. Tétel

Ha egy $[n,k]$-paraméterű ciklikus kód generátormátrixának $0 \leq i_0 < \cdots < i_{t-1} < n$ indexű oszlopai, ahol $k \geq t \in \mathbb{N}$, lineárisan függetlenek, akkor tetszőleges l egész számmal az $(i_j - l) \bmod n$ indexű oszlopok is lineárisan függetlenek, ahol $t > j \in \mathbb{N}$.

Δ

Bizonyítás:

Mivel az i_j oszlopindexek páronként különbözőek, ezért az $(i_j - l) \bmod n$ indexek is ilyenek, és nyilván mindegyik n-nél kisebb nemnegatív egész szám, tehát a mátrix különböző oszlopainak indexei. Generátormátrix sorai a kód elemei. Ha a kód ciklikus, akkor ezeket a sorokat ciklikusan elléptetve ismét kódszavakat kapunk, és ha az eredeti sorok lineárisan függetlenek voltak, akkor minden sort ugyananynyival elléptetve, a kapott vektorok is lineárisan függetlenek lesznek, vagyis ismét generátormátrixot kapunk. Az új mátrix oszlopai közül pontosan azok lineárisan függetlenek, amelyek az eredeti helyükön is lineárisan függetlenek voltak, így valóban igaz az állítás.

□

Ha ismerjük egy lineáris kód $\mathbf{G}$ generátor- és $\mathbf{H}$ ellenőrző mátrixát, akkor meg tudjuk adni a duális kód valamely $\mathbf{G}^D$ generátor- és $\mathbf{H}^D$ ellenőrző mátrixát, hiszen például $\mathbf{G}^D = \mathbf{H}$ és $\mathbf{H}^D = \boldsymbol{G}$ egy alkalmas választás. Ebből látható, hogy a duális kód generátorpolinomja $g^{(D)} = h_0^{-1}h^*$, hiszen a ciklikus kód generátormátrixában a generátorpolinom szerepel, elől a konstans taggal, míg $\mathbf{H}$-ban az ellenőrző polinom, de balról a legmagasabb fokú taggal. A h_0^{-1}-gyel való szorzás azért kell, mert a generátorpolinom

főpolinom. Mivel $(gh)^* = g^*h^*$, és $g_0h_0 = (gh)_0 = -e$, ezért a duális kód ellenőrző polinomja $h^{(D)} = g_0^{-1}g^*$. Ha az eredeti kód n hosszúságú, akkor $h_0^{-1}h^*$ is osztója $x^n - e$-nek, így

5.13. Tétel

Ciklikus kód duálisa is ciklikus kód.

Δ

Gyakran a h által generált kódot tekintik a g-hez tartozó ciklikus kód duálisának. Ez nem azonos az előbbivel, de skalárekvivalens vele. Nyilván mindkettő azonos paraméterű kódot generál (mert h konstans tagja nem zérus, így h és h^* foka azonos). A h által generált kód egy lehetséges generátormátrixában az i-edik sor az x^ih polinomhoz tartozó vektor, vagyis az i-edik sor j-edik eleme h_{j-i}, míg a definíció szerinti duális kódban az $x^i(h_0^{-1}h^*)$ polinomból az előbb megadott pozíción álló elem $h_0^{-1}h_{k+i-j}$. Összehasonlítva a két mátrixot látjuk, hogy az előbbi oszlopait h_0^{-1}-gyel szorozva, majd az $i \mapsto n-k-1-i$ és $j \mapsto n-1-j$ megfeleltetéssel az elsőként említett generátormátrix a másodikba megy át, ám ezek az átalakítások egy bázistranszformációt és oszlopok permutálását jelentik.

Másként nézve, ha a duális kódot a $g^{(D)} = h_0^{-1}h^*$ polinom generálja, akkor a kódpolinomok halmaza $C^{(D)} = \{ag^{(D)} | a \in \mathbb{F}_q[x] \wedge \delta(a) < n-k\}$, és $h^{(D)} = \frac{x^n-e}{g^{(D)}} = \frac{x^n-e}{h_0^{-1}h^*} = -h_0g^* = g_0^{-1}g^*$, míg a másik esetben, vagyis ha $\tilde{g}^{(D)} = h$, akkor $\tilde{C}^{(D)} = \{a\tilde{g}^{(D)} | a \in \mathbb{F}_q[x] \wedge \delta(a) < n-k\}$ és $\tilde{h}^{(D)} = g$. Tetszőleges f polinomra és $t \in \mathbb{N}$-re $f \mapsto \tilde{f} = x^t(f \circ x^{-1})$ involúció, ugyanis

$$\begin{aligned} x^t\left(\tilde{f} \circ x^{-1}\right) &= x^t\left(\left(x^t(f \circ x^{-1})\right) \circ x^{-1}\right) = x^t\left((x^t \circ x^{-1})\left((f \circ x^{-1}) \circ x^{-1}\right)\right) \\ &= x^t\left(x^{-t}\left(f \circ (x^{-1} \circ x^{-1})\right)\right) = x^t\left(x^{-t}(f \circ x)\right) = (x^tx^{-t})f = f, \end{aligned}$$

és a legfeljebb t-edfokú polinomok halmazának önmagába való bijekciója, mert ebben az esetben $\tilde{f}$ ugyanazon gyűrű fölötti legfeljebb t-edfokú polinom. Most legyen $c = ag^{(D)}$, $\tilde{a} = x^{n-k-1}(a \circ x^{-1})$ és $\tilde{c} = h_0x^{n-1}(c \circ x^{-1})$. Ekkor

$$\begin{aligned} \tilde{c} &= h_0x^{n-1}(c \circ x^{-1}) = h_0x^{n-1}\left(\left(ag^{(D)}\right) \circ x^{-1}\right) \\ &= \left(x^{n-k-1}(a \circ x^{-1})\right)\left(h_0x^k\left(g^{(D)} \circ x^{-1}\right)\right) \\ &= \tilde{a}\left(h_0x^k(h_0^{-1}h^* \circ x^{-1})\right) = \tilde{a}(h^*)^* = \tilde{a}h = \tilde{a}\tilde{g}^{(D)}, \end{aligned}$$

vagyis a $c \mapsto \tilde{c} = h_0x^{n-1}(c \circ x^{-1})$ és a $\tilde{c} \mapsto c = (-g_0)x^{n-1}(\tilde{c} \circ x^{-1})$ pár biztosítja az átjárást az egyik generátumból a másikba, illetve vissza (ez utóbbira megadott kifejezés az előbbihez teljesen hasonlóan igazolható). Az is könnyen látható, hogy a leképezése felel meg a mátrixok esetén az i, míg a c leképezése a j index megfeleltetésének a két generálás esetén.

A ciklikus kódra adott generátormátrix általában nem standard alakú, azonban az $u \mapsto ug$ helyett más megfeletetést alkalmazva a kód szisztematikussá tehető. Legyen az $[n,k]_q$-paraméterű ciklikus kódban $u \mapsto v = x^{n-k}u - \left(x^{n-k}u \bmod g\right)$. Mivel $(a \bmod b) \bmod b = a \bmod b$, ezért az előbbi v-re $v \bmod g = 0$, vagyis g osztója v-nek, v tehát kódpolinom. Az így generált kód szisztematikus az utolsó k pozíciójára, mert $x^{n-k}u$-ban az $n-k$-nál alcsonyabbfokú tagok együtthatója 0, és a maradék legfeljebb $n-k-1$-edfokú, azaz v-ben az $n-k$-nál nem kisebb fokszámú tagok együtthatói egybeesnek u ugyanolyan sorrendben álló együtthatóival. Az előbbiek alapján, ha $r = x^{n-k}u \bmod g$, akkor az $\mathbf{u}$ üzenethez tartozó kódszó $\mathbf{v}^T = -\mathbf{r}^T|\mathbf{u}^T$. Ekkor generátormátrixot kapunk, ha az x^i-khez tartozó $-\mathbf{r}^{(i)^T}\left|\mathbf{e}^{(i)^T}\right.$ kódszavakat mint sorvektorokat tartalmazó mátrixot tekintjük, ahol $\mathbf{e}^{(i)}$ a k-dimenziós tér

i-edik egységvektora, és $\mathbf{r}^{(i)}$ az x^{n-k+i} g-vel való osztásakor keletkező maradékának, $\mathbf{r}^{(i)}$-nek megfelelő vektor, vagyis $\mathbf{G}^{(sz)} = (-\mathbf{P}^T\ \mathbf{I}_k)$, ahol $\mathbf{P}$ i-edik oszlopa $\mathbf{r}^{(i)}$ (az sz jelölés a szisztematikus generálásra utal). Ebből az is következik, hogy az így generált kód ellenőrző mátrixa $\mathbf{H} = (\mathbf{I}_{n-k}\ \mathbf{P})$.

Most nézzük meg, hogy milyen generátormátrixot kapunk, ha a homogén lineáris rekurzióval generáljuk a kódot. Ekkor $\mathbf{G}^{(hlr)}$ sorai lehetnek a $\underbrace{0\ \dots\ 0}_{i}\ e\ \underbrace{0\ \dots\ 0}_{k-1-i}$ üzenetekhez tartozó kódszavak, és ebben az esetben a kód generátormátrixa $\mathbf{G}^{(hlr)} = (\mathbf{I}_k\ \mathbf{T})$, vagyis ez is standard alakú, és a generált kód szisztematikus. Most vegyük tekintetbe, hogy a kód ciklikus. Ekkor nyilván a generátormátrix oszlopainak ciklikus eltolásával ismét a kód egy generátormátrixát kapjuk, tehát $\mathbf{G}' = (\mathbf{T}\ \mathbf{I}_k)$ is ugyanezt a kódot generálja. Ez viszont csak úgy lehet, ha $\mathbf{P} = -\mathbf{P}^T$, amit a következőképpen láthatunk be. Mivel $\mathbf{G}'$ generátormátrix, ezért sorainak lineáris kombinációjával megkapjuk például $\mathbf{G}^{(sz)}$ i-edik sorát. Ekkor ez a lineáris kombináció az egységmátrix hasonló együtthatós lineáris kombinációjaként éppen az egységmátrix i-edik sorát adja, ami csak úgy lehet, ha a lineáris kombinációban minden együttható 0 az i-edik kivételével, amely e, vagyis a két mátrix i-edik sora, és így a teljes mátrix is, megegyezik.

A lineáris kódok előnye az általános, strukturálatlan kódokkal szemben, hogy könnyebb a generálás, másrészt a szindróma segítségével könnyebb a hibajavítás is. A ciklikus kódok erősebb struktúrával rendelkeznek, mint általában egy lineáris kód, és ez megmutatkozott például abban is, hogy míg a lineáris kód generálásához egy egész mátrix kell, addig a ciklikus kódot teljes egészében meghatározza a generátorpolinomja (persze ha ismerjük a kód hosszát is). Most belátjuk, hogy a hibajavítás szempontjából is tömörebben tudjuk megadni a ciklikus kódot, mint egy általános lineáris kód esetén.

Tekintsük a g által generált $[n,k]_q$-paraméterű C ciklikus kódot, és legyen S az $\mathbb{F}_q$ fölötti, n-nél alacsonyabbfokú polinomok halmaza (beleértve a nullpolinomot is). $v \in S$ pontosan akkor eleme a kódnak, ha g osztója v-nek, vagyis ha $v \bmod g = 0$. Tetszőleges $v \in S$-re legyen $s = v \bmod g$. s a g-vel való osztás maradéka, ezért $\delta(s) < \deg(g) = n - k$, és $\deg(v) < n - k$ esetén $s = v \bmod g$, vagyis minden, legfeljebb $n - k - 1$-edfokú polinom fellép maradékként, így a különböző maradékok száma q^{n-k}. Az S $v^{(1)}$ és $v^{(2)}$ elemére a $v^{(1)} \bmod g = s^{(1)} = s^{(2)} = v^{(2)} \bmod g$ egyenlőség pontosan akkor teljesül, amikor $\left(v^{(2)} - v^{(1)}\right) \bmod g = \left(v^{(2)} \bmod g\right) - \left(v^{(1)} \bmod g\right) = s^{(2)} - s^{(1)} = 0$, vagyis ha $\mathbf{v}^{(2)} - \mathbf{v}^{(1)} \in C$, azaz akkor és csak akkor, ha a két polinomhoz tartozó vektor szindrómája azonos. Ez azt jelenti, hogy kölcsönösen egyértelmű megfeleltetés adható az $\mathbb{F}_q$ fölötti n-dimenziós tér C szerinti szindrómái, valamint a megfelelő polinomok g-vel való osztási maradékai között, így ez a maradék ugyanúgy alkalmazható hibajavításra, mint a lineáris kódok esetén a szindróma.

Egészen szoros a kapcsolat egy vektor szindrómája és az előbbi osztási maradék között, ha a kódolást az $u \mapsto x^{n-k}u - \left(x^{n-k}u \bmod g\right)$ szabállyal végezzük. Ekkor a $v = \sum_{i=0}^{n-1} v_i x^i$ polinomhoz tartozó v vektor szindrómája

$$\mathbf{s} = \mathbf{H}\mathbf{v} = (\mathbf{I}_{n-k}\ \mathbf{P})\mathbf{v} = (\mathbf{I}_{n-k}\ \mathbf{P})\begin{pmatrix}\mathbf{v}^{(p)}\\ \mathbf{v}^{(a)}\end{pmatrix} = \mathbf{v}^{(p)} + \mathbf{P}\mathbf{v}^{(a)} = \sum_{i=0}^{n-k-1} v_i\mathbf{e}^{(i)} + \sum_{i=n-k}^{n-1} v_i\mathbf{r}^{(i-(n-k))},$$

és ennek a vektornak az

$$\begin{aligned} s &= \sum_{i=0}^{n-k-1} v_i x^i + \sum_{i=n-k}^{n-1} v_i\left(x^{n-k+(i-(n-k))} \bmod g\right) \\ &= \sum_{i=0}^{n-1} v_i\left(x^i \bmod g\right) = \sum_{i=0}^{n-1} v_i x^i \bmod g = v \bmod g \end{aligned}$$

polinom felel meg. Az átalakításnál kihasználtuk, hogy $\sum_{i=0}^{n-k-1} v_i x^i$ maradéka a g-vel való osztáskor önmaga. Azt látjuk tehát, hogy ebben az esetben a korábban említett bijektív megfeleltetés során egy szindrómát az általa reprezentált polinomnak feleltetünk meg.

Ciklikus kódban egy vektor eltoltjának szindrómáját az eredeti vektor szindrómájából is meghatározhatjuk. Legyen s a v és $s^{\rightarrow}$ a $v_{\rightarrow}$ szindrómája. Ekkor

$$\begin{aligned} s^{\rightarrow} &= v_{\rightarrow} \bmod g = (xv \bmod (x^n - e)) \bmod g \\ &= x(v \bmod g) \bmod g = xs \bmod g = xs - s_{n-k-1} g, \end{aligned}$$

ahol s_{n-k-1} az s polinom $n-k-1$-edfokú tagjának együtthatója.

Most a ciklikus kódok más tulajdonságait vizsgáljuk. Az $[n,k]_q$-paraméterű C ciklikus kód a kód g generátorpolinomjának legfeljebb $n-1$-edfokú többszöröseiből áll, így egy legfeljebb $n-1$-edfokú $c \in \mathbb{F}_q[x]$ polinom pontosan akkor kódszó, ha osztható g-vel. Ebből kapjuk a következő tételt.

5.14. Tétel

Az $\mathbb{F}_q$ fölötti legfeljebb $n-1$-edfokú c polinom pontosan akkor eleme a g polinom által generált $[n,k]_q$-paraméterű C ciklikus kódnak, ha a g egy t-szeres gyöke legalább t-szeres gyöke c-nek.

Δ

Bizonyítás:

Legyen α a g t-szeres gyöke. Ha $c \in C$, akkor $(x-\alpha)^t | g | c$, és így α legalább t-szeres gyöke c-nek. Fordítva, ha $\alpha_0, \dots, \alpha_{l-1}$ a g páronként különböző gyökei a $t_0, \dots, t_{l-1}$ multiplicitásokkal, és minden $l > i \in \mathbb{N}$-re α_i a c legalább t_i-szeres gyöke, akkor minden i-re $(x-\alpha_i)^{t_i}$ osztója c-nek, és így ezek legkisebb közös többszöröse is osztja c-t. De az α_i-k páronként különbözőek, így az $x-\alpha_i$ gyöktényezők, de akkor ezek bármely pozitív egész kitevős hatványa is páronként relatív prím, és így az $(x-\alpha_i)^{t_i}$ polinomok legkisebb közös többszöröse ezek szorzata, vagyis g, tehát g osztója c-nek.

□

Az $x^n - e$ polinom gyökei n-edik egységgyökök. A továbbiakban feltesszük hogy az $[n,k]_q$-paraméterű kódban n és q relatív prím. Ekkor $x^n - e$ gyökei egyszeresek, létezik primitív n-edik egységgyök, és a polinom gyökei egy primitív n-edik egységgyök páronként különböző, $n > i \in \mathbb{N}$ kitevős hatványai.

Ha $x^n - e$ gyökei egyszeresek, akkor minden osztójának, tehát g-nek a gyökei is egyszeresek, és az előbbi tétel úgy módosul, hogy c akkor és csak akkor kódpolinom, ha g minden gyöke gyöke c-nek. Ennél kevesebb is elég. Legyen $g = \prod_{i=0}^{t-1} m_i$ a g $\mathbb{F}_q$ fölötti irreducibilis felbontása. Ha α_j gyöke m_i-nek, akkor m_i lényegében véve (egy esetleges nem nulla konstans szorzótól eltekintve) α_j $\mathbb{F}_q$ fölötti minimálpolinomja, így m_i akkor és csak akkor osztója c-nek, ha α_j gyöke c-nek, és nyilván c akkor és csak akkor kódpolinom, ha valamennyi m_i-vel osztható. Ebből azt kapjuk, hogy c akkor és csak akkor kódpolinom, ha valamennyi m_i legalább egy gyöke gyöke c-nek. Mindez azt jelenti, hogy az $\mathbb{F}_q$ fölötti, n hosszúságú kódszavakat tartalmazó ciklikus kód megadható mint a legbővebb halmaz, amelynek bizonyos elemek a gyökei. Ha az előírt gyökök $\alpha_0, \dots, \alpha_{l-1}$, ahol l nemnegatív egész, és az α_i-k páronként különböző, $\mathbb{F}_q$ fölötti n-edik egységgyökök, továbbá $m_{\alpha_i}^{(\mathbb{F}_q)}$ az α_i $\mathbb{F}_q$ fölötti minimálpolinomja, akkor ezen polinomok legkisebb közös többszöröse a legalacsonyabb fokú olyan polinom, amelynek a megadott egységgyökök mindegyike gyöke, és ha ez a polinom g, akkor tehát a g által generált kód a legbővebb, amelynek minden megadott α_i gyöke.

Legyen a g által generált $[n,k]_q$-paraméterű ciklikus kód C, $\alpha_0, \dots, \alpha_{l-1}$ a g gyökeinek olyan halmaza, amely a g valamennyi, $\mathbb{F}_q$ fölött irreducibilis tényezőjének legalább egy gyökét tartalmazza, és S az $\mathbb{F}_q$ fölötti, n-nél alacsonyabbfokú polinomok halmaza. Ekkor az előbbiek szerint az S-beli c

pontosan akkor eleme a kódnak, ha valamennyi megadott α_i gyöke a polinomnak. Ha $c = \sum_{i=0}^{n-1} c_i x^i$, akkor tehát c akkor és csak akkor eleme S-nek, ha minden $l > i \in \mathbb{N}$ -re $0 = \hat{c}(\alpha_i) = \sum_{j=0}^{n-1} c_j \alpha_i^j$. Most legyen $\widetilde{\mathbf{H}}$ egy $l \times n$-méretű mátrix, amelyben az $l > i \in \mathbb{N}$ és $n > j \in \mathbb{N}$ indexekre $\widetilde{H}_{i,j} = \alpha_i^j$. Ekkor $\left(\widetilde{\mathbf{H}}\mathbf{v}\right)_i = \sum_{j=0}^{n-1} \widetilde{H}_{i,j} v_j = \sum_{j=0}^{n-1} \alpha_i^j v_j = \hat{v}(\alpha_i)$, vagyis $\mathbf{v}$ akkor és csak akkor kódszó, ha $\widetilde{\mathbf{H}}\boldsymbol{v} = \mathbf{0}$. $\widetilde{\mathbf{H}}$ rangja l. Ehhez elég megmutatni, hogy a sorai lineárisan függetlenek. Mivel az α_i-k páronként különböző n-edik egységgyökök, ezért $l \leq n$. Tekintsük az első l oszlopból álló részmátrix determinánsát. Ez a páronként különböző α_i-k által generált Vandermonde-determináns, így az értéke nem 0, ami mutatja, hogy ez a részmátrix reguláris, vagyis a sorai lineárisan függetlenek. Ebből viszont következik, hogy $\widetilde{\mathbf{H}}$ sorai is lineárisan függetlenek.

A megadott $\widetilde{\mathbf{H}}$ azonban általában nem a kód ellenőrző mátrixa, ugyanis α_i általában nem eleme $\mathbb{F}_q$-nak, és így $\widetilde{\mathbf{H}}$ nem egy $\mathbb{F}_q$ test fölötti mátrix. Legyen $\mathbb{F}_{q^r}$ az $\mathbb{F}_q$ legszűkebb olyan bővítése, amely tartalmazza a kód megadott gyökeit, és legyen $\left\{\beta^{(i)} \middle| r > i \in \mathbb{N}\right\}$ az $\mathbb{F}_{q^r}$ egy $\mathbb{F}_q$ fölötti bázisa. $\mathbb{F}_{q^r}$ valamennyi eleme egyértelműen felírható a $\beta^{(i)}$-k $\mathbb{F}_q$-beli együtthatós lineáris kombinációjaként, így kölcsönösen egyértelmű megfeleltetés adható $\mathbb{F}_{q^r}$ elemei, valamint az $\mathbb{F}_q^r$ elemei között, és az is igaz, hogy ez a megfeleltetés művelettartóan képezi le $\mathbb{F}_{q^r}$-t mint $\mathbb{F}_q$ fölötti lineáris teret az $\mathbb{F}_q$ fölötti $\mathbb{F}_q^r$ lineáris térre. Helyettesítsük most $\widetilde{\mathbf{H}}$ elemeit a megfelelő $\mathbb{F}_q^r$-beli elemmel, tehát egy r-komponensű oszlopvektorral. Ekkor egy $\mathbb{F}_q$ fölötti $lr \times n$-méretű $\mathbf{H}'$ mátrixot kapunk. Ennek a mátrixnak a sorai azonban nem feltétlenül lineárisan függetlenek. Legyen $\mathbf{H}$ az előbbi mátrix sorainak egy maximális lineárisan független rendszeréből álló mátrix. Az nyilván igaz, hogy egy $\mathbf{v} \in \mathbb{F}_q^n$-re $\widetilde{\mathbf{H}}\mathbf{v} = \mathbf{0}$ akkor és csak akkor, ha $\mathbf{H}'\mathbf{v} = \mathbf{0}$, és ha $\mathbf{H}'\mathbf{v} = \mathbf{0}$, akkor $\mathbf{H}\mathbf{v} = \mathbf{0}$. De $\mathbf{H}'$ minden sora a $\mathbf{H}$ sorainak lineáris kombinációja, így ha $\mathbf{H}\mathbf{v} = \mathbf{0}$, akkor $\mathbf{H}'\mathbf{v} = \mathbf{0}$ is teljesül, és végeredményben $\widetilde{\mathbf{H}}\mathbf{v} = \mathbf{0}$ pontosan akkor igaz, ha $\mathbf{H}\mathbf{v} = \mathbf{0}$, így $\mathbf{H}$ a kód ellenőrző mátrixa.

Mivel $\widetilde{\mathbf{H}}$ sorai lineárisan függetlenek $\mathbb{F}_{q^r}$, de ekkor $\mathbb{F}_q$ fölött is, ezért van $\widetilde{\mathbf{H}}$-ban l $\mathbb{F}_q$ fölött lineárisan független oszlop. Az ezeknek megfelelő $\mathbf{H}'$-beli oszlopok is lineárisan függetlenek $\mathbb{F}_q$ fölött, és így $\mathbf{H}'$-ben van l $\mathbb{F}_q$ fölött lineárisan független sor. Ekkor $\mathbf{H}$ sorainak száma legalább l, ugyanakkor legfeljebb lr, hiszen ennyi sora volt $\mathbf{H}'$-nek, azaz ha a kód $[n, k]$-paraméterű, vagyis $\mathbf{H}$ sorainak száma, azaz $\mathbf{H}$ rangja $n - k$, akkor $l \leq n - k \leq lr$, és innen $n - lr \leq k \leq n - l$.

Az előbbi eredmények alapján tegyük fel, hogy α a q-elemű test fölötti n-edik primitív egységgyök, és az $[n, k]_q$-paraméterű kódnak – esetleg többek között – $\alpha^{\tau+i}$-k páronként különböző gyökei, ahol $\tau \in \mathbb{Z}$, $2 \leq \delta \in \mathbb{N}$, és $\delta - 1 > i \in \mathbb{N}$. Azt nyilván feltehetjük, hogy $k > 0$, mert különben a kód csupán a nullvektorból állna, és így $\delta \leq n$ (hiszen csak n különböző n-edik egységgyök van, és ha $\delta > n$, akkor valamennyi n-edik egységgyök gyöke a kódnak, tehát minden kódszónak legalább n gyöke van, ami csak úgy lehet, ha egyedül a nullpolinom eleme a kódnak, mert minden más kódpolinom legfeljebb $n - 1$-edfokú, azaz legfeljebb $n - 1$ gyöke van), továbbá $0 \leq \tau < n$. Legyen a kód előbbi gyökeire $\alpha_i = \alpha^{\tau+i}$. Ekkor $\widetilde{H}_{i,j} = \left(\alpha^{\tau+i}\right)^j = \left(\alpha^{j\tau}\right)\left(\alpha^j\right)^i$ a $\delta - 1 > i \in \mathbb{N}$ és $n > j \in \mathbb{N}$ indexekre. Tekintsük a $\widetilde{\mathbf{H}}$ első $\delta - 1$ sorából és a $0 \leq j_0 < \cdots < j_{\delta-2} < n$ indexű oszlopokból álló $\delta - 1$-edrendű $\mathbf{M}^{(j_0,\ldots,j_{\delta-2})}$ részmátrix determinánsát. Ebben a determinánsban a t-edik oszlopban mindegyik elem tartalmazza szorzóként a 0-tól különböző $\alpha^{j_t\tau}$-t. Ha ezt az elemet kiemeljük az oszlopból, akkor a t-edik oszlop i-edik sorában $\left(\alpha^{j_t}\right)^i$ áll, vagyis ha minden oszlopból kiemeltük az adott oszlophoz tartozó közös tényezőt, akkor a visszamaradt determináns egy csupa különböző elemmel generált Vandermonde-determináns, tehát különbözik nullától. Ez azt jelenti, hogy $\widetilde{\mathbf{H}}$ bármely legfeljebb $\delta - 1$ oszlopa lenárisan független, de akkor ez igaz $\mathbf{H}$-ra is, és így a kód távolsága legalább δ. Bebizonyítottuk tehát a következőt.

5.15. Tétel

Legyen C egy $[n, k, d]_q$-paraméterű ciklikus kód, ahol $k > 0$, α egy $\mathbb{F}_q$ fölötti primitív n-edik egységgyök, $\tau \in \mathbb{Z}$, $2 \leq \delta \in \mathbb{N}$, és $\delta - 1 > i \in \mathbb{N}$-re $\alpha^{\tau+i}$ a C gyöke. Ekkor $d \geq \delta$, ha $\delta \leq n$.

Δ

A tétel alapján annak az $\mathbb{F}_q$ fölötti legbővebb, n-hosszúságú kódszavakból álló, legalább egydimenziós C ciklikus kódnak a távolsága, amelynek az n-edik primitív egységgyök $\delta - 1$ egymás utáni hatványa a gyöke, legalább δ. Az így konstruált kód az $\mathbb{F}_q$ **fölötti** $(n, \tau, \delta)_q$**-paraméterű BCH**-kód, ahol τ az első gyök kitevője. (A BCH-kód elnevezés a három megalkotójának nevéből ered: **B***ose* és *Ray*-**C***haudhuri* 1960-ban, **H***ocquenghem* 1959-ben foglalkozott ezzel a kódkonstrukcióval).

A BCH-kód olyan kód tervezésére ad lehetőséget, amelynek minimális távolsága egy előre adott értéknél nem kisebb, márpedig a javítható hibák száma a távolsággal van összefüggésben.

A kód gyökeivel kapcsolatban még egy dolgot említünk. Legyen $g|x^n - e$, de $\hat{g}(e) \neq 0$. e gyöke az $x^n - e$ polinomnak, ezért még $g^{(1)} = (x - e)g$ is osztója $x^n - e$ -nek. Ha C a g és $C^{(1)}$ a $g^{(1)}$ által generált ciklikus kód, akkor a nyilvánvaló $g\big|g^{(1)}$ következtében $C^{(1)} \subseteq C$, és egy C-beli $\mathbf{c}$ akkor és csak akkor eleme $C^{(1)}$-nek, ha c-nek gyöke e, azaz ha $0 = \hat{c}(e) = \sum_{i=0}^{n-1} c_i e^i = \sum_{i=0}^{n-1} c_i$. Ez azt jelenti, hogy $C^{(1)}$ paritáselemes maximális részkódja C-nek.

BCH-kódnak például e pontosan akkor gyöke, ha egy $\delta - 1 > i \in \mathbb{N}$-re $(\tau + i) \bmod n = 0$.

A szisztematikus lineáris kódok egy, főként ciklikus kódokra alkalmazható dekódolási eljárása a **hibacsapda-dekódolás**. Ilyen esetben mind a kódszó, mind a vett szó, mind a hibavektor felírható $\mathbf{c}^{(a)^T}\left|\mathbf{c}^{(p)^T}\right.$ alakban, ahol a az adatrészre, p a paritásrészre utal. Ekkor igaz az alábbi

5.16. Tétel

Legyen $\mathbf{G} = (\mathbf{I}_k \; -\mathbf{P}^T)$ az $[n, k, d]$-paraméterű C kód generátormátrixa, $\mathbf{v}$ egy $\frac{d}{2}$-nél kevesebb hibát tartalmazó szó, és $\boldsymbol{\varepsilon}$ a hibavektor. Ekkor $\boldsymbol{\varepsilon}^{(a)} = \mathbf{0}$ akkor és csak akkor, ha $w(\mathbf{s}) < \frac{d}{2}$.

Δ

A tétel szerint, ha a szindróma súlya kisebb, mint a távolság fele, akkor valamennyi hiba a paritásrészben van, vagyis az adatrész hibátlan, és mivel a kód szisztematikus, ezért a kódszó, tehát a vett szó adatrésze maga az eredeti üzenet, így a javítás és dekódolás ebben az esetben annyiból áll, hogy elhagyjuk a vett szó paritásrészét.

Bizonyítás:

Felhasználjuk, hogy $\mathbf{G} = (\mathbf{I}_k \; -\mathbf{P}^T)$, ezért $\mathbf{H} = (\mathbf{P} \; \mathbf{I}_{n-k})$, és így $\mathbf{s} = \mathbf{H}\boldsymbol{\varepsilon} = \mathbf{P}\boldsymbol{\varepsilon}^{(a)} + \boldsymbol{\varepsilon}^{(p)}$, továbbá $\frac{d}{2} > t = w(\boldsymbol{\varepsilon}) = w\left(\boldsymbol{\varepsilon}^{(a)^T}\left|\boldsymbol{\varepsilon}^{(p)^T}\right.\right) = w\big(\boldsymbol{\varepsilon}^{(a)}\big) + w\big(\boldsymbol{\varepsilon}^{(p)}\big)$.

Először legyen $\boldsymbol{\varepsilon}^{(a)} = \mathbf{0}$. Ekkor $\mathbf{s} = \mathbf{P}\boldsymbol{\varepsilon}^{(a)} + \boldsymbol{\varepsilon}^{(p)} = \boldsymbol{\varepsilon}^{(p)}$ és $w\big(\boldsymbol{\varepsilon}^{(a)}\big) = w(\mathbf{0}) = 0$, tehát a szindróma súlya ebben az esetben $w(\mathbf{s}) = w\big(\boldsymbol{\varepsilon}^{(p)}\big) = 0 + w\big(\boldsymbol{\varepsilon}^{(p)}\big) = w\big(\boldsymbol{\varepsilon}^{(a)}\big) + w\big(\boldsymbol{\varepsilon}^{(p)}\big) = w(\boldsymbol{\varepsilon}) < \frac{d}{2}$.

Fordítva tegyük fel, hogy $\boldsymbol{\varepsilon}^{(a)} \neq \mathbf{0}$. Ekkor $\mathbf{c}^T = \boldsymbol{\varepsilon}^{(a)^T}\mathbf{G}$ sem $\mathbf{0}$, így a súlya legalább d. De

$$\mathbf{c}^T = \boldsymbol{\varepsilon}^{(a)^T}\mathbf{G} = \boldsymbol{\varepsilon}^{(a)^T}(\mathbf{I}_k \; -\mathbf{P}^T) = \boldsymbol{\varepsilon}^{(a)^T}\left|\left(-\mathbf{P}\boldsymbol{\varepsilon}^{(p)}\right)^T\right.,$$

és ennek a vektornak a súlya

$$d \leq w(\mathbf{c}) = w\left(\boldsymbol{\varepsilon}^{(a)^T}\left|\left(-\mathbf{P}\boldsymbol{\varepsilon}^{(a)}\right)^T\right.\right) = w\big(\boldsymbol{\varepsilon}^{(a)}\big) + w\big(\mathbf{P}\boldsymbol{\varepsilon}^{(a)}\big).$$

Innen

$$w\left(\mathbf{P}\boldsymbol{\varepsilon}^{(a)}\right) \geq d - w\left(\boldsymbol{\varepsilon}^{(a)}\right) \geq d - \left(w\left(\boldsymbol{\varepsilon}^{(a)}\right) + w\left(\boldsymbol{\varepsilon}^{(p)}\right)\right)$$
$$= d - w(\boldsymbol{\varepsilon}) > d - \frac{d}{2} = \frac{d}{2} > w(\boldsymbol{\varepsilon}) > w\left(\boldsymbol{\varepsilon}^{(p)}\right),$$

amivel a szindróma súlyára ebben az esetben azt kapjuk, hogy

$$w(\mathbf{s}) = w\left(\mathbf{P}\boldsymbol{\varepsilon}^{(a)} + \boldsymbol{\varepsilon}^{(p)}\right) \geq \left|w\left(\mathbf{P}\boldsymbol{\varepsilon}^{(a)}\right) - w\left(\boldsymbol{\varepsilon}^{(p)}\right)\right| = w\left(\mathbf{P}\boldsymbol{\varepsilon}^{(a)}\right) - w\left(\boldsymbol{\varepsilon}^{(p)}\right)$$
$$\geq \left(d - w\left(\boldsymbol{\varepsilon}^{(a)}\right)\right) - w\left(\boldsymbol{\varepsilon}^{(p)}\right) = d - \left(w\left(\boldsymbol{\varepsilon}^{(a)}\right) + w\left(\boldsymbol{\varepsilon}^{(p)}\right)\right)$$
$$= d - w\left(\boldsymbol{\varepsilon}^{(a)^T} \middle| \boldsymbol{\varepsilon}^{(p)^T}\right) = d - w(\boldsymbol{\varepsilon}) > d - \frac{d}{2} = \frac{d}{2},$$

vagyis most $w(\mathbf{s}) > \frac{d}{2}$.

□

Mielőtt továbbmennénk, és az előbbi eredményt ciklikus kódokra alkalmaznánk, vegyük figyelembe, hogy $\mathbf{v}^{(p)} - \mathbf{s} = \mathbf{v}^{(p)} - \left(\mathbf{P}\mathbf{v}^{(a)} + \mathbf{v}^{(p)}\right) = -\mathbf{P}\mathbf{v}^{(a)}$, vagyis ha a szindróma súlya kisebb, mint a kód távolságának a fele (azaz ha minden hiba a vett szó paritásrészében van), akkor

$$\mathbf{u}^T = \mathbf{u}^{(a)^T} \left|\mathbf{u}^{(p)^T} = \mathbf{u}^{(a)^T} \right|-\left(\mathbf{P}\mathbf{u}^{(a)}\right)^T = \mathbf{v}^{(a)^T} \left|-\left(\mathbf{P}\mathbf{v}^{(a)}\right)^T = \mathbf{v}^{(a)^T} \right|\left(\mathbf{v}^{(p)} - \mathbf{s}\right)^T,$$

tehát az eredeti kódszót úgy kapjuk, hogy a vett szó paritásrészéből kivonjuk a szindrómát.

Most tegyük fel, hogy a kód egy standard alakú generárormátrixszal generált ciklikus kód. Ha a szindróma súlya kisebb, mint a távolság fele, akkor az előbbiekben leírt módon járunk el: egyszerűen elhagyjuk a vett szó paritásrészét, és előttünk áll az eredeti üzenet. Ha azonban a szindróma súlya nagyobb a kód távolságának felénél, akkor a vett szó adatrésze is tartalmaz hibát. A vett szó $\mathbf{v} = \mathbf{u} + \boldsymbol{\varepsilon}$, és ebből $\mathbf{v}_{\rightarrow} = \mathbf{u}_{\rightarrow} + \boldsymbol{\varepsilon}_{\rightarrow}$. Mivel a kód ciklikus, ezért $\mathbf{u}_{\rightarrow}$ is kódszó, tehát vizsgálhatjuk $\mathbf{u}_{\rightarrow}$ szindrómáját (a korábbiakból tudjuk, hogy ezt közvetlenül $\mathbf{v}$ szindrómájából is megkapjuk). Ha ennek a súlya ismét nagyobb, mint $\frac{d}{2}$, akkor ezt az eltoltat ciklikusan újra eltolhatjuk, és így tovább. Amennyiben n egymás utáni egylépéses ciklikus jobbraléptetés minden lépésében a szindróma súlya meghaladja $\frac{d}{2}$-t, akkor egyik lépésben sem tudjuk kihasználni a hibacsapda-dekódolás előnyeit, és az n lépés után visszajutunk a kiinduló helyzetbe, így ekkor ezzel a módszerrel nem tudjuk megoldani a dekódolást. Tegyük azonban fel, hogy valamely $n > l \in \mathbb{N}$ -re a $\mathbf{v}_{\overrightarrow{(l)}}$ vektor $\mathbf{s}^{\overrightarrow{(l)}}$ szindrómájának súlya kisebb $\frac{d}{2}$-nél. Ekkor $\mathbf{v}_{\overrightarrow{(l)}}^{(a)^T} \left|\mathbf{v}_{\overrightarrow{(l)}}^{(p)^T} - \mathbf{s}^{\overrightarrow{(l)}^T} = \mathbf{u}_{\overrightarrow{(l)}}^{(a)^T} \right|\mathbf{u}_{\overrightarrow{(l)}}^{(p)^T} = \mathbf{u}_{\overrightarrow{(l)}}{}^T$, és ebből újabb $n - l$ jobbraléptetéssel (vagy l balraléptetéssel) $\mathbf{u}^T$-re jutunk, tehát a hibacsapda-dekódolással megkapjuk az eredeti, hibátlan üzenetet, amelyből elhagyva a paritásrészt, rendelkezésünkre áll a kódolatlan üzenet.

A hibacsapda-dekódolást akkor tudjuk hatékonyan alkalmazni, ha bármilyen $\frac{d}{2}$-nél kevesebb hiba esetén valahány léptetéssel elérhető, hogy valamennyi hiba a szó paritásrészében legyen. Ehhez az szükséges, hogy bármilyen is legyen a hibaminta (természetesen a távolság felénél kevesebb hibahellyel), legyen legalább egy olyan szomszédos hibapár (szomszédosnak tekintve az utolsó és első hibát is), amelyek között legalább k hibátlan pozíció áll, hiszen ekkor eltolhatjuk úgy a vett szót, hogy az előbb említett hibátlan helyek mindegyike a szó adatrészébe essen. Tegyük fel, hogy a vett szóban $\frac{d}{2} > t \in \mathbb{N}^+$ hiba van. Két hiba átlagos távolsága $\frac{n}{t}$, és ha ez nagyobb k-nál, azaz $t < \frac{n}{k}$, akkor van legalább egy olyan szomszédos hibapár, amelynek két hibája között minimum $\left\lceil\frac{n}{t}\right\rceil - 1 \geq k + 1 - 1 = k$ hibátlan hely található. Ha $k < n$ (és hibát javítani csak ilyen esetben lehet), akkor ez a feltétel $t = 1$ esetén minden további nélkül teljesül (hiszen az egy hiba biztosan betolható a paritásrészbe). Most tegyük fel, hogy $t > 1$. Az $\frac{n}{t} > k$ feltételből $t < \frac{n}{k}$, és ez a javításhoz elengedhetetlen $t < \frac{d}{2}$ feltétellel azt adja, hogy

hibacsapda-dekódolással biztosan javítható bármely $\frac{d}{2}$-nél kevesebb hiba, ha $\frac{d}{2} \leq \frac{n}{k} = \frac{1}{\mathcal{R}}$, ahol $\mathcal{R}$ a kódsebesség. Ez azt jelenti, hogy a hibacsapda-dekódolás csak igen kis kódsebesség esetén alkalmazható legalább két hiba javítására, hiszen az ilyen hiba javításához $d \geq 5$, tehát $\mathcal{R} \leq \frac{2}{5} = 0{,}4$.

Végezetül megjegyezzük, hogy a hibacsapda-dekódolás akkor is működik, ha $\mathbf{G}$ nem standard alakú, de van k oszlopa, amely egy esetleges oszloppermutációval k-adrendű egységmátrix.

6. Kódkonstrukció I.

Ebben a részben azt vizsgáljuk, hogy adott kódból vagy kódokból hogyan lehet új kódot konstruálni, és hogyan függnek az új kód paraméterei az eredeti kód(ok) paramétereitől. A teljesség kedvéért megvizsgáljuk a patologikus eseteket is, de természetesen nem ezek a lényegesek. A konstrukciók egy része inkább csak elméleti szempontból, elméleti megfontolásoknál érdekes, más módszerek azonban a gyakorlatban is jelentősek, segítségükkel ugyanis valamilyen jó kódból kiindulva, a konkrét felhasználáshoz jobban igazodó, jó tulajdonságú kódot lehet létrehozni.

Kiterjesztés (extending). A q-elemű S szimbólumhalmaz fölötti $(n, M, d)_q$-paraméterű C kód minden kódszavát jobbról kiegészítjük egy, a q''-elemű S''- halmazból vett új komponenssel. Az új C' kód szimbólumai a q'-méretű $S' = S \cup S''$ halmaz elemei. Ha C' $(n', M', d')_{q'}$-paraméterű, akkor nyilván $n' = n + 1$, a kód mérete nem változik, tehát $M' = M$, és $q \leq q' = q + q'' - \tilde{q} \leq q + q''$, ahol $\tilde{q} = |S \cap S''|$. Most még megnézzük az új kód távolságát.

Ha $M = 1$, akkor sem a régi, sem az új kódnak nincs értelmezve a távolsága. Most legyen a kódnak legalább két eleme. A kód távolsága nyilván nem csökken, ha az eredeti komponenseket kiegészítjük egy újjal, hiszen ha két kódszó valamelyik pozíción eltért, akkor a kiegészítés után is különbözik ezen a pozíción. Az is magától értetődő, hogy a távolság legfeljebb eggyel nőhet, ugyanis $d(\mathbf{u}u_{n+1}, \mathbf{v}v_{n+1}) = d(\mathbf{u}, \mathbf{v}) + d(u_{n+1}, v_{n+1})$, és a jobb oldali második tag, $d(u_{n+1}, v_{n+1})$, 0 vagy 1, attól függően, hogy $u_{n+1} = v_{n+1}$ vagy $u_{n+1} \neq v_{n+1}$, tehát $d \leq d' \leq d + 1$. d akkor és csak akkor nem változik, ha C-ben van olyan d távolságú kódszópár, amelyeket azonos elemmel egészítettünk ki. Összefoglalva

Kiterjesztés(n, M, d, q, q'', $\tilde{q}$; n', M', d', q')
  $n' = n + 1$
  $q' = q + q'' - \tilde{q}$
  $M' = M$
  ha $M > 1$
    ha van olyan $\mathbf{u} \in C$ és $\mathbf{v} \in C$, hogy $d(\boldsymbol{u}, \boldsymbol{v}) = d$ és $u_{n+1} = v_{n+1}$
      $d' = d$
    különben
      $d' = d + 1$
    elágazás vége
  különben
    d' nem létezik
  elágazás vége
Kiterjesztés vége.

Az új komponenst természetesen nem „hasraütés-szerűen” választjuk, hanem egy $f: S^n \to S''$ függvénnyel határozzuk meg, vagyis $u_{n+1} = f(u_1, \dots, u_n)$. Ha most az **u**-t elküldve, a vétel helyére **v** érkezik, akkor ellenőrizzük, hogy teljesül-e a $v_{n+1} = f(v_1, \dots, v_n)$ egyenlőség. Ha nem, akkor biztosan hibás a vett szó, de azt ebből az eredményből nem lehet megállapítani, hogy melyik komponense(i) hibás(ak), és mi a hiba. Természetesen az a szerencsétlen helyzet is előfordulhat, hogy a $v_1, \dots, v_n$ jegyek mindegyike azonos az eredeti szó megfelelő komponensével, vagyis maga az eredeti üzenet hibátlanul érkezett meg, és csupán a kiegészítő ellenőrző jegy sérült.

Amennyiben a kód valamilyen algebrai struktúrára épül, akkor az f függvény speciális alakot ölt. A leggyakoribb ilyen függvények a következőek.

Legyen S additív Abel-csoport, $\emptyset \neq C \subseteq S^n$, $n \geq i \in \mathbb{N}^+$-ra $k_i \in \mathbb{Z}$, c az $S = S''$ egy rögzített eleme, és legyen $u_{n+1} = -\sum_{i=1}^{n} k_i u_i + c$. C' akkor és csak akkor csoportkód, ha bármely két elemének különbsége is kódszó. Mivel a kivonást komponensenként végezzük, és C' minden eleme egy eredeti

kódszó kiegészítésével keletkezett, ezért szükséges, hogy az első n komponensből álló részek különbsége kódszó legyen C-ben, vagyis hogy C csoportkód legyen. Ha viszont C csoportkód, és $\mathbf{u}$, $\mathbf{v}$ C két eleme, amelyek különbsége $\mathbf{w}$, akkor még teljesülnie kell a $w_{n+1} = u_{n+1} - v_{n+1}$ egyenlőségnek. De

$$-\sum_{i=1}^{n} k_i w_i + c = w_{n+1} = u_{n+1} - v_{n+1} = \left(-\sum_{i=1}^{n} k_i u_i + c\right) - \left(-\sum_{i=1}^{n} k_i v_i + c\right)$$
$$= -\sum_{i=1}^{n} k_i (u_i - v_i) = -\sum_{i=1}^{n} k_i w_i$$

akkor és csak akkor teljesül, ha $c = 0$. Mivel minden lineáris kód egyben csoportkód, ezért az eddigiek szükségesek ahhoz is, hogy az új kód lineáris legyen. Ez azonban elégséges is, ugyanis az előbbi feltétellel $aw_{n+1} = a(-\sum_{i=1}^{n} k_i w_i) = -\sum_{i=1}^{n} k_i (aw_i)$.

Lineáris kód és $c = 0$ esetén tehát C' is lineáris, és C' generátor- és ellenőrző mátrixa

$$\mathbf{G}' = (\mathbf{G} \; -\mathbf{G}\mathbf{k}) \quad \mathbf{H}' = \begin{pmatrix} \mathbf{k}^T & e \\ \mathbf{H} & \mathbf{0}^{(n-k)} \end{pmatrix},$$

ahol $\mathbf{G}$ és $\mathbf{H}$ az eredeti kód megfelelő mátrixa, $(\mathbf{k})_i = k_i e$, és $\mathbf{0}^{(n-k)}$ az $n-k$-méretű nullvektor.

Csoportkód ilyen kiterjesztésénél a kód távolsága pontosan akkor nem nő, ha van olyan d-súlyú $\mathbf{u}$ kódszó, amelyre $u_{n+1} = -\sum_{i=1}^{n} k_i u_i = 0$. Most tegyük fel, hogy C csoportkód, valamennyi i indexre és S minden u elemére $k_i u_i = 0$ csak $u = 0$ esetén igaz (ez például biztosan teljesül, ha minden k_i értéke 1), és legyen $d = 1$. Ha $\mathbf{u} \in C$-re $d(\mathbf{u}) = 1$ (ilyen van, mert a kód távolsága a feltevésünk szerint 1), és az egyetlen nem nulla komponense u_l, akkor $u_{n+1} = -\sum_{i=1}^{n} k_i u_i = -k_l u_l \neq 0$, így kiterjesztés után a megfelelő kódszó súlya 2 lesz. Ez minden 1-súlyú kódszóra igaz, és a legalább 2-súlyú kódszavak súlya a kiterjesztésnél biztosan nem csökken, így most a kiterjesztett kód távolsága 2 lesz, vagyis egy 1-súlyú kód kiterjesztésével egy pontosan 1-hiba jelző kódot kapunk. Már a távolságból is látható, hogy ez a kód minimális távolságú dekódolással nem képes javítani a hibát, de ez közvetlenül is belátható. Legyen $\varepsilon \neq 0$ a csoport o-rendű eleme, i, j két különböző index, $d = (k_i, k_j)$, $k^{(i)} = \frac{k_j}{d}$ és $k^{(j)} = \frac{k_i}{d}$, továbbá $\varepsilon_i = k^{(i)}\varepsilon$ és $\varepsilon_j = k^{(j)}\varepsilon$. $0 = \varepsilon_i = k^{(i)}\varepsilon = \frac{k_j}{d}\varepsilon$ akkor és csak akkor, ha $o \left| \frac{k_j}{d} \right.$, ami lehetetlen, hiszen o nem osztója k_j-nek, tehát $\varepsilon_i \neq 0$, és hasonlóan, $\varepsilon_j \neq 0$. Ha az i-edik, és csak az i-edik helyen van egy ε_i hiba, majd a j-edik, és csak a j-edik helyen egy ε_j hiba, akkor $k_i\varepsilon_i = k_i k^{(i)}\varepsilon = k\varepsilon = k_j k^{(j)}\varepsilon = k_j\varepsilon_j$, ahol k a k_i és k_j legkisebb közös többszöröse, és így nem tudhatjuk, hogy melyik pozícióban lépett fel a hiba, tehát nem is tudunk javítani.

A kódkiterjesztésnél k_i általában 1, és egyik leggyakoribb alkalmazása a bináris kódok **paritásbit**tel való kiegészítése. Ez azt jelenti, hogy ha az eredeti kódszóban az 1-ek száma páros, akkor a kódszót egy 1-gyel, ellenkező esetben egy 0-val egészítik ki, tehát a kiterjesztett kód minden kódszavában az 1-esek száma páratlan. Ez a **páratlanra való kiegészítés**, és ekkor valamennyi kódszó, és így a kód súlya is, páratlan. Hasonlóan működik a **párosra való kiegészítés**, csupán most akkor fűzünk 1-et a kódszóhoz, ha az eredeti kódszó páratlan sok 1-est tartalmazott, és ebben az esetben a nem nulla kódszavak, és ha van nem nulla kódszó, akkor a kód súlya is, páros. Az előbbit használják a számítógépek operatív memóriájánál: mielőtt a gép kiírna a memóriába egy bájtot, páratlanra egészíti ki, és az így kapott kilencbites kódszó kerül a memóriába, kiolvasáskor pedig a gép ellenőrzi, hogy a kiolvasott bájtban valóban páratlan-e az 1-esek száma. Ha igen, akkor rendben van, ellenkező esetben hibajelzés jön létre, amely például egy megszakítást generálhat. Párosra való kiegészítést használnak viszont általában az aszinkron adatátvitelnél.

A paritásbit kiszámítása $u_{n+1} = \bigoplus_{i=1}^{n} u_i \oplus c$ szerint történik, ahol $c = 0$ vagy $c = 1$, és az előbbiek alapján a kód akkor és csak akkor lineáris, ha az eredeti kód lineáris és $c = 0$ (bináris esetben egy kód pontosan akkor lineáris, ha csoportkód, így a két esetet nem kell megkülönböztetni).

Ha egy bináris kód d távolsága páratlan, akkor a kiterjesztett kód távolsága eggyel nagyobb. Legyen ugyanis **u** és **v** két eredeti kódszó, akkor a fentebbi képlet alapján

$$u_{n+1} \oplus v_{n+1} = (\oplus_{i=1}^{n} u_i \oplus c) \oplus (\oplus_{i=1}^{n} v_i \oplus c) = \oplus_{i=1}^{n} (u_i \oplus v_i)$$
$$= \sum_{i=1}^{n} (u_i \oplus v_i) \bmod 2 = w(\mathbf{u} - \mathbf{v}) \bmod 2 = d(\mathbf{u}, \mathbf{v}) \bmod 2,$$

és ha $d(\mathbf{u}, \mathbf{v}) = d$, akkor $d(\mathbf{u}, \mathbf{v}) \bmod 2 = d \bmod 2 = 1$, a két paritásbit különböző, így a kiterjesztett kódban a két kódszó $d + 1$ helyen tér el egymástól. Ebből következően, ha létezik $(n, M, 2t + 1)_2$-paraméterű kód, akkor van $(n + 1, M, 2t + 2)_2$-paraméterű kód is.

Azt már láttuk, hogy a kiterjesztett kód (feltéve, hogy $k_i u$ csak $u = 0$ esetén 0) egy hibát mindig képes jelezni. Bináris esetben ennél többet tud a kód, ugyanis minden olyan esetben jelez, amikor a hibák száma páratlan. Ekkor ugyanis

$$w(\mathbf{u} + \boldsymbol{\varepsilon}) = \sum_{i=1}^{n+1} (u_i \oplus \varepsilon_i) = \sum_{i=1}^{n+1} (u_i + \varepsilon_i - 2u_i\varepsilon_i) = \sum_{i=1}^{n+1} u_i + \sum_{i=1}^{n+1} \varepsilon_i - 2\sum_{i=1}^{n+1} u_i\varepsilon_i$$
$$= w(\mathbf{u}) + w(\boldsymbol{\varepsilon}) - 2\sum_{i=1}^{n+1} u_i\varepsilon_i \equiv w(\mathbf{u}) + 1\ (2),$$

és mivel korábban láttuk, hogy egy paritásbittel kiterjesztett bináris kódban minden kódszó súlya azonos paritású, és a hibás vektor súlyának paritása ezzel ellentétes, ezért észrevesszük a hibát. Ugyanakkor az előbbi levezetésből látható, hogy ha a hibák száma páros, akkor $w(\mathbf{u} + \boldsymbol{\varepsilon}) \equiv w(\mathbf{u})\ (2)$, tehát a hibát nem vesszük észre, a hiba nem jelezhető. Összefoglalva tehát, egy bináris kódot egy paritásbittel kiterjesztve, a kiterjesztett kód minden páratlan hibát jelez, de egyetlen páros hibát sem jelez (általában csak annyit tudtunk megállapítani, hogy bármely 1-hibát jelez a rendszer, és van olyan kettős hiba, ami nem jelezhető, hiszen a kód távolsága 2).

Ha $\mathcal{S}$ gyűrű, és $S = S''$, akkor a kiegészítő jegy számítása például $u_{n+1} = \sum_{i=1}^{n} a_i u_i + c$ lehet, ahol $\mathbf{a} \in S^n$ és $c \in S$ rögzített elemek. Ennek speciális esete az $u_{n+1} = -\sum_{i=1}^{n} u_i + c$ szabály. Megint az a helyzet, hogy a kiterjesztett kód pontosan akkor csoportkód illetve lineáris kód, ha az eredeti kód hasonló tulajdonságú és $c = 0$. Ekkor a kiterjesztett kód generátor- és ellenőrző mátrixa

$$\mathbf{G}' = (\mathbf{G} \; -\mathbf{G}\mathbf{a}) \quad \mathbf{H}' = \begin{pmatrix} \mathbf{a}^T & e \\ \mathbf{H} & \mathbf{0}^{(n-k)} \end{pmatrix}$$

ahol $\mathbf{a}^T = (a_1, \ldots, a_n)$.

Ha $\mathcal{S}$ euklideszi gyűrű, és a maradék egyértelmű (ez nem kikötés az euklideszi gyűrű definíciójában, és van is olyan euklideszi gyűrű és euklideszi norma, amelyben ez nem igaz, például a Gauss-egészek gyűrűje az abszolút értékkel mint normával), akkor legyen $u_{n+1} = (\sum_{i=1}^{n} a_i u_i + c) \bmod s$, ahol s is a gyűrű rögzített eleme. Ez nem csoportkód még akkor sem, ha az eredeti kód az volt, és a konstans értéke 0, ugyanis az összeg maradéka általában nem azonos a maradékok összegével (legfeljebb a maradékok összegének maradékával). Erre a kódra egy példa a személyi szám. Ez egy olyan 11-jegyű decimális egész szám, ahol $u_{11} = \sum_{i=1}^{10} i u_i \bmod 11$. Ez a maradék 10 is lehet, amit a 10-es számrendszerben nem tudunk ábrázolni, ezért az olyan tízjegyű számokat, amelyeknél a maradék 10, nem használják. (A személyi szám ellenőrző jegy előtti utolsó három számjegye csupán arra szolgál, hogy megkülönböztesse azokat, akiknek egyébként az első hét jegyből álló azonosítója megegyezik. Ha egy adott kiegészítéssel a maradék 10, akkor az előbbi háromjegyű számot eggyel növelve a súlyozott összeg vagy $10 \cdot 1$=10-zel nő, vagy ha az utolsó számjegy 9 volt, akkor $9 \cdot 10 - 1 \cdot 9 = 81$-gyel vagy $9 \cdot 10 + 9 \cdot 9 - 1 \cdot 8 = 163$-mal csökken, attól függően, hogy a kilencedik jegy milyen volt. Mivel a változtatás

előtt az ellenőrző összeg 11-gyel osztva 10-et adott maradékul, és a változtatás egyik esetben sem osztható 11-gyel, így az új szám biztosan nem 10-et ad maradékul a 11-gyel való osztáskor.)

Átszúrás (puncturing). Ez a kiterjesztés megfordítása: minden kódszóból elhagyjuk egy előre megadott, rögzített pozíción álló komponensét. Ha az eredeti kód szóhosszúsága 1, akkor az új kód üres. Ellenkező esetben az a kérdés, hogy van-e a kódban két olyan kódszó, amelyek csak a kijelölt pozíción különböznek, ekkor ugyanis átszúrás után ez a két kódszó azonos lesz, csökken a kód mérete, míg ha nincs ilyen kódszópár, akkor a kód mérete nem változik. Nézzük az új kód távolságát. Ha eredetileg csak egy kódszó volt, vagy az eredeti kód valamennyi kódszava csak a most elhagyott pozíción különbözött, akkor sem a régi, sem az új kódnak nincs távolsága. Ha csökken a kód mérete, és az új kód legalább kételemű, akkor az új kód távolsága bármilyen, n-nél kisebb pozitív egész szám lehet. Minden más esetben az átszúrt kód távolsága vagy megegyezik az eredeti kód távolságával, vagy eggyel kisebb nála, hiszen ha két kódszó valahány helyen eltért egymástól, akkor elhagyva egy pozíciót, az eltérő helyek száma biztosan nem nő, és legfeljebb eggyel kevesebb, mint volt. Összefoglalva:

Átszúrás(l; n, M, d; n', M', d')
  ha $n = 1$
    $C' = \emptyset$
  különben
    $n' = n - 1$
    ha $M = 1$
      $M' = 1$
    különben ha van olyan kódszópár, amely csak az l-edik pozíción különbözik
      ha mindegyik kódszópár csak az l-edik pozíción különbözik
        $M' = 1$
      különben
        $1 < M' < M$
        $1 \leq d' < n$
      elágazás vége
    különben
      $M' = M$
      ha van olyan d-távolságú kódszópár, amely az l-edik pozíción különbözik
        $d' = d - 1$
      különben
        $d' = d$
      elágazás vége
    elágazás vége
  elágazás vége
Átszúrás vége.

Könnyen belátható, hogy ha az eredeti kód csoportkód vagy lineáris kód, akkor az új kód is ilyen, feltéve, hogy az új kód nem üres. Nyilván érdektelen az az eset is, amikor C-nek egyetlen eleme van, amely csoportkódban (és így a lineáris kódban is) csak a nullelem lehet.

Most nézzük a lineáris kódokat. Az előzőek alapján feltehetjük, hogy $n > 1$. Ha C-nek legalább két eleme van, akkor a kód legalább egydimenziós. Legyen az eredeti kód generátor- és ellenőrző mátrixa $\mathbf{G}$ és $\mathbf{H}$, és az l-edik pozíció átszúrásával kapott kód megfelelő két mátrixa $\mathbf{G}^{(l)}$ és $\mathbf{H}^{(l)}$, továbbá az $\mathbf{u}$ átszúrásával előálló vektor $\mathbf{u}^{(l)}$. Ha $\mathbf{v} \in C'$, akkor $\mathbf{v} = \mathbf{u}^{(l)}$, ahol $\mathbf{u} = \sum_{i=1}^{k} \lambda_i \mathbf{g}_i \in C$ valamilyen λ_i együtthatókkal, és minden $n \geq j \in \mathbb{N}^+$-ra $u_j = \sum_{i=1}^{k} \lambda_i g_{i,j}$. Innen $\mathbf{u}^{(l)} = \sum_{i=1}^{k} \lambda_i \mathbf{g}_i^{(l)}$, vagyis $\mathbf{G}$ l-edik oszlopát elhagyva, a kapott mátrix sorai generálják az átszúrt kódot. Fordítva, ha $\mathbf{v}' = \sum_{i=1}^{k} \lambda_i' \mathbf{g}_i^{(l)}$, és $\mathbf{u}' = \sum_{i=1}^{k} \lambda_i' \mathbf{g}_i$, akkor $\mathbf{v}' = \mathbf{u}'^{(l)}$, az előbbi mátrix sorainak generátuma része C'-nek, és így az átszúrt mátrix sorai az átszúrt kód egy generátorrendszerének elemei.

Most tegyük fel, hogy esetleg $\mathbf{g}_1$ kivételével $\mathbf{G}$ valamennyi sorában az l-edik pozíción 0 áll. Ilyen generátormátrix mindig létezik. Ekkor tetszőleges μ_i együtthatókkal $\sum_{i=2}^{k} \mu_i \mathbf{g}_i^{(l)}$ pontosan akkor a nullvektor, amikor $\sum_{i=2}^{k} \mu_i \mathbf{g}_i$ a nullvektor, így az átszúrt generátormátrix sorai, az elsőt elhagyva, biztosan lineárisan függetlenek. Ha tehát az átszúrt mátrix sorai lenárisan összefüggőek, akkor ebben a mátrixban az első sor lineárisan függ a többi sortól, l kivételével minden j-re $g_{1,j} = \sum_{i=2}^{k} \mu_i g_{i,j}$. Az eredeti mátrix sorai lineárisan függetlenek, ami az előbbi egyenlőségek esetén csak úgy lehet, ha $g_{1,l} \neq \sum_{i=2}^{k} \mu_i g_{i,l} = 0$. Ekkor $\mathbf{g}_1 - \sum_{i=2}^{k} \mu_i \mathbf{g}_i = g_{1,l}\mathbf{e}_l$, tehát az l-edik egységvektor eleme a kódnak. Fordítva, tegyük fel, hogy ez a vektor kódszó. Ekkor van olyan generátormátrix, amelyben ez a vektor az első sor, és az összes többi sorban az l-edik pozíción 0 áll. Ha most elhagyjuk a mátrix l-edik oszlopát, akkor az első sor a nullvektor, amely nyilván lineárisan függ a többi sortól (mert már önmagában is lineárisan összefüggő), és a mátrix többi sora lineárisan független. Ha tehát $\mathbf{G}$ olyan, amelyben az l-edik oszlopban legfeljebb az első sorban áll 0-tól különböző elem, és ha a kódnak az l-edik egységvektor eleme, akkor az első sor ez az egységvektor (vagy valamely nem nulla konstansszorosa), akkor az l-edik pozíción átszúrt kód $\mathbf{G}^{(l)}$ generátormátrixát úgy kapjuk $\mathbf{G}$-ből, hogy elhagyjuk az l-edik oszlopot, és ha az első sorban csak az l-indexű elem különbözik nullától, akkor még elhagyjuk az első sort is. Ez utóbi esetben a kód dimenziója eggyel (és a mérete a q-adára) csökken, míg az ellenkező esetben a kód dimenziója (tehát a mérete is) változatlan.

Nézzük, hogyan változik átszúráskor a lineáris kód ellenőrző mátrixa. Ismét csak az az eset érdekes, amikor a komponensek száma legalább 2, és ha a kód a teljes tér egy nem triviális altere, vagyis ha $n > k \in \mathbb{N}$. $\mathbf{H}$ esetén is feltehetjük, hogy az l-edik oszlopban legfeljebb csak az első sorban van nullától különböző elem. Ha egy $\mathbf{h}$ vektorban az l-indexű komponens 0, akkor bármely $\mathbf{u}$ vektorral $(\boldsymbol{h}, \boldsymbol{u}) = \left(\boldsymbol{h}^{(l)}, \boldsymbol{u}^{(l)}\right)$, így $\mathbf{H}$-ban az első sort nem számítva, az l-edik pozíción átszúrt mátrix többi sora ortogonális az átszúrással kapott kód valamennyi vektorára, és ezek a sorok lineárisan függetlenek is, így ezek a sorok az átszúrt kód valamely ellenőrző mátrixának sorai lehetnek. Ha most az első sorban is 0 van az átszúrás helyén, akkor az átszúrt mátrix valamennyi sora lineárisan független, és az első sor is ortogonális az átszúrt kód minden elemére, így $\mathbf{H}^{(l)}$ a $\mathbf{H}$ átszúrásával kapott mátrix. Ez most tehát az az eset, amikor $\mathbf{H}$ l-edik oszlopa a nullvektor. Ekkor $\mathbf{H}$ minden sora merőleges az $\mathbf{e}_l$ egységvektorra, vagyis $\mathbf{e}_l$ eleme az eredeti kódnak. Fordítva, ha ez a vektor benne van C-ben, akkor a kód ellenőrző mátrixában az l-edik oszlop minden eleme 0, mert ha nem így lenne, és valamelyik sorban az l-indexű elem $v \neq 0$, akkor ennek a sornak és $\mathbf{e}_l$-nek a skalárszorzata $v \neq 0$ lenne. Mint már tudjuk, C dimenziója akkor és csak akkor csökken az l-edik pozíción való átszúráskor, ha $\mathbf{e}_l$ eleme a kódnak, és ebben és csak ebben az esetben $\mathbf{H}$ l-edik oszlopában csak 0 áll, továbbá ekkor $\mathbf{H}$-t átszúrva megkapjuk $\mathbf{H}^{(l)}$-t. Ha viszont $\mathbf{e}_l$ nem eleme a kódnak, akkor nem csökken a kód dimenziója, viszont eggyel csökken a hossza, a teljes tér dimenziója. Mivel C és $C^{\perp}$ dimenziójának összege a teljes tér dimenziójával egyenlő, ezért, ha átszúrásnál C dimenziója nem csökken, akkor csökkennie kell $C^{\perp}$ dimenziójának, és ezzel együtt az ellenőrző mátrix sorai számának. Mivel láttuk, hogy $\mathbf{H}$ átszúrtjában az első sort elhagyva, a kapott mátrix sorai lineárisan függetlenek, és valamennyien merőlegesek az átszúrt kód mindenegyes vektorára, ez a mátrix lesz az átszúrt kód ellenőrző mátrixa, $\mathbf{H}^{(l)}$. Az előbbiekben tehát igazoltuk az alábbi tételt.

6.1. Tétel

Legyen $n \geq 1$, az $[n, k]$-paraméterű C generátormátrixa $\mathbf{G} = \begin{pmatrix} \mathbf{g}_1^{(b)^T} & g_{1,l} & \mathbf{g}_1^{(j)^T} \\ \mathbf{G}^{(b)} & \mathbf{0}^{(k-1)} & \mathbf{G}^{(j)} \end{pmatrix}$ és ellenőrző mátrixa $\mathbf{H} = \begin{pmatrix} \mathbf{h}_1^{(b)^T} & h_{1,l} & \mathbf{h}_1^{(j)^T} \\ \mathbf{H}^{(b)} & \mathbf{0}^{(n-1-k)} & \mathbf{H}^{(j)} \end{pmatrix}$, és legyen $n \geq l \in \mathbb{N}^+$. Ekkor

1. $g_{1,l} = 0$ akkor és csak akkor, ha $\mathbf{e}_l \in C^{\perp}$, és így van olyan $\mathbf{H}$, amelyben az első sorban $h_{1,l} = e$, és minden más elem 0;
2. $h_{1,l} = 0$ pontosan akkor igaz, ha $\mathbf{e}_l \in C$, és ekkor $\mathbf{G}$-t meg lehet úgy választani, amelyben az első sor $\mathbf{e}_l^T$;

3. ha $\mathbf{e}_l \in C$, akkor $\mathbf{G}^{(l)} = (\mathbf{G}^{(b)}\ \mathbf{G}^{(j)})$ és $\mathbf{H}^{(l)} = \begin{pmatrix} \mathbf{h}_1^{(b)^T} & \mathbf{h}_1^{(j)^T} \\ \mathbf{H}^{(b)} & \mathbf{H}^{(j)} \end{pmatrix}$;
4. minden más esetben $\mathbf{G}^{(l)} = \begin{pmatrix} \mathbf{g}_1^{(b)^T} & \mathbf{g}_1^{(j)^T} \\ \mathbf{G}^{(b)} & \mathbf{G}^{(j)} \end{pmatrix}$ és $\mathbf{H}^{(l)} = (\mathbf{H}^{(b)}\ \mathbf{H}^{(j)})$.

Δ

Amennyiben egy bináris kód távolsága legalább 2, és páros, akkor egy olyan helyen átszúrva a kódot, ahol egy minimális távolságú kódszópár eltér, a kód távolsága csökken, tehát azt kaptuk, hogy ha létezik $(n+1, M, 2t+2)_2$ kód, akkor van $(n, M, 2t+1)_2$ kód is. A kiterjesztésnél látott ellenkező irányú megállapításból tehát azt kapjuk, hogy akkor és csak akkor van $(n, M, 2t+1)_2$-paraméterű kód, ha van $(n+1, M, 2t+2)_2$-paraméterű kód. Ezt majd a kódolási korlátoknál felhasználjuk.

Növelés (augmenting). Ennél az eljárásnál a kódhoz új kódszavakat veszünk, amelynek a komponensei esetleg más szimbólumhalmazból lehetnek. Az új szavak hozzávételével a meglévő szavak távolsága nem változik, így a kód minimális távolsága – ha volt – biztosan nem nő, de hogy mennyi lesz, azt általánosságban nem tudjuk megmondani. Azt sem lehet elvileg megmondani, hogy az új kód csoport- vagy lineáris kód lesz-e, ez ugyanis semmi korrelációt nem mutat az eredeti kóddal.

Növelés(n, M, d, q, $\tilde{q}$; n', M', d', q')
$n' = n$
$q \le q' = q + q'' - \tilde{q} \le q + q''$
$M' > M$
d' (ha $M > 1$, akkor $d' \le d$)
Növelés vége.

Legyen C egy $(n, M, d)_2$-paraméterű kód, ekkor **a kód komplementere** $\bar{C} = \{\mathbf{1} + \mathbf{u} | \mathbf{u} \in C\}$, ahol $\mathbf{1}$ a csupa 1-ből álló szó (vagyis a komplementer kód szavait úgy kapjuk, hogy az eredeti kódszóban a 0-t 1-re és az 1-et 0-ra cseréljük). Jelöljük az így kapott kódszót $\bar{\mathbf{u}}$-sal. Ekkor

$$d(\bar{\mathbf{u}}, \bar{\mathbf{v}}) = \sum_{\substack{i=1 \\ (\bar{\mathbf{u}})_i \neq (\bar{\mathbf{v}})_i}}^{n} 1 = \sum_{\substack{i=1 \\ (\mathbf{u})_i \neq (\mathbf{v})_i}}^{n} 1 = d(\mathbf{u}, \mathbf{v}),$$

amiből következik, hogy $\bar{C}$ paraméterei megegyeznek C paramétereivel. Most legyen $C' = C \cup \bar{C}$. A kódszavak hossza nem változott, az alkalmazott szimbólumoké sem, ellenben megváltozhatott a kódszavak száma (nőhetett), valamint a kód távolsága, amely a növelésre megállapított tulajdonságok alapján legfeljebb kisebb lehet, mint az eredeti kódé volt (már ha annak volt távolsága). Határozzuk meg az új kód távolságát. Ha veszünk két kódszót C'-ből, akkor vagy mindkettő az eredeti kódnak az eleme, vagy mindkettő a komplementer kódból van, és ekkor a távolságuk azonos az eredetijük távolságával, így az ilyen kódpárok távolságának minimuma azonos az eredeti kód távolságával, d-vel. Az utolsó eset, hogy mondjuk $\mathbf{u} \in C$ és $\mathbf{v} \in \bar{C}$, de $\mathbf{u} \neq \mathbf{v}$. $\mathbf{v} \in \bar{C}$-ből $\bar{\mathbf{v}} \in C$, míg $\boldsymbol{u} \neq \boldsymbol{v}$ azt jelenti, hogy $\mathbf{0} \neq \mathbf{u} + \mathbf{v} = \mathbf{u} + \bar{\mathbf{v}} + \mathbf{1}$, vagyis $\mathbf{u} + \bar{\mathbf{v}} \neq \mathbf{1}$. A két kódszó távolsága

$$d(\mathbf{u}, \mathbf{v}) = \sum_{\substack{i=1 \\ u_i \neq v_i}}^{n} 1 = \sum_{\substack{i=1 \\ u_i = (\bar{\mathbf{v}})_i}}^{n} 1 = n - \sum_{\substack{i=1 \\ u_i \neq (\bar{\mathbf{v}})_i}}^{n} 1 = n - d(\mathbf{u}, \bar{\mathbf{v}}).$$

Ez az érték biztosan nagyobb, mint 0, ugyanis kikötöttük, hogy a két kódszó különböző, így viszont $d(\mathbf{u}, \bar{\mathbf{v}}) < n$, tehát az ilyen távolságok maximuma is kisebb, mint a kódszavak hossza, n. Ezekből az

eredményekből azt kapjuk, hogy $d' = \min\left\{d, n - \max_{\substack{\mathbf{u}\in C \wedge \mathbf{v}\in C \\ \mathbf{u}\neq\mathbf{v}}}\{d(\mathbf{u},\mathbf{v})\}\right\}$ lesz az újonnan szerkeszett, növelt kód távolsága.

Ha C lineáris, és $C \cap \bar{C} \neq \emptyset$, akkor $C = \bar{C}$. Ha ugyanis $\mathbf{u} \in C \cap \bar{C}$, akkor $\mathbf{u} \in C$ és $\mathbf{u} \in \bar{C}$, az utóbbiból $\bar{\mathbf{u}} \in C$, és a linearitásból $\mathbf{1} = \mathbf{u} + \bar{\mathbf{u}} \in C$, majd ismét a linearitásból tetszőleges $\bar{\mathbf{v}} \in \bar{C}$-re $\bar{\mathbf{v}} = \mathbf{1} + \mathbf{v} \in C$, azaz $\bar{C} \subseteq C$. De ugyanígy kapjuk azt is, hogy $C \subseteq \bar{C}$, tehát valóban igaz, hogy $C = \bar{C}$. A $C \cap \bar{C} \neq \emptyset$ feltétel ekvivalens azzal, hogy $\mathbf{1} \in C$, hiszen a kód lineáris, tehát $\mathbf{0} \in C$, vagyis $\mathbf{1} \in \bar{C}$ mindig igaz. Azt látjuk tehát, hogy egy lineáris bináris kód esetén vagy $\mathbf{1} \in C$, és ekkor $C = \bar{C}$, vagy $C \cap \bar{C} = \emptyset$,. Az első esetben $C \cup \bar{C} = C$, tehát a komplementálással nem változik a kód. A második esetben viszont $M' = 2M$ (vagy, mivel a kód lineáris, ezért $k' = k + 1$), és ekkor a növelt kód távolsága $d' = \min\left\{d, n - \max_{\mathbf{u}\in C}\{w(\mathbf{u})\}\right\}$.

Lineáris kód esetén, amennyiben a kód a teljes tér valódi altere, akkor az előbbi konstrukció általánosításaként eljárhatunk úgy, hogy egy $\mathbf{u} \in \mathbb{F}_q^n \setminus C$ vektorral képezzük a $C' = [C, \mathbf{u}]$ generátumot. Az így kapott kód az eredetinél pontosan eggyel nagyobb dimenziójú kód lesz.

Törlés (expunging, expurgating, throwing away codewords). Ez az előbbi növelés párja: kódszavakat hagyunk el. Szűkebb halmaz minimuma nem kisebb, mint az eredeti halmazé, tehát ha marad a kódban legalább két elem, akkor távolsága nagyobb, vagy egyenlő, mint a kiinduló kód távolsága volt. A csoporttulajdonságról és a linearitásról ismét semmit nem lehet általánosságban mondani

Törlés$(n, M, d; n', M', d')$
  $n' = n$
  $M' < M$
  ha $M' > 1$
    $d' \geq d$
  elágazás vége
Törlés vége.

Egy alkalmazása a konstrukciónak, amikor egy bináris kódban csak a páros súlyú kódszavakat hagyjuk meg. Ha egy bináris kód lineáris, akkor vagy minden kódszó páros súlyú, vagy pontosan a kódszavak fele ilyen tulajdonságú. Legyen ugyanis $\mathbf{u}$ és $\mathbf{v}$ két kódszó. Mivel

$$w(\mathbf{u}+\mathbf{v}) = \sum_{i=1}^{n}(u_i \oplus v_i) = \sum_{i=1}^{n}(u_i + v_i - 2u_iv_i) = \sum_{i=1}^{n}u_i + \sum_{i=1}^{n}v_i - 2\sum_{i=1}^{n}u_iv_i$$
$$= w(\mathbf{u}) + w(\mathbf{v}) - 2\sum_{i=1}^{n}u_iv_i \equiv w(\mathbf{u}) + w(\mathbf{v})\ (2),$$

ezért a páros súlyú kódszavak részcsoportot képeznek (ezek halmaza nem üres, mert a nullvektor súlya páros). Az összefüggésből az is látszik, hogy két kódszó különbsége akkor és csak akkor eleme a részcsoportnak, ha a súlyuk paritása megegyezik, így valamennyi páratlan súlyú kódszó, ha van, azonos mellékosztályban van az előző részcsoport szerint. De egy részcsoport szerinti mellékosztályok számossága azonos, így ha van páratlan súlyú kódszó, akkor pontosan a kódszavak fele ilyen. Ez tehát azt jelenti, hogy ebben az esetben a csökkentéssel a kód mérete a felére, és a dimenziója eggyel csökkent.

Nem feltétlenül bináris, de legalább két vektort tartalmazó lineáris kód esetén egy lehetséges eljárás, hogy a kód egy valódi alterét tartjuk meg.

Rövidítés (shortening). Ez a konstrukció a csökkentés és átszúrás kombinációja. Ha adott a C kód, akkor ebből elhagyunk bizonyos kódszavakat, majd a megmaradt kódszavakat átszúrjuk egy adott pozíción. A kódszavak száma nyilván csökken, a kódhosszúság szintén (ez utóbbi eggyel). Mi a helyzet a távolsággal? A csökkentésnél nem csökken, legfeljebb nő a távolság, míg az átszúrásnál (a speciális esetektől eltekintve) legfeljebb csökken, így két ellentétes hatás érvényesül. Ha a két módosítás között

semmi kapcsolat nincs, akkor nem lehet általánosságban megmondani, hogy hogyan változik a rövidített kód távolsága. De ilyen általánosan nincs is értelme a konstrukciónak, hiszen így ez nem több, mint két, egymástól független eljárás egymás utáni alkalmazása. A gyakorlatban rögzítjük a kódszavak valamely pozícióját, valamint a szimbólumhalmaz egy elemét, majd azokat a kódszavakat tartjuk meg, amelyeknek a megadott pozíción lévő komponense a megadott elemmel azonos, és végül ezen a pozíción átszúrjuk a kódot, vagyis

$$C' = \{(u_1, \dots, u_{l-1}, u_{l+1}, \dots, u_n) | (u_1, \dots, u_{l-1}, c, u_{l+1}, \dots, u_n) \in C\},$$

ahol l a kijelölt pozíció indexe, és c az S adott eleme. Most egyáltalán nem biztos, hogy csökken a kódszavak száma, de az is előfordulhat, hogy az új kód üres lesz (vagy mert az adott pozíción nem szerepel a megadott karakter, vagy mert az eredeti szóhosszúság 1 volt). Ha azonban az új kód legalább két szót tartalmaz, akkor a távolsága legalább akkora, mint a kiinduló kódé volt. Azt már mondtuk, hogy a csökkentés következtében a kód távolsága nem csökkenhet. De az átszúrás sem csökkenti most a kód távolságát, ugyanis a csökkentés után már csak olyan kódszavak maradtak, amelyek az átszúrás helyén megegyeztek, és így két megmaradt kódszó távolsága nem változik, ha ezt a közös szimbólumot elhagyjuk.

Rövidítés(l, c; n, M, d; n', M', d')
  ha $n > 1$ és van olyan kódszó, amelyben az l-edik pozíción c áll
    $n' = n - 1$
    $M' \leq M$
    ha $M' > 1$
      $d' \geq d$
    elágazás vége
  elágazás vége
Rövidítés vége.

A rövidítés egy igen gyakran alkalmazott eljárás, a későbbiek során többször találkozunk vele. Lineáris kódok esetén a rövidített kód akkor és csak akkor lesz lineáris, ha vagy 0-ra rövidítünk, vagy a kód tartalmazza azt az egységvektort, amelynek egyetlen, 0-tól különböző komponense az átszúrás helyén áll. Tegyük ugyanis fel, hogy a rövidítést egy nullától különböző c-re végezzük, és az egyszerűség kedvéért az utolsó pozícióra történik a rövidítés. Ha $\mathbf{u}$ és $\mathbf{v}$ eleme a rövidített kódnak, akkor benne kell, hogy legyen $\mathbf{u} + \mathbf{v}$ is, vagyis az eredeti kódban benne volt $\mathbf{u}c$, $\mathbf{v}c$ és $(\mathbf{u} + \mathbf{v})c$, továbbá a linearitás következtében $\mathbf{u}c + \mathbf{v}c = (\mathbf{u} + \mathbf{v})(2c)$. Ekkor viszont, ismét a linearitás miatt, az eredeti kódnak eleme $(\mathbf{u} + \mathbf{v})(2c) - (\mathbf{u} + \mathbf{v})c = \mathbf{0}c$, és mivel $c \neq 0$, ezért $c^{-1}(\mathbf{0}c) = \mathbf{0}e$ is (vagyis ebben az esetben az eredeti kód távolsága 1).

Amennyiben egy lineáris kódot nem 0-ra rövidítünk, és a rövidített kód is lineáris, akkor az előbbiek szerint a kiinduló kód tartalmazza $\mathbf{e}^{(l)}$-et, ahol l a rövidítés pozíciója. Ebből viszont az következik, hogy bármely olyan $\mathbf{u}$ vektorral együtt, amelyben az elhagyott pozíción c áll, a kódnak eleme $\mathbf{u} - c\mathbf{e}^{(l)}$ is, amely mindenütt megegyezik $\mathbf{u}$-val, kivéve a rövidítés helyét, ahol viszont 0 áll. Mivel ez fordítva is igaz, ezért ez azt jelenti, hogy c-re rövidítve a kódot ugyanazt az eredményt kapjuk, mintha 0-ra rövidítettünk volna, így ha rövidítéssel lineáris kódból lineáris kódot akarunk kapni, akkor elegendő 0-ra rövidíteni.

Nézzük meg, hogy mi lesz a rövidített kód generátor- és ellenőrző mátrixa, feltéve, hogy mind az eredeti, mind az új kód lineáris. Az előbbiek szerint feltehetjük, hogy 0-ra rövidítünk az l-edik pozíción. Két eset lehetséges: vagy mindegyik kódszóban 0 áll ezen a helyen, és akkor a rövidítés egyszerűen csak egy átszúrás, vagy pontosan a kódszavak q-adrésze marad meg (ami ekvivalens azzal, hogy a dimenzió eggyel csökken). Az első esetet már megtárgyaltuk az átszúrásnál, így most a másik esetet nézzük. Mivel az l-edik pozíción nem csak 0 áll, ezért a generátormátrixban van legalább egy olyan sor, amelynek l-edik komponense különbözik 0-tól. Egy ilyen sor megfelelő konstansszorosait levonva a többi sorból, ismét a kód egy generátormátrixát kapjuk, amelyben az előbbi sor kivételével minden más sor l-edik

komponense 0. Mivel generátormátrix sorai lineárisan függetlenek, ezért az átszúrás helyén 0-t tartalmazó sorok is lineárisan függetlenek, és mivel az átszúrás helyén megegyeznek, ezért elhagyva az l-edik komponenst, az átszúrt vektorok is lineárisan függetlenek. Az ezen vektorok által generált tér azonos azzal a térrel, amelyet az átszúrás előtt kapott vektorok generátumából kapunk, az l-edik, mindenütt 0-ból álló pozíció törlése után, így megkaptuk a rövidített kód generátormátrixát. Ezek után az ellenőrző mátrix meghatározása is könnyű. Mivel átszúrás előtt az új generátormátrix valamennyi sorában a rövidítés helyén 0 állt, és ezeket a vektorokat az eredeti kód ellenőrző mátrixának bármely sorával szorozva 0-t kapunk, ezért **H**-ból elhagyva az l-edik oszlopot, az így kapott mátrix tetszőleges sorát a rövidített kód generátormátrixának bármely sorával szorozva szintén 0-t kapunk, ami, figyelembe véve a dimenziókat is, mutatja, hogy ez a mátrix lesz a rövidített kód ellenőrző mátrixa. Mindezt egybevetve az átszúrásnál mondottakkal, igazoltuk az alábbi tételt.

6.2. Tétel

Egy legalább kétdimenziós térben értelmezett C lineáris kód esetén C és $C^{\perp}$ egyikének átszúrása az l-edik pozíción ekvivalens a másik kód l-edik pozíción 0-ra való rövidítésével.

Δ

Hosszabítás (lengthening). Ez az eljárás a rövidítés megfordítása, vagyis egy kiterjesztés és egy növelés egymás utáni végrehajtása, így a tulajdonságai könnyen megadhatóak.

Direkt összeg. Ez a konstrukció két kódból hoz létre egy újat. Legyen C_1 az S_1 szimbólumhalmaz feletti $(n_1, M_1, d_1)_{q_1}$- és C_2 az S_2 feletti $(n_2, M_2, d_2)_{q_2}$-paraméterű kód. C elemei a C_1 és C_2 szavainak egymás mellé írásából állnak elő, vagyis $\mathbf{u}|\mathbf{v}$ alakúak, ahol $\mathbf{u} \in C_1$ és $\mathbf{v} \in C_2$. Ekkor C egy $S = S_1 \cup S_2$ feletti kód, és $\max\{q_1, q_2\} \leq q \leq q_1 + q_2$. A kódszavak hossza nyilván $n = n_1 + n_2$, és a kód mérete $M = M_1 M_2$. $d(\mathbf{u}_1|\mathbf{v}_1, \mathbf{u}_2|\mathbf{v}_2) = d(\mathbf{u}_1, \mathbf{u}_2) + d(\mathbf{v}_1, \mathbf{v}_2)$, továbbá $\mathbf{u}_1|\mathbf{v}_1 = \mathbf{u}_2|\mathbf{v}_2$ akkor és csak akkor teljesül, ha $\mathbf{u}_1 = \mathbf{u}_2$ és $\mathbf{v}_1 = \mathbf{v}_2$, ennélfogva minden olyan esetben, amikor $\mathbf{u}_1|\mathbf{v}_1 \neq \mathbf{u}_2|\mathbf{v}_2$, $d(\mathbf{u}_1|\mathbf{v}_1, \mathbf{u}_2|\mathbf{v}_2) = d(\mathbf{u}_1, \mathbf{u}_2) + d(\mathbf{v}_1, \mathbf{v}_2) \geq \min\{d(\mathbf{u}_1, \mathbf{u}_2), d(\mathbf{v}_1, \mathbf{v}_2)\} \geq \min\{d_1, d_2\}$, így C távolsága nem lehet kisebb, mint d_1 és d_2 minimuma. De nagyobb sem lehet ennél a minimumnál, ugyanis az első kódban van olyan kódszópár, amelynek a távolsága pontosan d_1 és a második kódban olyan pár, amelynek a távolsága d_2, ezért az új kódban is lesz olyan kódszópár, amelynek a távolsága az előbb megadott érték bármelyike, tehát az összetett kód távolsága pontosan a két kód távolságának a minimuma.

Direkt_összeg$(n_1, M_1, d_1, q_1, n_2, M_2, d_2, q_2, \tilde{q}; n, M, d, q)$
  $n = n_1 + n_2$
  $\max\{q_1, q_2\} \leq q = q_1 + q_2 - \tilde{q} \leq q_1 + q_2$
  $M = M_1 M_2$
  ha $\min\{M_1, M_2\} > 1$
    $d = \min\{d_1, d_2\}$
  különben ha $M_1 > 1$
    $d = d_1$
  különben ha $M_2 > 1$
    $d = d_2$
  elágazás vége
Direkt_összeg vége.

Azonos karakterisztikájú test fölött lineáris kódok direkt összege is lineáris, a konstruált kód paraméterei, ha az eredeti két kód $[n_1, k_1]_{q_1}$- illetve $[n_2, k_2]_{q_2}$-paraméterű, $[n_1 + n_2, k_1 + k_2]_{p^{[s_1, s_2]}}$, ahol $q_1 = p^{s_1}$, $q_2 = p^{s_2}$, p a két test közös karakterisztikája, és az indexben a szögletes zárójel a legkisebb közös többszöröst jelöli. A kód generátor- illetve ellenőrző mátrixa

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_1 & \mathbf{0}^{(k_1, n_2)} \\ \mathbf{0}^{(k_2, n_1)} & \mathbf{G}_2 \end{pmatrix} \quad \mathbf{H} = \begin{pmatrix} \mathbf{H}_1 & \mathbf{0}^{(n_1 - k_1, n_2)} \\ \mathbf{0}^{(n_2 - k_2, n_1)} & \mathbf{H}_2 \end{pmatrix}.$$

$\mathbf{u}$, $\mathbf{u}+\mathbf{v}$ konstrukció. Két azonos karakterisztikájú test fölött definiált lineáris kódból képezünk egy új lineáris kódot a kódok direkt összegéhez hasonlóan, azzal az eltéréssel, hogy a kód második részében nem egy C_2-beli kódszó áll, hanem ehhez még hozzáadjuk az első részben álló C_1-beli kódszót. Amennyiben a két kód hossza különböző, akkor a rövidebben a kódszavakat balról megfelelő számú nullával egészítjük ki a kód második részéhez. Az új kód a két kód elemeit tartalmazó legszűkebb test feletti kód, a kódszavak hossza $n = n_1 + \max\{n_1, n_2\}$, és dimenziója a két kód dimenziójának összege lesz. Még meg kell határozni az új kód távolságát. Ha mindkét kód csak a nullvektort tartalmazta, akkor ez igaz az új kódra is, a kódnak nincs távolsága. Ha az első kód nulldimenziós, de a második nem, akkor az új kód kódszavai csak annyiban térnek el a második kód kódszavaitól, hogy mindegyik elején lesz egy n_1 hosszúságú nullstring, így a kód távolsága azonos lesz a második kód távolságával. Amennyiben a helyzet fordított, tehát az első kód legalább egydimenziós, de a második kód csupán a nullvektort tartalmazza, akkor most egy olyan kódot kapunk, amelynek a kódszavai dadognak, mert az eredeti kód kódszavait kétszer egymás mellé írjuk. Ebből az következik, hogy most a kód távolsága az első kód távolságának a kétszerese. Végül vizsgáljuk meg azt a (normális) esetet, amikor mindkét kód legalább egydimenziós. Mivel mindegyik kód lineáris, ezért a távolság helyett nézhetjük a súlyokat, és tudjuk, hogy a kód minimális távolsága a minimális súlyú nem nulla kódszó súlya. Egy kódszó akkor és csak akkor nulla az új kódban, ha mindkét kiinduló komponense a nullvektor, ezért azon $\mathbf{u}|\mathbf{u}+\mathbf{v}$ kódszavak súlyát kell vizsgálnunk, amelyekben $\mathbf{u}$ és $\mathbf{v}$ legalább egyike nem nulla. Ez a halmaz két részre particionálható: az egyikben vannak azok, amelyekben $\mathbf{v} = \mathbf{0}$, míg a másikban a többi vektor. A súlyokra általánosan teljesül a $w(\mathbf{u}|\mathbf{u}+\mathbf{v}) = w(\mathbf{u}) + w(\mathbf{u}+\mathbf{v})$ egyenlőség. Amennyiben $\mathbf{v} = \mathbf{0}$, akkor $w(\mathbf{u}|\mathbf{u}+\mathbf{v}) = w(\mathbf{u}) + w(\mathbf{u}) = 2w(\mathbf{u})$, és mivel most $\mathbf{v} = \mathbf{0}$, ezért ha az összetett kód kódszava nem nulla, akkor $\mathbf{u} \neq \mathbf{0}$, így $w(\mathbf{u}|\mathbf{u}+\mathbf{v}) = 2w(\mathbf{u}) \geq 2d_1$. A másik osztályban $\mathbf{v} \neq \mathbf{0}$. Ekkor

$$\begin{aligned} w(\mathbf{u}|\mathbf{u}+\mathbf{v}) &= w(\mathbf{u}) + w(\mathbf{u}+\mathbf{v}) \geq w(\mathbf{u}) + |w(\mathbf{v}) - w(\mathbf{u})| \\ &\geq w(\mathbf{u}) + w(\mathbf{v}) - w(\mathbf{u}) = w(\mathbf{v}) \geq d_2, \end{aligned}$$

tehát a két eredményből $d \geq \min\{2d_1, d_2\}$. Ugyanakkor ha $\mathbf{u}_1$ és $\mathbf{v}_2$ olyan C_1- illetve C_2-beli kódszó, amelynek a súlya rendre d_1 és d_2, akkor $w(\mathbf{u}_1|\mathbf{u}_1 + \mathbf{0}_2) = 2d_1$, $w(\mathbf{0}_1|\mathbf{0}_1 + \mathbf{v}_2) = d_2$, ezért a kód távolsága nem nagyobb a $2d_1$ és d_2 minimumánál, és így a kód távolsága pontosan ez a minimum.

u_u + v_konstrukció$(n_1, k_1, d_1, q_1, n_2, k_2, d_2, q_2; n, k, d, q)$
  $q = p^{[s_1,s_2]}$
  $n = n_1 + \max\{n_1, n_2\}$
  $k = k_1 + k_2$
  ha $\min\{k_1, k_2\} > 0$
    $d = \min\{2d_1, d_2\}$
  különben ha $k_1 > 0$
    $d = 2d_1$
  különben ha $k_2 > 0$
    $d = d_2$
  elágazás vége
u_u + v_konstrukció vége.

A kód generátormátrixához a két generátormátrixot azonos hosszal kell megadni, amit úgy érünk el, hogy a kisebb hosszúságú kód mátrixát például jobbról nullákkal egészítjük ki. Ezzel a kiegészítéssel $\mathbf{G}_i' = (\mathbf{G}_i\ \mathbf{0}^{(k_i, n-n_i)})$, ahol $n = \max\{n_1, n_2\}$, $i \in \{1,2\}$ és $\mathbf{G} = \begin{pmatrix} \mathbf{G}_1 & \mathbf{G}_1' \\ \mathbf{0}^{(k_2,n_1)} & \mathbf{G}_2' \end{pmatrix}$. **A** kód egy ellenőrző mátrixa $\mathbf{H} = \begin{pmatrix} \mathbf{H}_1 & \mathbf{0}^{(n_1-k_1,n)} \\ -\mathbf{H}_2'' & \mathbf{H}_2' \end{pmatrix}$, ahol $\mathbf{H}_2' = (\mathbf{H}_2\ \mathbf{0}^{(n_2-k_2,n-n_2)})$, $\mathbf{H}_2'' = (\widetilde{\mathbf{H}}_2\ \mathbf{0}^{(n_2-k_2,n-n_2)})$, és $\widetilde{\mathbf{H}}_2$ a $\mathbf{H}_2$ első, $\min\{n_1, n_2\}$ számú oszlopát tartalmazó mátrix, mert $\mathbf{H}\mathbf{G}^T = \mathbf{0}$.

Maradékkód (residual code). Ez a konstrukció is lineáris kódból állít elő új kódot. Legyen az $[n, k, d]_q$-paraméterű C lineáris kódban $k > 1$ és $\left(1 + \frac{1}{q-1}\right) d \leq n$, továbbá $\mathbf{0} \neq \mathbf{u}$ egy $\left(1 + \frac{1}{q-1}\right) d$-nél

kisebb w súlyú kódszó. Az eredeti kóddal ekvivalens kódot kapunk, ha úgy rendezzük át az oszlopokat, hogy $\mathbf{u}$ nem nulla elemei a kódszó bal szélső w pozícióján álljanak, és akkor is ekvivalens átalakítást végzünk, ha ezen bal szélső w oszlop mindegyikét egy olyan nem nulla konstanssal szorozzuk, hogy $\mathbf{u}$-ban valamennyi nem nulla elem az egységelem legyen, ezért eleve tegyük fel, hogy van a kódban ilyen minimális súlyú $\mathbf{u}$ kódszó. Írjuk a tér $\mathbf{v}^T = v_0 \dots v_{w-1} v_w \dots v_{n-1}$ vektorát $\mathbf{v}^T = \mathbf{v}^{(b)^T} \mathbf{v}^{(j)^T}$ alakban, ahol $\mathbf{v}^{(b)^T} = v_0 \dots v_{w-1}$ és $\mathbf{v}^{(j)^T} = v_w \dots v_{n-1}$, ekkor $\mathbf{u}^{(b)^T} = \underbrace{e \dots e}_{w}$ és $\mathbf{u}^{(j)^T} = \underbrace{0 \dots 0}_{n-w}$. Nem nulla vektor kiegészíthető bázissá, így van a kódnak olyan bázisa, amelyben szerepel $\mathbf{u}$, tehát olyan generátormátrixa, amelynek első sora $\mathbf{u}^T$, azaz $\mathbf{G} = \begin{pmatrix} \bar{\mathbf{e}}^{(w)^T} & \mathbf{0}^{(n-w)^T} \\ \mathbf{G}^{(b)} & \mathbf{G}^{(j)} \end{pmatrix}$, ahol $\bar{\mathbf{e}}^{(w)}$ a csupa e-ből álló w-dimenziós vektor. Legyen C' a $\mathbf{G}^{(j)}$ által generált kód. Megmutatjuk, hogy C' egy $[n-w, k-1, d']_q$-paraméterű kód, ahol $d' \geq d - \left\lfloor \left(1 - \frac{1}{q}\right) w \right\rfloor$.

A kód hossza nyilván $n-w$. Vegyük $\mathbf{G}$ utolsó $k-1$ sorának valamely $\mathbf{v}^T = \mathbf{v}^{(b)^T} \mathbf{v}^{(j)^T}$ nem triviális lineáris kombinációját. Mivel a testnek q eleme van, a test egy-egy eleme a w-komponensű $\mathbf{v}^{(b)}$-ben átlagosan $\frac{w}{q}$-szor fordul elő, így van a testnek legalább egy olyan eleme, amely legalább $\left\lceil \frac{w}{q} \right\rceil$-szor szerepel. Legyen ez az elem c, és nézzük a $\mathbf{w} = \mathbf{v} - c\mathbf{u}$ vektort. Ez szintén a generátormátrix sorainak nem triviális lineáris kombinációja, így nem a nullvektor, ugyanakkor az utolsó $n-w$ pozícióján megegyezik $\mathbf{v}$-vel, hiszen $\mathbf{u}^{(j)} = \mathbf{0}^{(n-w)}$. Ha az első w hely valamely t-indexű pozíciójára $v_t = c$, akkor $w_t = v_t - cu_t = c - ce = 0$, így $\mathbf{w}$ első w pozíciójából legalább $\left\lceil \frac{w}{q} \right\rceil$ helyen 0 áll, tehát $\mathbf{w}^{(b)}$-ben legfeljebb $w - \left\lceil \frac{w}{q} \right\rceil = \left\lfloor \left(1 - \frac{1}{q}\right) w \right\rfloor$ helyen van 0-tól különböző elem. Ha egy kódszó nem a nullvektor, akkor a súlya legalább d, amiből következik, hogy $\mathbf{w}$, de akkor $\mathbf{v}$ utolsó $n-w$ pozícióján is minimum $d - \left\lfloor \left(1 - \frac{1}{q}\right) w \right\rfloor$ nullától különböző elemnek kell lennie. $\left\lfloor \left(1 - \frac{1}{q}\right) w \right\rfloor \leq \left(1 - \frac{1}{q}\right) w < d$, így $d - \left\lfloor \left(1 - \frac{1}{q}\right) w \right\rfloor > 0$, vagyis $\mathbf{w}^{(j)}$ nem $\mathbf{0}$, és a súlya legalább $d - \left\lfloor \left(1 - \frac{1}{q}\right) w \right\rfloor$. Ez tehát azt jelenti, hogy $\mathbf{G}^{(j)}$ sorai lineárisan függetlenek, továbbá C' egy $k-1$-dimenziós kód, és a távolsága legalább $d - \left\lfloor \left(1 - \frac{1}{q}\right) w \right\rfloor$.

Speciális esetként legyen $w = d$, ekkor $d - \left\lfloor \left(1 - \frac{1}{q}\right) w \right\rfloor = d - \left\lfloor \left(1 - \frac{1}{q}\right) d \right\rfloor = \left\lceil \frac{d}{q} \right\rceil$, és most a kapott maradékkód egy $[n-d, k-1, d']_q$-paraméterű kód a $d' \geq \left\lceil \frac{d}{q} \right\rceil$ távolsággal.

7. Kódolási korlátok

A kódolási korlátok a kód három paramétere, nevezetesen a kódszavak n hossza, a kód M mérete és d távolsága közötti kapcsolatra mutatnak rá, arra, hogy ha közülük kettőt megadunk, a harmadik már nem vehet fel tetszőleges értéket. A fő probléma az, hogy nagy kódsebességhez és kis hibavalószínűséghez a Shannon-tétel szerint hosszú kódszavakra, azaz nagy n-re, és minimális távolságú dekódolás esetén nagy kódtávolságra, tehát nagy d-re van szükség, ám ez a két feltétel ellentmondó: ha nagy a kód távolsága, akkor az összes lehetséges szónak csak kis része használható kódolásra, vagyis kicsi lesz $\frac{M}{q^n}$ és az $\mathcal{R} = n^{-1}\log_q M$ kódsebesség, ahol q a kódoló szimbólumok száma.

A továbbiakban többször lesz szükségünk egy adott szótól legfeljebb t távolságra lévő szavak számára, ahol t tetszőleges nemnegatív valós szám. Ezt az értéket $V_q(n,t)$-vel jelöljük. A V jelölés azt fejezi ki, hogy ez az érték mintegy az adott szó mint középpont körüli t sugarú gömb „térfogata”. Ha adott egy $\mathbf{u} \in S^n$ szó, ahol S a szimbólumok halmaza, és $n \geq i \in \mathbb{N}$, akkor $(q-1)^i$ olyan szó van S-ben, amely rögzített i számú pozícióban különbözik $\mathbf{u}$-tól, hiszen ezen pozíciók mindegyikén S bármely eleme előfordulhat, kivéve azt az egyet, amely $\mathbf{u}$-ban az adott helyen áll. Ebből következik, hogy

$$V_q(n,t) = \sum_{i=0}^{\lfloor t \rfloor} \binom{n}{i} (q-1)^i,$$

feltéve, hogy $n \geq t \in \mathbb{R}_0^+$, míg $V_q(n,t) = q^n$, ha $n < t \in \mathbb{R}$.

Egy másik, többször hivatkozott kifejezés a kódsebesség lesz, amelyet korábban már definiáltunk: egy $(n,M)_q$-paraméterű kód sebessége $\mathcal{R} = n^{-1}\log_q M$. Innen közvetlenül kapjuk, hogy egy n-hosszúságú kódszavakból álló, $\mathcal{R}$ kódsebességű kódban a kódszavak száma $M = q^{n\mathcal{R}}$.

A továbbiakban S jelöli a kódoló szimbólumok halmazát, q az S elemeinek számát, amelyről feltesszük, hogy legalább 2, n a kódszavak hosszát, amely minimum 2, és d a kód távolságát, amely szintén legalább 1, továbbá $M > 1$, ahol M a kódszavak száma.

7.1. Definíció

Az $(n,M,d)_q$-paraméterű C kód

- **maximális**, ha nincs olyan $(n,M',d')_q$-paraméterű C' kód, amely valódi részként tartalmazza C-t, és amelyre $d' \geq d$;
- **optimális**, ha $M = \max\{M' \mid \exists C' : (n,M',d)_q \text{ kód}\}$, vagyis C a lehető legnagyobb méretű n-hosszúságú, d-távolságú kód. A q szimbólummal felírható, n-hosszúságú és d-távolságú optimális kód méretét $A_q(n,d)$-vel jelöljük.

Δ

Ha $\mathbf{u}$ és $\mathbf{v}$ a C két olyan eleme, amelyre $d(\mathbf{u},\mathbf{v}) = d(C)$, és $C \subseteq C'$, akkor $\mathbf{u}$ és $\mathbf{v}$ C'-ben is benne van, így $d(C') \leq d(\mathbf{u},\mathbf{v}) = d(C)$, tehát a maximális kódnál $d' \geq d$ helyett írható $d' = d$ is.

Egy optimális kód nyilván maximális is, de ez fordítva nem igaz. Legyen például

$$C = \{0000,0101,0110,1011,1100\} \subseteq \{0,1\}^4.$$

Ez egy $(4,5,2)_2$-paraméterű maximális kód. A maximalitást beláthatjuk úgy, hogy a kódban nem szereplő 4-hosszúságú bináris sorozatok mindegyikéhez van a kódban olyan szó, amely legfeljebb csak egy helyen különbözik a kiválasztott szótól, de a következő módon is. 0000-tól legalább 2-távolságra lévő szavak legalább két 1-est tartalmaznak. Azok a pontosan két 1-est tartalmazó szavak, amelyekben a második pozíción 1 áll, benne vannak a kódban. Ha viszont egy 2-súlyú szó ezen a pozíción 0, akkor csak úgy különbözhet legalább két helyen az 1011 kódszótól, ha a három 1-esből legalább kettő 0, de ekkor az így kapott szó súlya legfeljebb 1, tehát nem lehet kódszó. Az 1111 csak 1 távolságra van 1011-től, tehát szintén nem szerepelhet a megadott kód bővítésében. Végül ha a nem kódszó $\mathbf{v}$ súlya 3, akkor a második pozícióján 1 áll, és a további három pozíció egyikén és csak egyikén 0, ám ekkor valamelyik 2-súlyú kódszótól vett távolsága 1, így ilyen $\mathbf{v}$-vel sem bővíthető a kód. Ugyanakkor C nem optimális, hiszen például $C = \{aaaa, aabb, abab, abba, baab, baba, bbaa, bbbb\}$ is 4-hosszúságú és 2-távolságú, 2 szimbólummal felírt kód, és a kódszavak száma 8. Az ennek a fejezetnek egy későbbi részén ismertetett *Singleton*-korlát alkalmazásával belátható, hogy ez a kód optimális, vagyis két szimbólummal legfeljebb nyolc szóból állhat egy kód, ha a távolsága 2.

Ezek után rátérünk a korlátok ismertetésére. Nézzük először a „triviális" korlátokat.

Az első korlát a legkisebb távolságú kódra vonatkozik. Legyen $C = S^n$, ekkor C egy $(n, q^n)_q$-kód, hiszen $|S^n| = |S|^n = q^n$. $q > 1$ és $n \geq 1$ következtében $M = q^n \geq q > 1$, és két különböző szó távolsága legalább 1, így bármely legalább két elemből álló kód távolsága minimum 1. Ugyanakkor a teljes halmazban van két olyan szó, amely pontosan egy helyen, mondjuk az első pozíción különbözik, tehát a kód távolsága legfeljebb 1, vagyis d pontosan 1. Mivel q szimbólummal legfeljebb q^n szó írható fel, ezért C optimális n-hosszúságú, 1-távolságú kód, és

$$A_q(n, 1) = q^n.$$

Most a legnagyobb távolságú kódokat nézzük. Tegyük először fel, hogy C egy $(n, M, n)_q$-paraméterű kód. Ekkor a kódhoz tartozó bármely két különböző szó mindegyik pozícióban, tehát az elsőben is különbözik egymástól. De ilyen szó legfeljebb q darab lehet, hiszen a különböző szimbólumok száma q, tehát q-nál több szó esetén legalább kettő megegyezik ezen a pozíción. Ebből következik, hogy $A_q(n, n) \leq q$. A másik irányhoz vegyük az S halmaz tetszőleges n (nem feltétlenül különböző) permutációját, és legyen $q \geq i \in \mathbb{N}^+$-ra és $n \geq j \in \mathbb{N}^+$-ra $\pi^{(j)}(i)$ az S i-edik eleme a j-edik permutációban. Ekkor az $\mathbf{u}^{(i)^T} = \pi^{(1)}(i) \dots \pi^{(n)}(i)$ vektorok száma q, és ha a k és $l \neq k$ pozitív egészek egyike sem nagyobb q-nál, akkor bármely $1 \leq i \leq n$ egészre $\pi^{(i)}(k) \neq \pi^{(i)}(l)$, így $d(\mathbf{u}^{(k)}, \mathbf{u}^{(l)}) = n$, és a q darab $\mathbf{u}^{(j)}$-ből álló kód távolsága n, vagyis $A_q(n, n) \geq q$, így a korábbi ellenkező irányú relációval együtt

$$A_q(n, n) = q.$$

Bináris kódokra érvényes a következő korlát:

$$A_2(n, 2k + 1) = A_2(n + 1, 2k + 2).$$

Ez azért igaz, mert a kódkonstrukcióknál láttuk, hogy akkor és csak akkor létezik n-hosszúságú, $2k + 1$-távolságú bináris kód, ha van $n + 1$-hosszúságú, $2k + 2$ távolságú bináris kód, így ez igaz a legtöbb kódszóból álló megfelelő paraméterű kódokra is.

Most különböző távolságú optimális kódokat hasonlítunk össze. Ekkor

$$d_1 < d_2 \Rightarrow A_q(n, d_1) \geq A_q(n, d_2).$$

Legyen ugyanis C_2 egy $(n, M, d_2)_q$-kód. Ekkor van a kódban olyan $\mathbf{u}$ és $\mathbf{v}$ kódszó, amely pontosan d_2 helyen különbözik. Válasszunk ki ebből a d_2 pozícióból tetszőleges, de rögzített $d_2 - d_1$ helyet, és szúrjuk át a kódot ezeken a pozíciókon. Az új kódban, C-ben, az $\mathbf{u}$-ból és $\mathbf{v}$-ből kapott kódszó $d_2 - (d_2 - d_1) = d_1 > 0$ helyen tér el, és bármely más kódszópárban is legalább ennyi az eltérések száma, amiből következik, hogy egyrészt az új kód mérete azonos az eredeti kód méretével, másrészt az új kód

távolsága d_1, így C egy $(n-(d_2-d_1), M, d_1)_q$-kód. Most legyen u az S szimbólumhalmaz tetszőleges eleme. Terjesszük ki C-t oly módon, hogy minden szó végére írjunk d_2-d_1 darab u-t, és legyen az így kapott kód C_1. C_1-ben a kódszavak hossza n, a kódszavak száma M, és mivel valamennyi kódszót ugyanazon toldalékkal egészítettük ki, a kódszavak távolsága, tehát magának a kódnak a távolsága sem változott, így C_1 egy $(n, M, d_1)_q$-paraméterű kód, ami mutatja, hogy ha létezik $(n, M, d_2)_q$-paraméterű kód, akkor biztosan létezik $(n, M, d_1)_q$-paraméterű kód is. De $A_q(n, d_1) \geq M$, és mivel ez bármely $(n, M, d_2)_q$-kód esetén igaz, igaz akkor is, amikor C_2 optimális, vagyis amikor $M = A_q(n, d_2)$, így $A_q(n, d_1) \geq M = A_q(n, d_2)$.

A másik összehasonlításban a kódszavak hossza tér el. Ebben az esetben

$$A_q(n+1, d) \leq qA_q(n, d).$$

Válasszunk ugyanis egy $(n+1, M, d)_q$-paraméterű C kódot. A kódszavak száma M, az alkalmazott szimbólumok száma q, így van olyan $u \in S$, amely a kódszavak első betűjeként legalább $\frac{M}{q}$-szor fordul elő. Rövidítsünk az első pozíción erre az u-ra. Az új kód $(n, M', d')_q$-paraméterű, ahol $M' \geq \frac{M}{q}$ és $d' \geq d$. Ez bármely $(n+1, M, d)_q$-kód esetén igaz, így akkor is, amikor C optimális, vagyis amikor $M = A_q(n+1, d)$, tehát $A_q(n, d) \geq A_q(n, d') \geq M' \geq \frac{1}{q} A_q(n+1, d)$, és innen átszorzással kapjuk az állítást.

Most nézzünk további korlátokat. Ezek egyrészt alsó, másrészt felső határt adnak adott hosszúságú és távolságú kódok méretére. A felső határ azt jelenti, hogy a megadott hosszúsággal és távolsággal maximum hány kódszót tudunk kiválasztani, az azonban egyáltalán nem biztos, hogy létezik is ilyen kód, vagyis a korlátok nem adnak garanciát arra, hogy ez a maximum ténylegesen elérhető. Ugyanakkor az alsó korlát azt garantálja, hogy mindig lehet találni ennyi kódszóból álló, a megadott hosszúsággal és távolsággal felépített kódot. Elsőként egy alsó korlátot adunk.

***Varshamov-Gilbert* korlát**. Ennek két változatát szokás megadni.

1.

$$A_q(n, d) \geq \frac{q^n}{V_q(n, d-1)}.$$

Ez az első alak tetszőleges szimbólumhalmaz esetén érvényes. A korlát azt mutatja, hogy mindig kiválasztható legalább $\frac{q^n}{V_q(n,d-1)}$ szó S^n-ből úgy, hogy bármely két különböző szó távolsága minimum d. Legyen ugyanis C egy $(n, M, d)_q$-paraméterű maximális kód. A kódszavak körüli $d-1$-sugarú gömbök uniója lefedi S^n-t. Ha nem így lenne, akkor lenne olyan $\mathbf{u} \in S^n$, amelynek bármely kódszótól való távolsága legalább d. Ekkor viszont $\mathbf{u}$ hozzávehető C-hez úgy, hogy az új halmaz bármely két elemének távolsága minimum d, vagyis egy $(n, M+1, d)_q$-paraméterű, a C-t tartalmazó kódunk lenne, ami lehetetlen, hiszen C maximális kód. Ebből következik, hogy a gömbök térfogatainak összege legalább akkora, mint S^n térfogata, vagyis q^n. De valamennyi gömb térfogata $V_q(n, d-1)$, és összesen M gömb van, tehát a gömbök térfogatának együttes összege $MV_q(n, d-1) \geq q^n$, ahonnan átosztással kapjuk, hogy $A_q(n, d) \geq M \geq \frac{q^n}{V_q(n,d-1)}$.

2. A másik változat lineáris kódok méretére ad alsó határt, így q prímhatvány. A korlát szerint ha egy $l \in \mathbb{N}$-re

$$q^l < \frac{q^n}{V_q(n-1, d-2)},$$

ahol $2 \le d \le n$, akkor van $[n, l, d]_q$-paraméterű kód. A bizonyításhoz felhasználjuk, hogy ha egy $\mathbb{F}_q$ fölötti $(n-l) \times n$-méretű, $n-l$-rangú $\mathbf{H}$ mátrix bármely legfeljebb $d-1$ oszlopa lineárisan független, akkor $\mathbf{H}$ egy $[n, l, d']_q$-kód ellenőrző mátrixa, ahol $d' \ge d$, így elég megmutatni, hogy ha a megadott feltétel teljesül, akkor van ilyen $\mathbf{H}$ mátrix.

A $0 \le i \le u < v$ egész számokkal $\binom{u}{i} < \binom{v}{i}$, és $2 \le d \le n$ esetén $0 \le d-2 < n-1$. Ekkor

$$q^{d-2} = \big((q-1)+1\big)^{d-2} = \sum_{i=0}^{d-2} \binom{d-2}{i} (q-1)^i$$
$$< \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i = V_q(n-1, d-2) < q^{n-1},$$

és mivel $q > 1$, ezért $d-2 < n-l$, azaz $d-1 \le n-l$. Az $n-l$-dimenziós térben van $n-l$ lineárisan független vektor. Ha $\mathbf{H}^{(n-l)}$ egy olyan $(n-l) \times (n-l)$-méretű mátrix, amelynek oszlopai az $\mathbb{F}_q^{n-l}$ tér lineárisan független vektorai, akkor $\mathbf{H}^{(n-l)}$ rangja $n-l$, így az oszlopai, de akkor az oszlopaiból kiválasztott bármely $d-1$ oszlop is lineárisan független. Ha most ehhez a mátrixhoz újabb oszlopokat adunk, akkor a mátrix rangja nem változik. Tegyük fel, hogy már kiválasztottunk $n-l \le j < n$ olyan vektort, amelyből bármely $d-1$ lineárisan független, és $\mathbf{H}^{(j)}$ az ezen vektorokból mint oszlopvektorokból álló mátrix. Legyen T azon vektorok halmaza, amelyeket a $\mathbf{H}^{(j)}$ oszlopaiból kiválasztott $d-2$-elemű részhalmazok generálnak, vagyis azok a vektorok tartoznak T-be, amelyek előállnak a j vektorból vett legfeljebb $d-2$ vektor lineáris kombinációjaként. T-ben legfeljebb $\sum_{i=0}^{d-2} \binom{j}{i} (q-1)^i$ vektor van. De $j < n$ –ből $j \le n-1$, így $\binom{j}{i} \le \binom{n-1}{i}$, ha $j \ge i \in \mathbb{N}$, tehát

$$\sum_{i=0}^{d-2} \binom{j}{i} (q-1)^i \le \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i = V_q(n-1, d-2) < q^{n-l}.$$

Ez az egyenlőtlenség azt mutatja, hogy van még olyan vektor $\mathbb{F}_q^{n-l}$-ben, amely a $\mathbf{H}^{(j)}$ oszlopaiból kiválasztott bármely $d-2$ vektortól lineárisan független, vagyis amelyet az előbbi j vektorból álló $\mathbf{H}^{(j)}$ mátrixhoz $j+1$-edik oszlopként csatolva, a kapott $\mathbf{H}^{(j+1)}$ mátrix bármely $d-1$ oszlopa lineárisan független. Mivel ez $j = n-1$-re is igaz, ezért igaz az állítás.

Ha q prímhatvány, akkor két alsó korlátot is kaptunk $A_q(n, d)$-re: egyrészt az 1. pontban megadott $A_q(n, d) \ge \frac{q^n}{V_q(n, d-1)}$ korlátot, másrészt ha 2.-ben $k = \max\left\{ l \in \mathbb{N} \middle| q^l < \frac{q^n}{V_q(n-1, d-2)} \right\}$, akkor van $[n, k, d]_q$-kód, tehát $(n, q^k, d)_q$-paraméterű kód, hiszen az $\mathbb{F}_q$ fölötti k-dimenziós tér elemeinek száma q^k, és így $A_q(n, d) \ge q^k$. Mindenesetre $\frac{q^n}{V_q(n, d-1)} < \frac{q^n}{V_q(n-1, d-2)}$, ugyanis

$$V_q(n-1, d-2) = \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < \sum_{i=0}^{d-1} \binom{n-1}{i} (q-1)^i$$
$$< \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i = V_q(n, d-1),$$

ezért ha van olyan l nemnegatív egész, amellyel $\frac{q^n}{V_q(n,d-1)} < q^l < \frac{q^n}{V_q(n-1,d-2)}$, akkor a másodikként megadott korlát szigorúbb, azaz nagyobb alsó korlátot biztosít az adott paraméterű kódok méretére. Megmutatjuk, hogy mindig van ilyen pozitív egész l (feltéve, hogy q prímhatvány!), vagyis a második korlát minden esetben jobb becslést ad.

Legyen $1 < a$ és $sa < b$, ahol a és b valós számok, és $1 < s \in \mathbb{N}$. $1 < a$, ezért van olyan $l \in \mathbb{N}^+$, hogy $s^{l-1} \leq a < s^l$, és innen $a < s^l \leq sa < b$. $d \leq n$, ezért $V_q(n, d-1) < V_q(n, n) = q^n$, és így $\frac{q^n}{V_q(n,d-1)} > 1$. Ha $a = \frac{q^n}{V_q(n,d-1)}$ és $b = \frac{q^n}{V_q(n-1,d-2)}$, akkor az állítás igazolásához elegendő belátni, hogy $q\frac{q^n}{V_q(n,d-1)} < \frac{q^n}{V_q(n-1,d-2)}$, vagyis hogy $qV_q(n-1, d-2) < V_q(n, d-1)$. Ez viszont igaz, ugyanis

$$\begin{aligned}
qV_q(n-1,d-2) &= q\sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i \\
&= (q-1)\sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i + \sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i \\
&= \sum_{i=1}^{d-1}\binom{n-1}{i-1}(q-1)^i + \sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i \\
&= 1 + \sum_{i=1}^{d-2}\left(\binom{n-1}{i-1} + \binom{n-1}{i}\right)(q-1)^i + \binom{n-1}{d-2}(q-1)^{d-1} \\
&< 1 + \sum_{i=1}^{d-2}\left(\binom{n-1}{i-1} + \binom{n-1}{i}\right)(q-1)^i + \left(\binom{n-1}{d-2} + \binom{n-1}{d-1}\right)(q-1)^{d-1} \\
&= \sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i = V_q(n,d-1).
\end{aligned}$$

Eredményünk szerint tehát a lineáris kódra adott második feltétel nagyobb alsó korlátot ad $A_q(n,d)$-re, mint az első, és ez a korlát nem csupán azt biztosítja, hogy van ennyi kódszóból álló n-hosszúságú, d-távolságú kód a q-elemű ábécé fölött, de még lineáris kód is létezik ezekkel a paraméterekkel. Ne feledjük azonban, hogy ez csak olyan q-ra igaz, amely egy prímszám pozitív egész kitevős hatványa.

Ha egy $(n, M, d)_q$-paraméterű C kódban $M \geq \frac{q^n}{V_q(n,d-1)}$, vagyis legalább annyi kódszóból áll, amennyit a Varshamov-Gilbert korlát garantál, akkor C **kielégíti a Varshamov-Gilbert korlátot**. Amennyiben C egy kódcsalád, vagyis minden $n \in \mathbb{N}^+$-ra C_n egy $(n, M_n, d_n)_q$-paraméterű kód, és mindegyik C_n kielégíti a Varshamov-Gilbet korlátot, akkor C egy **jó kód**.

A Varshamov-Gilbert korlátot más alakban is megadhatjuk, felhasználva a kódsebességet. Ha $M \geq \frac{q^n}{V_q(n,d-1)}$, akkor $V_q(n, d-1) \geq \frac{q^n}{M} = \frac{q^n}{q^{n\mathcal{R}}} = q^{n(1-\mathcal{R})}$, vagyis bármely adott q-hoz, n-hez és d-hez létezik olyan kód, amelynek a sebességére teljesül az

$$\mathcal{R} \geq 1 - n^{-1}\log_q V_q(n, d-1)$$

egyenlőtlenség.

Áttérünk a felső korlátokra.

***Hamming*-korlát, gömbkitöltési korlát**:

$$A_q(n,d) \leq \frac{q^n}{V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right)}.$$

Valóban, egy d-távolságú kódban a kódszavak köré írt, $\frac{d}{2}$-nél kisebb t-sugarú gömbök páronként diszjunktak, azaz a térfogatuk összege nem haladhatja meg a teljes tér térfogatát, q^n-t. A legnagyobb ilyen sugár $\left\lfloor\frac{d-1}{2}\right\rfloor$, és mivel a kódszavak körüli azonos sugarú gömbök térfogata azonos, ezért $MV_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right) \leq q^n$, ahol M a kódban lévő kódszavak száma. Ez minden $(n,M,d)_q$ kódra igaz, ezért igaz az optimális kódra is. Lineáris kód esetén $M = q^k$ egy nemnegatív egész k-val, és ekkor a Hamming-korlát alakja $V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right) \leq q^{n-k}$.

Egy $(n,M,d)_q$-paraméterű C kód **tökéletes**, **teljes** vagy **perfekt**, ha $M = \frac{q^n}{V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right)}$, illetve lineáris kód esetén ha $V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right) = q^{n-k}$. A kód tehát akkor tökéletes, ha a kódszavak száma a Hamming-korlát által megadott maximális érték. Korábban láttuk, hogy egy $[n,k,d]$-kód esetén minden olyan szó, amelynek a súlya kisebb, mint $\frac{d}{2}$, mellékosztályvezető. De a $\frac{d}{2}$-nél kisebb súlyú szavak száma megegyezik a nullvektor körüli $\left\lfloor\frac{d-1}{2}\right\rfloor$ -sugarú gömb térfogatával, $V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right)$-vel, és ha a kód tökéletes, akkor ez q^{n-k}-val, amely viszont a kód szerinti mellékosztályok száma, vagyis tökéletes kód esetén pontosan a $\frac{d}{2}$-nél kisebb súlyú vektorok mellékosztályvezetők. Ez más szavakkal azt jelenti, hogy ha a kód tökéletes, akkor a $\frac{d}{2}$-nél kisebb súlyú hibaminták és csak ezek a hibaminták javíthatóak, más szóval a kód kijavít, tehát helyesen javít minden olyan hibát, ahol a hibahelyek száma kisebb, mint $\frac{d}{2}$, és egyetlen olyan hibát sem javít helyesen, amelyben a hibák száma legalább $\frac{d}{2}$.

Páros távolságú kód nem lehet tökéletes. Legyen ugyanis $\mathbf{u}$ és $\mathbf{v}$ két olyan kódszó, amelyek távolsága pontosan d, ahol d a kód távolsága. Ha d páros, akkor van olyan $\mathbf{w}$ szó, amely mindkét kódszótól pontosan $\frac{d}{2}$ távolságra van. $\left\lfloor\frac{d-1}{2}\right\rfloor \leq \frac{d-1}{2} < \frac{d}{2}$, így $\mathbf{w}$ nincs benne sem az $\mathbf{u}$, sem a $\mathbf{v}$ kódszó körüli $\left\lfloor\frac{d-1}{2}\right\rfloor$-sugarú gömbben, és nem lehet benne egyetlen $\mathbf{c}$ kódszó körüli $\left\lfloor\frac{d-1}{2}\right\rfloor$ -sugarú gömbben sem, mert ha $\mathbf{c} \neq \mathbf{u}$, akkor $d(\mathbf{c},\mathbf{u}) \geq d$, és $d(\mathbf{u},\mathbf{w}) = \frac{d}{2}$ felhasználásával a háromszög-egyenlőtlenségnek a különbségre vonatkozó alakjából azt kapjuk, hogy

$$d(\mathbf{c},\mathbf{w}) \geq |d(\mathbf{c},\mathbf{u}) - d(\mathbf{u},\mathbf{w})| \geq d(\mathbf{c},\mathbf{u}) - d(\mathbf{u},\mathbf{w}) \geq d - \frac{d}{2} = \frac{d}{2}.$$

Ez viszont azt jelenti, hogy $\mathbf{w}$ nincs benne a kódszavak körüli $\left\lfloor\frac{d-1}{2}\right\rfloor$ -sugarú gömbök uniójában, vagyis M határozottan kisebb, mint a Hamming-korlátban megadott lehetséges maximális érték, így a kód nem tökéletes.

Tökéletes kód nem sok létezik, ami érthető, hiszen a tökéletesség azt jelenti, hogy a teljes tér egyrétűen lefedhető azonos sugarú gömbökkel. Mivel kevés tökéletes kód van, ezért érdekesek és fontosak az úgynevezett **kváziperfekt** kódok, amelyekre $\frac{q^n}{V_q\left(n,\left\lfloor\frac{d+1}{2}\right\rfloor\right)} \leq M < \frac{q^n}{V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right)}$, vagyis amelyeknél a kódszavak körüli $\left\lfloor\frac{d-1}{2}\right\rfloor$-sugarú gömbök nem tartalmaznak valamennyi szót, de az 1-gyel nagyobb sugarú gömbök már igen. Lineáris kódnál ez azt jelenti, hogy valamennyi mellékosztályvezető legfeljebb $\left\lfloor\frac{d+1}{2}\right\rfloor$ súlyú, azaz javítható minden $\frac{d}{2}$-nél kisebb súlyú hiba, de nem javítható egyetlen olyan hiba sem, amelyben a hibás helyek száma nagyobb $\frac{d+1}{2}$-nél.

Mint már mondtuk, nem sok tökéletes kód van. Tökéletes minden Hamming-kód, amelyekkel majd részletesen foglalkozunk, továbbá a **Golay-kódok** fele. Négy Golay-kód van, a $[24,12,8]_2$-paraméterű G_{24}, az ebből átszúrással kapott $[23,12,7]_2$-paraméterű G_{23}, a $[12,6,6]_3$-paraméterű G_{12}, és az

ebből átszúrással kapott $[11,6,5]_3$-paraméterű G_{11} kód. $V_2\left(23,\left\lfloor\frac{7-1}{2}\right\rfloor\right)=\sum_{i=0}^{3}\binom{23}{i}=2048=2^{23-12}$ és $V_3\left(11,\left\lfloor\frac{5-1}{2}\right\rfloor\right)=\sum_{i=0}^{2}\binom{11}{i}2^i=243=3^{11-6}$, így a két átszúrt kód tökéletes. Bizonyítható, hogy ha egy nem triviális q-áris kód perfekt, ahol q prímhatvány, akkor a kód paraméterei azonosak egy Hamming- vagy egy Golay-kód paramétereivel, továbbá a második esetben maga a kód is ekvivalens a megfelelő Golay-kóddal, míg ha a kód paraméterei egy Hamming-kód paramétereivel azonosak, és a kód lineáris, akkor a kód ekvivalens az ugyanolyan paraméterű Hamming-kóddal. Másként mondva lényegében véve nincs más $[23,12,7]_2$-paraméterű tökéletes kód, mint G_{23}, minden $[11,6,5]_3$-paraméterű tökéletes kód ekvivalenciától eltekintve a G_{11} kód, és minden $\left[\frac{q^r-1}{q-1},\frac{q^r-1}{q-1}-r,3\right]_q$-kód ekvivalens az ugyanilyen paraméterekkel rendelkező Hamming-kóddal. Az ilyen kódok tehát tökéletesek, de azt nem állítottuk, hogy csupán a felsorolt kódok perfektek (azt azonban igen, hogy a kódok halmazában igen ritkán fordul elő tökéletes kód).

A Hamming-korlátot is átírhatjuk olyan alakba, amelyben a méret helyett a kódsebesség áll. A megfelelő átalakítás után kapjuk, hogy bármely kódban

$$\mathcal{R}\le 1-n^{-1}\log_q V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right).$$

***Singleton*-korlát**. Legyen C egy $(n,M,d)_q$-paraméterű kód. Ha ezt átszúrjuk $d-1$ helyen, akkor még mindig legalább egy helyen különbözik az eredeti kód bármely két kódszava, vagyis átszúrás után is M különböző kódszavunk lesz, és a kódszavak hossza $n-d+1$. De a q szimbólummal felírható $n-d+1$ hosszúságú szavak száma q^{n-d+1}, vagyis legfeljebb ennyi különböző kódszó lehet, ahonnan $M\le q^{n-d+1}$, és mivel ez bármely $(n,M,d)_q$-kódra igaz, ezért

$$A_q(n,d)\le q^{n-d+1}.$$

A kódsebességet tartalmazó alak most úgy szól, hogy

$$\mathcal{R}\le 1-n^{-1}(d-1).$$

A 7.1. Definíció után a 65. oldalon megadott példában a második kód $(4,8,2)_2$-paraméterű volt, és $2^{4-2+1}=8$, vagyis a kód valóban optimális.

Lineáris kód esetén a Singleton-korlátot az $M=q^k$ összefüggéssel kapjuk: $q^k\le q^{n-d+1}$, vagyis bármely $[n,k,d]_q$-kódban

$$k\le n-d+1,$$

vagy átrendezés után

$$d\le n-k+1.$$

Ezt a korlátot másként is megkaphatjuk: ha a kód $[n,k,d]_q$-paraméterű, akkor az ellenőrző mátrixában bármely $d-1$ oszlop lineárisan független, vagyis a mátrixban van $d-1$ lineárisan független oszlop, a mátrix rangja legalább $d-1$. De a rang nem lehet nagyobb a sorok számánál, jelen esetben $n-k$-nál, így $d-1\le n-k$, ahonnan $d\le n-k+1$. Az olyan lineáris kódot, amelyben a Singleton-korlát egyenlőséggel teljesül, vagyis amelyben $d=n-k+1$, **maximális távolságú kód**nak, vagy **MDS**-kódnak neveznek, amelyekkel később részletesen foglalkozunk.

***Plotkin*-korlát**. Tekintsünk ismét egy $(n,M,d)_q$-kódot. Vegyük a kódszavakból alkotott rendezett párokat, és adjuk össze ezek távolságait, ekkor $T=\sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in C}d(\mathbf{u},\mathbf{v})$. Bármely $\mathbf{u}$ és $\mathbf{v}\neq\mathbf{u}$ kódszópárra $d(\mathbf{u},\mathbf{u})=0$ és $d(\mathbf{u},\mathbf{v})\ge d$, ezért $T=\sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in C}d(\mathbf{u},\mathbf{v})\ge\sum_{i=1}^{M}\sum_{i=1}^{M-1}d=M(M-1)d$. Most T értékét felülről is megbecsüljük. Rendezzük sorba az S szimbólumhalmaz elemeit, és indexeljük

őket a sorrendnek megfelelően 1-től q-ig. Jelölje $k_{i,j}$ azt a számot, ahányszor a j-edik szimbólum a kódszavak i-edik pozícióján előfordul. A T számításánál két adott kódszó esetén rögtön megnéztük, hogy mely pozíciókon tértek el, és ezek számát összegeztük. De eljárhatunk úgy is, hogy először csak az első pozíciót vizsgáljuk, és meghatározzuk, hogy ezen a pozíción összesen hány eltérés van, majd egymás után ezt minden pozícióra elvégezzük, és összeadjuk az egyes pozíciókon kapott eltérések számát. Az i-edik pozíción $k_{i,j}\left(M-k_{i,j}\right)$ eltérő pár van (mindegyik párt mindkét sorrendben számolva). Ha ugyanis kiválasztjuk S j-edik elemét, akkor ez az adott pozíción $k_{i,j}$-szer fordul elő, és külön-külön mindegyik előfordulás akkor és csak akkor tér el egy másik kódszó ezen pozíción álló szimbólumától, ha ez nem a j-edik szimbólum. De összesen M szó van, ebből $k_{i,j}$-ben ugyanaz a szimbólum áll, vagyis $M-k_{i,j}$ olyan szó van, amely a kiválasztott szótól eltér az i-edik pozíción. Összefoglalva tehát $T=\sum_{i=1}^{n}\sum_{i=1}^{q}k_{i,j}\left(M-k_{i,j}\right)$. Mivel valamennyi i indexre $\sum_{i=1}^{q}k_{i,j}=M$, ezért az előbbi összeg $T=\sum_{i=1}^{n}\sum_{i=1}^{q}k_{i,j}\left(M-k_{i,j}\right)=nM^2-\sum_{i=1}^{n}\sum_{i=1}^{q}k_{i,j}^2$. T akkor a legnagyobb, ha az egyenlet jobb oldalán álló $\sum_{i=1}^{n}\sum_{i=1}^{q}k_{i,j}^2$ összeg a legkisebb. Az összeg minden tagja pozitív, így akkor kapjuk a minimumot, ha mindegyikük a lehető legkisebb. Nézzük ugyanis $\sum_{i=1}^{r}t_i^2$-et, ahol t_i valós szám és az összegük m. Legyen $t=\frac{m}{r}$ és $t_i=t+u_i$. Ekkor $\sum_{i=1}^{r}u_i=\sum_{i=1}^{r}(t_i-t)=\sum_{i=1}^{r}t_i-rt=m-m=0$, továbbá $\sum_{i=1}^{r}t_i^2=\sum_{i=1}^{r}(t+u_i)^2=rt^2+2t\sum_{i=1}^{r}u_i+\sum_{i=1}^{r}u_i^2=rt^2+\sum_{i=1}^{r}u_i^2\geq rt^2$. A jobb oldali összeg második tagjában minden elem nemnegatív, így a legkisebb értéket akkor kapjuk, ha valamennyi i-re $t_i=t=\frac{m}{r}$, és a minimális érték $\sum_{i=1}^{r}t^2=\sum_{i=1}^{r}\left(\frac{m}{r}\right)^2=\frac{m^2}{r}$. A most kapott eredményt az eredeti összegre alkalmazva $T=nM^2-\sum_{i=1}^{n}\sum_{i=1}^{q}k_{i,j}^2\leq n\left(M^2-\frac{M^2}{q}\right)=nM^2\vartheta$, ahol $\vartheta=1-\frac{1}{q}$.

A T-re kapott alsó és felső korlát egybevetéséből azt kapjuk, hogy $M(M-1)d\leq nM^2\vartheta$. M-mel egyszerűsítve és átrendezve $M(d-\vartheta n)\leq d$. Most kössük ki, hogy $d>\vartheta n$. Ezzel a feltétellel $d-\vartheta n$ pozitív, tehát osztva vele az egyenlőtlenség iránya nem változik, vagyis $M\leq\frac{d}{d-\vartheta n}$, és ez az optimális kódra is igaz, tehát ha $d>\vartheta n$, akkor

$$A_q(n,d)\leq\frac{d}{d-\vartheta n}.$$

Ez az egyenlőtlenség a megadott feltétellel a Plotkin-korlát.

Bináris kódra a Plotkin-korlát szigorítható:

$$A_2(n,d)\leq 2\left\lfloor\frac{d}{2d-n}\right\rfloor.$$

Ha $q=2$, akkor $\vartheta=1-\frac{1}{2}=\frac{1}{2}$, tehát az eredeti korlátból $A_2(n,d)\leq 2\frac{d}{2d-n}$. Mivel $A_q(n,d)$ egész szám, ezért még az is igaz, hogy $A_2(n,d)\leq\left\lfloor 2\frac{d}{2d-n}\right\rfloor$. De bármely α valós számra $2\lfloor\alpha\rfloor\leq 2\alpha$, és mivel a bal oldalon egész szám áll, ezért $2\lfloor\alpha\rfloor\leq\lfloor 2\alpha\rfloor$, így a most bizonyítandó bináris korlát valóban legfeljebb akkora maximális kódméretet ad, mint az általános Plotkin-korlát. Lássuk be ezt az erősebb korlátot. Páros M esetén $\frac{M}{2}\leq\frac{1}{2}\frac{d}{d-\frac{1}{2}n}=\frac{d}{2d-n}$-ből $\frac{M}{2}=\left\lfloor\frac{M}{2}\right\rfloor\leq\left\lfloor\frac{d}{2d-n}\right\rfloor$, tehát $M\leq 2\left\lfloor\frac{d}{2d-n}\right\rfloor$. A páratlan esethez visszatérünk T-hez. Mivel M páratlan és $q=2$, ezért a maximális T-t adó kifejezésben $\frac{M}{q}$ nem egész. Most azonban minden i-re csak két $k_{i,j}$ értékünk van, és ha az egyik k_i, akkor a másik $M-k_i$, így most a $\sum_{i=1}^{n}\left(k_i^2+(M-k_i)^2\right)$ összeg minimumát keressük, ahol k_i egész szám. $x^2+(M-x)^2=2x^2-2Mx+M^2$ minimuma az $\frac{M}{2}$ helyen van, és erre a pontra a függvény szimmetrikus, továbbá ettől a ponttól jobbra és balra távolodva egyaránt szigorúan monoton nő a függvény értéke. Ekkor az $\frac{M}{2}$-t közrefogó két legközelebbi egész szám, $\frac{M-1}{2}$ és $\frac{M+1}{2}$ adja a T függvény minimumát az egész helyeken, és bármelyiket választhatjuk, hiszen a másik érték a másik szimbólum előfordulásainak száma. Azt kaptuk tehát,

hogy $M(M-1)d \le T \le n\frac{(M-1)(M+1)}{2}$, ha $q=2$ és M páratlan. $M-1$-gyel osztva $\big((M+1)-1\big)d \le n\frac{M+1}{2}$, ebből átrendezés után $(2d-n)(M+1) \le 2d$, és innen $\frac{M+1}{2} \le \frac{d}{2d-n}$. M páratlan, ezért $\frac{M+1}{2}$ egész szám, ekkor $\frac{M+1}{2} = \left\lfloor \frac{M+1}{2} \right\rfloor \le \left\lfloor \frac{d}{2d-n} \right\rfloor$, és $M \le M+1 \le 2\left\lfloor \frac{d}{2d-n} \right\rfloor$, vagyis páratlan M-re is teljesül az egyenlőtlenség.

Most egy más jellegű korlátot adunk. Meghatározzuk, hogy minimum milyen hosszúságú kóddal lehet adott k-dimenziós, d-távolságú lineáris kódot konstruálni. Ehhez a maradékkódot vesszük segítségül.

***Griesmer*-korlát**: ha C egy $[n,k,d]_q$-kód, akkor

$$n \ge \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

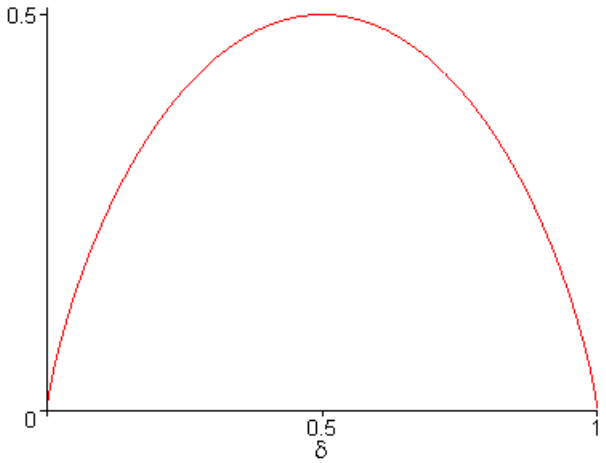
Láttuk ugyanis a maradékkódnál, hogy $[n,k,d]_q$-paraméterű C kódból $\left[n^{(1)}, k-1, d^{(1)}\right]_q$-paraméterű $C^{(1)}$ kódot kapunk, ahol $n^{(1)} = n-d = n-\left\lceil \frac{d}{q^0} \right\rceil$ és $d^{(1)} \ge \left\lceil \frac{d}{q} \right\rceil$. Legyen $C^{(0)} = C$, $n^{(0)} = n$ és $d^{(0)} = d$. Ha $k \ge 2$, akkor $C^{(1)}$-ből maradékképzéssel kapunk egy $\left[n^{(2)}, k-2, d^{(2)}\right]_q$-paraméterű $C^{(2)}$ kódot, ahol $n^{(2)} = n^{(1)} - d^{(1)} = n - d^{(0)} - d^{(1)}$ és $d^{(2)} \ge \left\lceil \frac{d^{(1)}}{q} \right\rceil \ge \left\lceil \frac{\left\lceil \frac{d}{q} \right\rceil}{q} \right\rceil = \left\lceil \frac{d}{q^2} \right\rceil$. Ha $k > j \in \mathbb{N}^+$, akkor $C^{(j)}$-ben $k-j$ pozitív, tehát a kód tartalmaz nem nulla kódszót, amelynek a súlya, és így a kód hossza is pozitív, és az eljárás megismételhető. Indukcióval azt kapjuk, hogy $n^{(j)} = n - \sum_{i=0}^{j-1} d^{(i)}$ és $d^{(j)} \ge \left\lceil \frac{d^{(j-1)}}{q} \right\rceil \ge \left\lceil \frac{d}{q^j} \right\rceil$. Ekkor $0 \le n^{(k)} = n^{(k-1)} - d^{(k-1)} = n - \sum_{i=0}^{k-1} d^{(i)} \le n - \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$, és átrendezéssel kapjuk az állított egyenlőtlenséget.

Most vezessük be a $\delta = \frac{d}{n}$ jelölést. Mivel innen $d = \delta n$, ezért $A_q(n,d) = A_q(n,\delta n)$, vagyis ez az n-től és δ-tól függő kifejezés, jelöljük $A_q^*(n,\delta)$-val. A Shannon-tételből tudjuk, hogy nagy kódsebességet és kis dekódolási hibát hosszú kódokkal lehet megvalósítani, ezért érdekes és fontos $A_q^*(n,\delta)$ aszimptotikus viselkedése. Ez indokolja, hogy bevezessük az $a_q(\delta) = \overline{\lim_{n\to\infty}}\left(n^{-1}\log_q A_q^*(n,\delta)\right)$ függvényt. Mivel $A_q^*(n,\delta)$ egy kód mérete, ezért $n^{-1}\log_q A_q^*(n,\delta)$ kódsebesség, azaz $a_q(\delta)$ a δ függvényében megadja az elérhető kódsebességek felső határát. Kérdéses még δ szerepe. Tudjuk, hogy minimális távolságú dekódolás esetén a javítható hibák száma d-vel arányos, így $\delta = \frac{d}{n}$ lényegében véve az n-hosszúságú kódszóban fellépő javítható hibák arányát fejezi ki. Ez azt jelenti, hogy $a_q(\delta)$ a javítható hibaarány függvényében elérhető maximális kódsebességet adja meg. Az $a_q(\delta)$-ra az alábbiakban megadott kifejezéseket **aszimptotikus korlát**oknak nevezzük.

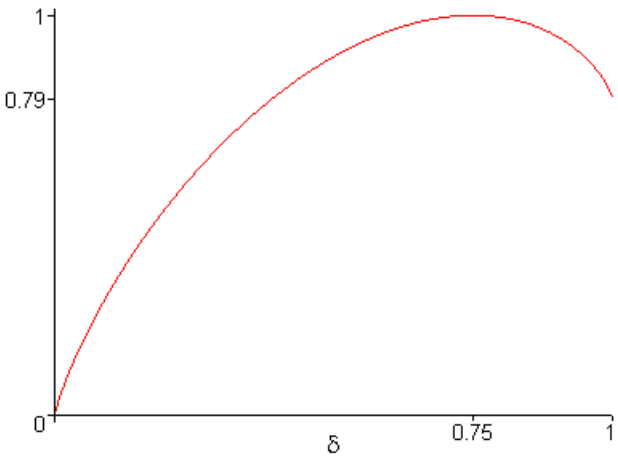
Mielőtt rátérnénk az aszimptotikus korlátok ismertetésére, ismertetünk néhány ezzel kapcsolatos dolgot. Korábban már volt szó az entrópiáról: ha Ω egy n elemi eseményből álló eseménytér, és az i-edik esemény bekövetkezésének valószínűsége p_i, akkor $I_i = -\log_r p_i$ ezen esemény egyedi információja, ahol r tetszőleges, 1-nél nagyobb valós szám, és ha $r=2$, akkor az információ egysége a bit. $H_r(p_1,\dots,p_n) = -\sum_{i=1}^n p_i \log_r p_i$ az eseménytér átlagos információtartalma, az entrópia. Láthatóan ez a függvény a pozitív p_i-ken értelmezett, ám kiterjeszthető az értelmezés arra az esetre is, amikor egyes i indexre p_i értéke 0, ugyanis $x\log x$-nek a 0-ban van jobb oldali határértéke, nevezetesen a 0. Legyen tehát definíciószerűen $I=0$, ha $p=0$, így H_r már a nemnegatív valós argumentumokon értelmezett, és természetesen $\sum_{i=1}^n p_i = 1$. Amennyiben $n=2$, akkor az előbbi feltétel azt jelenti, hogy $p_2 = 1-p_1$, vagyis p_1 helyett egyszerűen p-t írva az entrópia ebben az esetben egyetlen változótól, p-től függ, és ekkor azt írjuk, hogy $H_r(p)$, ahol p 1-nél nem nagyobb nemnegatív valós szám. Nézzük meg ezt a

függvényt. A definíció alapján $H_r(p) = -p\log_r p - (1-p)\log_r(1-p)$, és szintén a definíció miatt $H_r(0) = 1 = H_r(1)$, továbbá az is könnyen látható, hogy $H_r(p) = H_r(1-p)$. Ez másként írva $H_r\left(\frac{1}{2}+x\right) = H_r\left(\frac{1}{2}-x\right)$, vagyis a függvény szimmetrikus az abszcisszatengely $\frac{1}{2}$ pontján átmenő, és az ordinátatengellyel párhuzamos egyenesre. A függvény a $(0,1)$ intervallumban deriválható, és a deriváltja $H_r'(p) = -\log_r p + \log_r(1-p) = \log_r\frac{1-p}{p}$. A derivált akkor és csak akkor 0, amikor a logaritmusfüggvény argumentuma 1, vagyis amikor $\frac{1-p}{p} = 1$, vagyis, ha $p = \frac{1}{2}$. Mivel 0-ban és 1-ben a függvény értéke 0, és az intervallum többi pontjában pozitív, ezért a $p = \frac{1}{2}$ pontban maximuma van, továbbá a maximum értéke $H_r\left(\frac{1}{2}\right) = \log_r 2 = \frac{1}{\log_2 r}$, és ez 1, ha $r = 2$, míg $r > 2$ esetén 1-nél kisebb. A 0-ban a deriváltfüggvény jobb oldali határértéke $+\infty$, és a szimmetria miatt 1-ben a bal oldali határérték $-\infty$. A második derivált $H_r''(p) = -\frac{1}{\ln r}\frac{1}{p(1-p)}$, és ez $(0,1)$-ben negatív, így a függvény alulról konkáv.

Természetesen a H_r függvény argumentuma tetszőleges $1 \geq \delta \in \mathcal{R}_0^+$ érték lehet, nem kell, hogy valószínűség legyen. Ezek után megrajzolható a függvény, amelyet $r = 4$-re az 5. ábra mutat.



5. ábra



6. ábra

Szükségünk lesz az előbbi entrópiafüggvényből származtatott H_r^* függvényre is: ez szintén az 1-nél nem nagyobb nemnegatív valós számokon értelmezett, és $H_r^*(\delta) = H_r(\delta) + \delta\log_r(r-1)$, ahol $r > 1$. Rögtön látni, hogy $H_2^* = H_2$, továbbá $H_r^*(0) = 0$, $H_r^*(1) = \log_r(r-1)$, és $H_r^*(\delta) > 0$, ha $1 > \delta \in \mathbb{R}^+$. A derivált $H_r^{*\prime}(\delta) = H_r'(\delta) + \log_r(r-1) = \log_r\left(\frac{1-\delta}{\delta}(r-1)\right)$, így a $\delta = 1 - \frac{1}{r} = \vartheta$ pontban maximum van, és a maximum értéke 1. A 0-ban a derivált jobb oldali határértéke ismét $+\infty$, és 1-ben

a bal oldali határérték $-\infty$. $H_r^{*\prime\prime}(\delta) = -\frac{1}{\ln r}\frac{1}{\delta(1-\delta)} = H_r^{\prime\prime}(\delta)$ a $0 < \delta < 1$ intervallumban negatív, a függvény alulról konkáv. Az $r = 4$ esetre a függvényt a 6. ábra mutatja.

Használni fogjuk még az alábbi összefüggést, amelyet nem bizonyítunk: ha $0 \le \delta \le \vartheta$, akkor

$$\lim_{n\to\infty}(n^{-1}\log_r V_r(n, \lfloor \delta n \rfloor)) = H_r^*(\delta).$$

A továbbiakban δ tetszőleges nemnegatív valós szám lehet, így általában δn sem egész szám, és esetleg 0, ezért legyen $A_q(n, 0) = 1$, továbbá $A_q(n, t) = A_q(n, \lfloor t \rfloor)$, ahol $t \in \mathbb{R}_0^+$. Ezek után lássuk az aszimptotikus korlátokat.

A Varshamov-Gilbert korlátból egy aszimptotikus alsó korlátot kapunk: ha $0 \le \delta \le \vartheta$, akkor

$$a_q(\delta) \ge 1 - H_q^*(\delta).$$

A definíció és a Varshamov-Gilbert korlát első alakja alapján ugyanis

$$A_q^*(n, \delta) = A_q(n, \delta n) = A_q(n, d) \ge \frac{q^n}{V_q(n, d-1)} = \frac{q^n}{V_q(n, \delta n - 1)} \ge \frac{q^n}{V_q(n, \lfloor \delta n \rfloor)},$$

és ha $0 \le \delta \le \vartheta$, akkor

$$\begin{aligned} a_q(\delta) &= \overline{\lim_{n\to\infty}}\left(n^{-1}\log_q A_q^*(n, \delta)\right) \ge \overline{\lim_{n\to\infty}}\left(n^{-1}\log_q \frac{q^n}{V_q(n, \lfloor \delta n \rfloor)}\right) \\ &\ge \lim_{n\to\infty}\left(n^{-1}\log_q \frac{q^n}{V_q(n, \lfloor \delta n \rfloor)}\right) = 1 - \lim_{n\to\infty}\left(n^{-1}\log_q V_q(n, \lfloor \delta n \rfloor)\right) = 1 - H_q^*(\delta). \end{aligned}$$

A Hamming-korlát szerint $A_q(n, d) \le \frac{q^n}{V_q\left(n, \left\lfloor \frac{d-1}{2} \right\rfloor\right)}$, és ebből némi ügyeskedéssel kijön, hogy ha $0 \le \frac{\delta}{2} \le \vartheta$, akkor

$$a_q(\delta) \le 1 - H_q^*\left(\frac{\delta}{2}\right).$$

De $\vartheta \ge \frac{1}{2}$, ezért ez a korlát a teljes $0 \le \delta \le 1$ intervallumban érvényes.

Az aszimptotikus Singleton-korlát könnyen megkapható. A korlát szerint $A_q(n, d) \le q^{n-d+1}$, így $A_q^*(n, \delta) \le q^{n-\delta n+1}$, és innen $n^{-1}\log_q A_q^*(n, \delta) \le 1 - \delta + \frac{1}{n}$. A két oldal határértéke adja a korlátot:

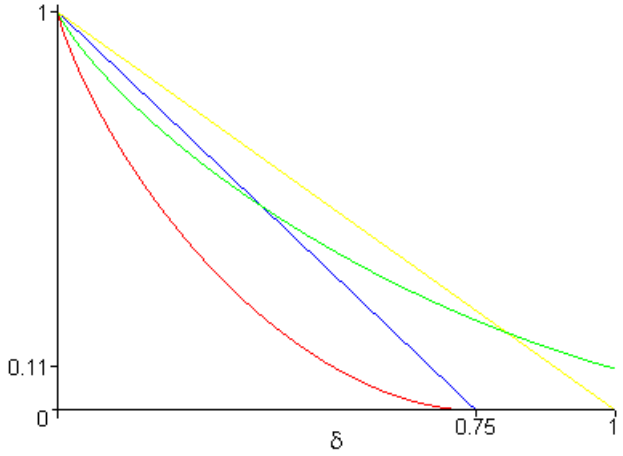
$$a_q(\delta) \le 1 - \delta, \text{ feltéve, hogy } 0 \le \delta \le 1.$$

A Plotkin-korlátból származtatott aszimptotikus korlát bonyolultabb. Ha $\vartheta < \delta \le 1$, akkor a Plotkin-korlát $A_q(n, d) \le \frac{d}{d-\vartheta n}$, vagyis $A_q^*(n, \delta) \le \frac{\delta}{\delta-\vartheta}$. A jobb oldali kifejezés értéke egy n-től független pozitív valós szám, így a logaritmusa sem függ n-től. Ezt n-nel osztva a kapott érték a 0-hoz tart, miközben n minden határon túl nő, így azt kaptuk, hogy a $\vartheta < \delta \le 1$ tartományban $a_q(\delta) = 0$. Nézzük ezek után a $0 \le \delta < \vartheta$ értékeket. Ekkor a Plotkin-korlát közvetlenül nem alkalmazható, ám némi ügyeskedéssel eredményre juthaunk. Legyen $n' = \left\lfloor \frac{d-1}{\vartheta} \right\rfloor$, ekkor $\frac{d-1}{\vartheta} - 1 < n' \le \frac{d-1}{\vartheta}$, és ebből $1 \le d - \vartheta n' <$

$1+\vartheta$. Tekintettel arra, hogy most $\frac{d}{n}=\delta<\vartheta$, ezért $n'=\left\lfloor\frac{d-1}{\vartheta}\right\rfloor\leq\frac{d-1}{\vartheta}<\frac{d}{\vartheta}<n$, és ha $d>1$ (amit feltehetünk, hiszen különben a triviális korlátot kapjuk), akkor $\frac{d-1}{\vartheta}-1=\frac{d-1-\vartheta}{\vartheta}>0$, hiszen $\vartheta<1$, és így $n'\geq 1$, mert n' egész szám. Rövidítsünk egy $(n,M,d)_q$-paraméterű C kódot egy $(n',M',d')_q$-paraméterű C' kóddá. A 67. oldalon láttuk, hogy tudunk egy kódot egy pozícióján úgy rövidíteni, hogy $M'\geq\frac{M}{q}$, vagyis $M\leq qM'$, és innen indukcióval azt kapjuk, hogy ha $n>n'$, akkor lehet $n-n'$ különböző helyen úgy rövidíteni, hogy az eredményül kapott C' kódban $q^{n-n'}M'\geq M$. A rövidítés során a kód távolsága nem csökken, így az is igaz, hogy $d'\geq d$. C'-re alkalmazható a Plotkin-korlát, ugyanis $1=\frac{n'}{n'}\geq\delta'=\frac{d'}{n'}\geq\frac{d}{n'}>\frac{d-1}{n'}\geq\vartheta$. Ekkor $M'\leq\frac{d'}{d'-\vartheta n'}$, és felhasználva, hogy $0<\vartheta n'<d\leq d'$, $\frac{d'}{d'-\vartheta n'}\leq\frac{d}{d-\vartheta n'}\leq d$, vagyis $M'\leq d$, és így $M\leq q^{n-n'}M'\leq q^{n-n'}d$. A korábban kapott $\frac{d-1}{\vartheta}-1<n'\leq\frac{d-1}{\vartheta}$ egyenlőtlenséget n-nel osztva $\frac{\delta}{\vartheta}-\frac{1}{n}\left(1+\frac{1}{\vartheta}\right)<\frac{n'}{n}\leq\frac{\delta}{\vartheta}-\frac{1}{n}\frac{1}{\vartheta}$, ahonnan látjuk, hogy ha n tart a végtelenhez, akkor $\frac{n'}{n}$ tart $\frac{\delta}{\vartheta}$-hoz. $M\leq dq^{n-n'}$ mindkét oldalát logaritmálva és n-nel osztva az $\frac{1}{n}\log_q M\leq\frac{1}{n}(n-n')+\frac{1}{n}\log_q d$ egyenlőtlenséget kapjuk, amelynek a jobb oldala az előbbi eredmény szerint $1-\frac{\delta}{\vartheta}$-hoz tart. Ez független a kód méretétől, így az optimális kód esetén is érvényes, tehát $a_q(\delta)\leq 1-\frac{\delta}{\vartheta}$. Ennek a kifejezésnek létezik a határértéke, amikor δ tart ϑ -hoz, és 0, amely megegyezik a korábban a $\vartheta<\delta\leq 1$ esetre kapott érték jobb oldali határértékével, vagyis

$$a_q(\delta)\begin{cases}\leq 1-\frac{\delta}{\vartheta}, & \text{ha } 0\leq\delta<\vartheta\\ =0, & \text{ha } \vartheta\leq\delta\leq 1.\end{cases}$$

A fentiekben megadott aszimptotikus korlátokat $q=4$ esetén a 7. ábra mutatja. Az alsó görbe a Varshamov-Gilbert korlát, a felső egyenes a Singleton-korlát, a másik egyenes adja a Plotkin-korlátot, és a negyedik görbe a Hamming-korlát. Az ábra is mutatja, hogy miért van szükség több különböző korlátra: különböző tartományban más és más korlát ad szigorúbb feltételt.



7. ábra

Az ismert kódcsaládok legtöbbjénél a szóhosszúság növekedésével vagy a $\delta=\frac{d}{n}$ relatív távolság, vagy a kódsebesség 0-hoz tart. A Varshamov-Gilbert korlátnál definiáltuk a jó kód fogalmát. Most ezt kicsit általánosítjuk. A növekvő szóhosszúságú (n_i,M_i,d_i)-paraméterű C_i kódokból álló kódszócsaládot jó kódnak mondjuk, ha aszimptotikusan mind a relatív távolsága, mind a sebessége nagyobb, mint 0. Ennél erősebb, ha $0<\delta=\lim_{n\to\infty}\frac{d}{n}<1-q^{-1}$, és $a_q(\delta)$ eléri az aszimptotikus Varshamov-Gilbert korlátot, azaz ha $a_q(\delta)\geq 1-H_q^*(\delta)$.

A megismert korlátok alkalmazására lássunk egy példát. Legyen $q = 2$, $n = 13$ és $d = 5$.

Mivel a kód bináris, és d páratlan, ezért $A_2(13,5) = A_2(14,6)$, így mindkettőt meghatározzuk, és közülük az erősebbet választjuk.

Az $A_q(n+1,d) \leq qA_q(n,d)$ szabály alkalmazásával $A_2(13,5) \leq 2^8 A_2(5,5) = 2^8 \cdot 2 = 512$, és hasonlóan kapjuk, hogy $A_2(14,6) \leq 2^8 A_2(6,6) = 512$.

Most nézzük a Varshamov-Gilbert korlátokat. 2 prímhatvány, alkalmazható a lineáris kódokra adott erősebb alak. $2^4 = 16 < \frac{q^n}{V_q(n-1,d-2)} = \frac{2^{13}}{\sum_{i=0}^{3}\binom{12}{i}} = \frac{8192}{299} \leq 32 = 2^5$, és a 14-hosszúságú kódokra hasonló számítással $8 < \frac{2^{14}}{\sum_{i=0}^{4}\binom{13}{i}} \leq 16$, tehát $A_2(13,5) \geq 16$, és az is igaz, hogy van $[13,4,5]_2$ kód.

A Singleton-korlátból $A_2(13,5) \leq 2^{13-5+1} = 512$, és ugyanezt kapjuk $A_2(14,6)$-ra, továbbá az 5-távolságú, 13-hosszúságú lineáris kódok legfeljebb 9-dimenziósak.

A Hamming-korláttal $A_q(n,d) \leq \frac{q^n}{V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right)}$, ami most $A_2(13,5) \leq \frac{2^{13}}{\sum_{i=0}^{2}\binom{13}{i}} = \frac{8192}{92} \approx 89{,}04$ és $A_2(14,6) \leq \frac{2^{14}}{\sum_{i=0}^{2}\binom{14}{i}} = \frac{16384}{106} \approx 154{,}57$, vagyis innen $A_2(13,5) \leq 89$.

A Plotkin-korlát nem alkalmazható közvetlenül, hiszen $\vartheta = 1 - \frac{1}{2} = \frac{1}{2}$, és 5 nem nagyobb, mint $\frac{1}{2} \cdot 13$, illetve 6 is kisebb 7-nél. Tudjuk azonban, hogy $2^4 A_2(9,5) \geq A_2(13,5)$, és 5 nagyobb, mint 9 fele, így alkalmazható a Plotkin-korlát. E szerint $A_2(9,5) \leq 2\left\lfloor\frac{5}{2\cdot 5-9}\right\rfloor = 10$, és innen $A_2(13,5) \leq 160$. A másik kódnál elég három pozícióval csökkenteni a kód hosszúságát. Most $2^3 A_2(11,6) \geq A_2(14,6)$ és $A_2(11,6) \leq 2\left\lfloor\frac{6}{2\cdot 6-11}\right\rfloor = 12$, tehát $A_2(14,6) \leq 96$, és ez adja a szigorúbb korlátot.

Az eddigieket összefoglalva azt kaptuk, hogy $16 \leq A_2(13,5) \leq 89$, továbbá lineáris kódokra $4 \leq k \leq \log_2 89 = 6{,}48$, vagyis $4 \leq k \leq 6$. Lineáris kódokra van még egy korlátunk, a Griesmer-korlát, amely minimális hosszt határoz meg, nevezetesen egy $[n,k,d]_q$ kódban $n \geq \sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil$. Ebből meghatározhatjuk a maximális k értéket is, amely kielégíti a $\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil \leq n < \sum_{i=0}^{k}\left\lceil\frac{d}{q^i}\right\rceil$ egyenlőtlenséget. Könnyű ellenőrizni, hogy most $k = 6$, vagyis nem kaptunk a korábbinál szigorúbb feltételt, így lineáris kódra a végeredmény $4 \leq k \leq 6$.

8. MDS-kódok

Az MDS kódok maximális távolságú kódok, **M***aximum* **D***istance* **S***eparable* kezdőbetűi adják az elnevezést. Az első két betű jelentése világos, az utolsó szó értelmére később visszatérünk.

Az 54. oldalon láttuk, hogy a Singleton-korlát szerint bármely $[n,k]_q$ lineáris kódra teljesül a $k \leq n-d+1$, vagy másként írva, a $d \leq n-k+1$ összefüggés. Ez mutatja, hogy lineáris kódnál a távolság legnagyobb értékét adott n és k esetén akkor kapjuk, ha az előbbi relációban egyenlőség áll, vagyis az ilyen kód az adott hosszúság és méret mellett maximális távolságú, és éppen az ilyen tulajdonságú kódokat neveztük ott maximális távolságúnak. Itt most ezt definícióként is megismételjük.

8.1. Definíció

Az $[n,k,d]_q$-paraméterű C kód **maximális távolságú** vagy **MDS kód**, ha $d = n-k+1$.

Δ

Az első kérdés az, hogy vajon létezik-e egyáltalán MDS-kód.

8.2. Tétel

Tetszőleges $n \in \mathbb{N}^+$-ra az $[n,n]_q$-paraméterű kód maximális távolságú, továbbá létezik $[n,1]_q$-, és ha $n \geq 2$, akkor $[n,n-1]_q$-paraméterű MDS-kód.

Δ

Bizonyítás:

$[n,n]_q$-kód a teljes n-dimenziós teret jelenti, és mivel $n > 0$ és $q \geq 2$, nem csupán a nullvektorból áll. Ekkor a kód távolsága pozitív, ezért $d \geq 1$. A Singleton-korláttal $1 \leq d \leq n-n+1 = 1$, ami csak egyenlőséggel igaz , tehát $d = n-n+1 = n-k+1$, hiszen most $k = n$.

Az $[n,1]_q$ kód egy nem nulla vektor $\mathbb{F}_q$-beli konstansszorosaiból áll. Ha a konstans nem nulla, akkor az adott kódszóban pontosan az a komponens nulla, amely a generáló vektorban, ezért ha n-súlyú vektorral generáljuk a kódot, akkor a nem nulla kódszavak súlya, és így a kód távolsága is n. Ekkor $d = n = n-1+1 = n-k+1$, a kód maximális távolságú.

Most legyen $n > 1$ és C egy $[n-1,n-1]_q$ kód, ekkor C távolsága 1. Terjesszük ki a kódot egy $[n,n-1]_q$ kóddá egy ellenőrzőjeggyel, vagyis legyen az eredetileg $\mathbf{v}^T = v_0 \ldots v_{n-2}$ kódszóhoz illesztett új komponens értéke $v_{n-1} = -\sum_{i=0}^{n-2} v_i$. Mivel C távolsága 1, a kiterjesztett kód távolsága 2 lesz (lásd az 54. oldalon), és $d = n-(n-1)+1 = n-k+1$, vagyis újra MDS-kódot kaptunk.

□

8.3. Definíció

A $k = 1$-hez, n-hez vagy $n-1$-hez tartozó maximális távolságú kód **triviális MDS kód**, minden más esetben **nem triviális MDS kód**.

Δ

Az alábbi tételben az MDS-kódok néhány alapvető tulajdonságát igazoljuk.

8.4. Tétel

Egy $[n,k,d]_q$-paraméterű C kódra, amelynek a generátormátrixa **G** és ellenőrző mátrixa **H**, az alábbi tulajdonságok ekvivalensek:

1. $d \geq n - k + 1$;
2. $d = n - k + 1$;
3. $\mathbf{H}$ bármely legalább d oszlopa lineárisan összefüggő;
4. $\mathbf{H}$ bármely d oszlopa lineárisan összefüggő;
5. bármely d pozícióhoz van olyan kódszó, amely pontosan ezen a d helyen nem nulla;
6. $\mathbf{G}$ bármely $n - d + 1$ oszlopa lineárisan független;
7. $\mathbf{G}$-ben van $n - d + 1$ lineárisan független oszlop.

Δ

Bizonyítás:

Elsőként megjegyezzük, hogy ha egy lineáris kódnak van távolsága, akkor mind k, mind d nagyobb, mint 0. Az állítást ciklikusan bizonyítjuk.

- A Singleton-korlát alapján $d \leq n - k + 1$, és ha 1. is teljesül, akkor $d = n - k + 1$.
- a $\mathbf{H}$ mátrixnak $n - k$ sora és n oszlopa van, így a rangja legfeljebb $n - k$, tehát bármely legalább $n - k + 1$, és ha 2. igaz, akkor bármely d oszlopa lineárisan összefüggő.
- Ez az előbbi pont alapján nyilvánvaló.
- Ha $\mathbf{H}$ bármely d oszlopa lineárisan összefüggő, akkor bármely $0 \leq i_0 < \cdots < i_{d-1} < n$ indexhez van olyan, nem csupa nulla $\mathbb{F}_q$-beli c_j együttható, amellyel $\sum_{j=0}^{d-1} c_j \tilde{\mathbf{h}}_{i_j} = \mathbf{0}$, ahol $\tilde{\mathbf{h}}_{i_j}$ az ellenőrző mátrix i_j-indexű oszlopa. Legyen $\mathbf{u} \in \mathbb{F}_q^n$ olyan, amelyben a megadott i_j indexekre $u_{i_j} = c_j$, és minden más l indexre $u_l = 0$. Ezzel az $\mathbf{u}$-val $\mathbf{Hu} = \mathbf{0}$, tehát $\mathbf{u} \in C$. Mivel $\mathbf{u}$ nem minden komponense 0, ezért $\mathbf{u} \neq \mathbf{0}$, és $\mathbf{u}$ kódszó, így $w(\mathbf{u}) \geq d$. Ugyanakkor $\mathbf{u}$ nem nulla komponenseinek száma legfeljebb d, így pontosan d, vagyis $\mathbf{u}$ olyan kódszó, amely a kiválasztott d pozíción, és csak ezeken a helyeken különbözik 0-tól.
- Ha valamely $\mathbf{G}$-re igaz 6., akkor a kód valamennyi generátormátrixára teljesül, hogy bármely $n - d + 1$ oszlopa lineárisan független. Ezen kívül elegendő megmutatni, hogy mondjuk $\mathbf{G}$ első $n - d + 1$ oszlopára teljesül az állítás, hiszen az oszlopcserékkel linerásian független oszlopok hasonló tulajdonságú oszlopokba mennek át, és ha egy kódban teljesül az előző állítás, akkor ez abban a kódban is igaz, amelyet az előbbiből az oszlopok permutációjával kapunk. Tekintsük most a kód azon – az előző pont alapján létező – $n - d + 1$ kódszavát, amelyek mindegyikében az utolsó $d - 1$ pozíción, valamint az első $n - d + 1$ hely kódszavanként különböző egyetlen helyén áll a nullától különböző elem, a további $n - d$ helyen pedig mindegyik kiválasztott kódszóban 0 áll. Mivel ezen kódszavak első $n - d + 1$ pozíciója – megfelelő sorrenddel – egy diagonálmátrix, ezért ezek a kódszavak lineárisan függetlenek, így a kód egy generátormátrixának sorai lehetnek, és ebben a mátrixban az első $n - d + 1$ oszlop lineárisan független.
- Ha 6. igaz, akkor 7. nyilvánvalóan teljesül.
- $\mathbf{G}$ sorai egy bázis elemei, tehát lineárisan függetlenek, és a számuk k, a mátrix rangja k. Ekkor a mátrix lineárisan független oszlopainak maximális száma is k, így, ha 7. teljesül egy kódban, akkor $k \geq n - d + 1$, azaz $d \geq n - k + 1$.

□

A 6.-ban megfogalmazott állítás azt jelenti, hogy maximális távolságú kód generátormátrixának bármely k oszlopa lineárisan független. Egy kódot akkor mondtunk valamely t pozíciójára nézve szeparábilisnak, ha $t = \lceil \log_q M \rceil$, ahol M a kód mérete, és ezen a t pozíción az alaphalmaz elemeiből álló minden lehetséges rendezett t-es legfeljebb egyszer fordul elő. Ekkor az eredeti üzeneteket beágyazhatjuk a kódba olymódon, hogy azonosítjuk őket a megfelelő részsorozattal. Ez viszont azt jelenti, hogy a kódszóban közvetlenül el tudjuk választani, el tudjuk szeparálni egymástól az üzenet jegyeit azoktól a jegyektől, amelyek a hibajavítást szolgálják, vagyis az ellenőrző jegyektől. Az előbbiek szerint MDS kódban bármely k pozíció lehet az üzenetjegyek helye, ez indokolja a kód nevében a szeparábilis jelzőt.

Az előző tételből közvetlenül kapjuk a következőt.

8.5. Tétel

A C lineáris kód akkor és csak akkor maximális távolságú, ha a duális kód is hasonló tulajdonságú.

Δ

Bizonyítás:
Lineáris kód generátormátrixa a duális kód ellenőrző mátrixa és fordítva, továbbá egy $[n,k]$-kód duálisa $[n,n-k]$-kód, és így a távolsága legfeljebb $n-(n-k)+1=k+1$. Ha C maximális távolságú, akkor generátormátrixában, tehát a duális kód ellenőrző mátixában bármely k oszlop lineárisan független, a duális kód távolsága így legalább $k+1$, és mivel ennél nagyobb nem lehet, ezért pontosan ennyi a távolsága, a duális kód is maximális távolságú. A szimmetria miatt visszafelé is hasonló a bizonyítás.

□

Most az MDS kódok más jellemzőit vizsgáljuk.

8.6. Tétel

Legyen az $[n,k]_q$-paraméterű C kód generátormátrixa $(\mathbf{I}_k\ \mathbf{A}^{(k,n-k)})$. C akkor és csak akkor maximális távolságú, ha **A** bármely kvadratikus részmátrixa reguláris.

Δ

Bizonyítás:
Bármely lineáris kód generátormátrixa ekvivalens átalakítással standard alakra hozható, ezért a **G**-re adott megkötés nem szűkíti az érintett kódok körét.

Legyen egy **A**-ból kiválasztott négyzetes részmátrix, **B**, s-méretű (ahol nyilván $k \geq s \in \mathbb{N}$). Sorcserével elérhető, hogy a **B** által meghatározott s sor a mátrix felső s sora legyen. A sorcserékkel $\mathbf{I}_k$ sorai is cserélődnek, de az továbbra is igaz lesz, hogy a sorcserékkel nyert mátrix első k oszlopának mindegyikében egyetlen helyen az egységelem, mindenütt másutt a nullelem áll, és különböző oszlopban álló egységelem a mátrix különböző sorához tartozik. Vegyük azt a $k-s$ oszlopot, amelyben az egységelem az alsó $k-s$ sor valamelyikében áll, és jelöljük az így keletkező $k-s$ méretű négyzetes mátrixot **T**-vel. Az előbbiek alapján az ugyanezen $k-s$ oszlop és a felső s sor részmátixa csupa nullelemből áll, ezért ezt $\mathbf{0}^{(s,k-s)}$-sel jelöljük. Oszlopcserékkel elérhetjük, hogy **B** oszlopai a mátrix első s oszlopába kerüljenek, és a **T** által meghatározott oszlopok következzenek olyan sorrendben, hogy az alsó $k-s$ sorban a $k-s$ méretű egységmátrix álljon; ekkor az ugyanezen oszlopokhoz tartozó felső s sorban továbbra is $\mathbf{0}^{(s,k-s)}$ áll, vagyis az átrendezés után keletkező $\mathbf{G}'$ mátrix a következő alakú:

$$\mathbf{G}' = \left(\begin{array}{cc|c} \mathbf{B} & \mathbf{0}^{(s,k-s)} & \mathbf{U} \\ \mathbf{X} & \mathbf{I}_{k-s} & \mathbf{V} \end{array}\right) = (\mathbf{C}\ \mathbf{D}),$$

ahol **C** az első k oszlopból álló négyzetes mátrix, vagyis a **B**-ből, **X**-ből, $\mathbf{0}^{(s,k-s)}$-ból és $\mathbf{I}_{k-s}$-ből álló részmátrix. **C** szerkezetéből látjuk, hogy $\det(\mathbf{C}) = \det(\mathbf{B})$, tehát **C** és **B** egyszerre szinguláris. Sorok és oszlopok sorrendjének változtatása a determináns abszolút értékét nem változtatja. **C** determinánsa viszont akkor és csak akkor 0, ha oszlopai, azaz **G** valamely k oszlopa lineárisan összefüggő. Más szavakkal ez azt jelenti, hogy amennyiben a kód maximális távolságú, tehát bármely k oszlop lineárisan független, akkor **A** bármely négyzetes részmátrixa reguláris, míg ha nem MDS, akkor van k lineárisan összefüggő oszlop **G**-ben, ez legalább egy oszlopot **A**-ból tartalmaz (hiszen **I** oszlopai lineárisan függetlenek), és akkor ez a k oszlop sor- és oszlopcserékkel a fenti alakú lesz, és a hozzá tartozó **B** szinguláris, vagyis **A** valamely kvadratikus részmátrixa nem reguláris.

□

8.7. Következmény

MDS-kód szisztematikus generátormátrixában az egységmátrixon kívüli elem nem nulla.

Δ

Bizonyítás:
Minden elem 1×1-es kvadratikus részmátrix, és ennek determinánsa maga a kiválasztott elem.

□

Az éppen bizonyított tételből korlátot kapunk egy MDS-kódban k lehetséges értékére.

8.8. Tétel

Nem triviális $[n,k]_q$-paraméterű MDS-kódban $2 \leq k \leq q-1$ és $n-q+1 \leq k \leq n-2$. Minden bináris MDS-kód triviális.

Δ

Bizonyítás:
Ekvivalens kódok távolsága azonos, ezért feltehetjük, hogy a kód generátormátrixa $(\mathbf{I}\ \mathbf{A})$ alakú, ahol **A** legfelső sorának minden eleme az egységelem: az előző következmény alapján **A** minden eleme nullától különbözik, és így van inverze, amivel a generátormátrix megfelelő oszlopát végigszorozva ekvivalens kódot kapunk. Feltettük, hogy a kód nem triviális, így $k \geq 2$, **G** tehát legalább két sorból áll. **A** minden sorában $n-k$ nem nulla elem van, és mivel a kód $q-1$ különböző nem nulla szimbólumból áll, ezért ha $n-k > q-1$, vagyis amennyiben $n-k \geq q$, akkor legalább egy nullától különböző szimbólum minimum kétszer szerepel **G** második sorának **A** által meghatározott részében. Legyen ez az elem u, és tekintsük az első sor $-u$-szorosának és a második sornak az összegét. Ez a **G** két sorának nem triviális lineáris kombinációja, tehát a kód nullától különböző eleme, és így a súlya legalább $n-k+1$. Ugyanakkor az utolsó $n-k$ oszlopban legalább két nullelem áll, míg az első k oszlopban (amit az egységmátrix határoz meg) pontosan két elem különbözik nullától, így a keletkezett kódszó súlya legfeljebb $n-k-2+2 = n-k$, ami ellentmond annak, hogy a kód maximális távolságú, és így szükségszerűen $n-k < q$, $n-q+1 \leq k$. Viszont ugyanezen meggondolás igaz a duális kódra is, hiszen MDS kód duálisa is maximális távolságú, így az előző egyenlőtlenségben k-t $n-k$-val helyettesítve is érvényes korlátot kapunk: $k \leq q-1$. Végül még azt kell tekintetbe venni, hogy definíció szerint nem triviális MDS kódban $2 \leq k \leq n-2$, így valóban fennáll a tételben felírt korlát.

Az előbbiek szerint nem triviális bináris MDS kódban $2 \leq k \leq 2-1 = 1$, ami lehetetlen.

□

Belátjuk, hogy ha létezik $[n,k]_q$-paraméterű MDS-kód, akkor tetszőleges $n-k \geq t \in \mathbb{N}$-re létezik $[n-t,k]_q$, illetve minden $k > t \in \mathbb{N}$ -re $[n-t,k-t]_q$-paraméterű MDS-kód.

8.9. Tétel

$[n,k]_q$-paraméterű MDS-kódot bármely $t \leq n-k$ helyen átszúrva $[n-t,k]_q$, illetve tetszőleges, $t < k$ pozíción 0-ra rövidítve $[n-t,k-t]_q$-paraméterű MDS-kódot kapunk.

Δ

Bizonyítás:
a) C távolsága $n-k+1$, és bármely $n-k+1$ pozícióhoz van olyan kódszó, amely ezeken és csak ezeken a pozíciókon nem nulla. Ha ebből az $n-k+1$ pozícióból ennél kevesebb t komponenst elhagyunk, akkor egyrészt továbbra is bármely két szó legalább $n-k+1-t > 0$ helyen eltér, másrészt lesz olyan szó, amelynek a súlya az előbbi érték, tehát a nyert kód hossza $n' = n-t$, elemeinek száma továbbra is q^k, így dimenziója $k' = k$, és a távolsága $d' = n-k+1-t = n'-k'+1$, azaz az új kód is maximális távolságú.

b) MDS-kódban nem lehet olyan pozíció, amelyen a kód valamennyi eleme 0, ugyanis ellenkező esetben ezt a pozíciót elhagyva a hossz csökkenne, de a dimenzió és a távolság változatlan maradna, ami lehetetlen, hiszen így megsértenénk a Singleton-korlátot. Ebből viszont következik, hogy minden pozíción az alaptest minden eleme ugyanannyiszor szerepel, így ha csak azokat a szavakat tartjuk meg, amelyeknél egy kijelölt pozíción 0 áll, akkor a kódszavak száma a q-adrészére csökken, és mivel a kód továbbra is lineáris, ezért ez azt jelenti, hogy k eggyel csökkent, tehát $n' = n - 1$, $k' = k - 1$. Rövidítésnél a távolság nem csökken, $d' \geq d$, ugyanakkor $d' \leq n' - k' + 1 = n - k + 1 = d$, tehát $d' = d$, és ismét MDS-kódunk lesz. Innen indukcióval kapjuk a tételbeli állítást.

□

A legfontosabb kérdésre még nem válaszoltunk: létezik-e egyáltalán a triviálistól különböző maximális távolságú kód. A későbbiekben egy gyakorlatilag is fontos kódról látjuk, hogy MDS kód. Most megmutatjuk, hogy adott q prímhatvány esetén minden $1 \leq k \leq n \leq q + 1$ feltételt kielégítő esetben létezik $[n, k]_q$-paraméterű maximális távolságú kód.

8.10. Tétel

Ha q prímhatvány, és k, n olyan természetes számok, hogy $1 \leq k \leq n \leq q + 1$, akkor van $[n, k]_q$-paraméterű (nem feltétlenül nem triviális) maximális távolságú kód.

Δ

Bizonyítás:

Soroljuk fel $\mathbb{F}_q$ elemeit valamilyen sorrendben, azaz legyen $\mathbb{F}_q = \{a_i | q > i \in \mathbb{N}\}$, és nézzük azt a $k \times (q + 1)$-méretű, $\mathbb{F}_q$ fölötti **A** mátrixot, amelyben a $0 \leq i < k$ és $0 \leq j < q$ indexekre $A_{i,j} = a_j^i$, míg az utolsó oszlop minden eleme nulla, az utolsó kivételével, amely tetszőleges nem nulla elem, tehát például az egységelem lehet (vagyis $A_{i,q} = \delta_{i,k-1} e$). Ebben a mátrixban az első q oszlopból bármely k Vandermonde-típusú mátrixot alkot, és az egyes oszlopok generátoreleme páronként különböző, így ezek az oszlopok lineárisan függetlenek, hiszen a megfelelő mátrix determinánsa nem nulla. Ha viszont az utolsó oszlophoz választunk $k - 1$ oszlopot, akkor az így keletkező kvadratikus mátrix determinánsa előjeltől eltekintve megegyezik a $k - 1$ oszlop első $k - 1$ sorához tartozó négyzetes részmátrix determinánsával, és ez ismét páronként különböző elemekkel generált Vandermonde-determináns, így ez a k oszlop is lineárisan független. Ebből következik, hogy amennyiben **A** tetszőleges n oszlopát egy $[n, k]_q$ kód **G** generátormátrixának tekintjük, akkor **G** bármely k oszlopa lineárisan független, tehát a generált kód maximális távolságú.

□

MDS-kódok dekódolása többek között többségi alapon történhet. Az alább ismertetett dekódolási eljárás egyúttal példát mutat arra, hogy hogyan lehet dekódolni abban az esetben, amikor a hibák egy részének a helyét ismerjük. Emlékeztetünk rá, hogy egy d-távolságú kód minimális távolságú dekódolással biztosan helyesen javít, ha $2t + r \leq d - 1$, ahol r azon hibák száma, amelyeknek ismerjük a helyét, és a hibák teljes száma $t + r$.

Tekintsünk egy $l \times m$ méretű, l-rangú **A** mátrixot, ahol $m \geq l$, és legyen $\mathbf{b}^T = \mathbf{a}^T \mathbf{A}$, ahol **a** egy l-komponensű vektor. Ha most $0 \leq i_0 < \cdots < i_{l-1} < m$ olyan indexek, amelyekhez tartozó **A**-beli oszlopok lineárisan függetlenek, I az előbbi indexek halmaza, és $\mathbf{A}^{(I)}$ az a mátrix, amely **A**-nak az I-beli indexekhez tartozó oszlopaiból áll, valamint $\mathbf{b}^{(I)}$ a **b**-ből hasonlóan nyert vektor, akkor az ${\mathbf{A}^{(I)}}^T \mathbf{x} = \mathbf{b}^{(I)}$ egyenletrendszernek pontosan egy megoldása van, hiszen $\mathbf{A}^{(I)}$ reguláris, és ez a megoldás nem lehet más, mint **a**. Ha viszont **c** a $\mathbf{b}^{(I)}$-től különböző l-méretű vektor, akkor az ${\mathbf{A}^{(I)}}^T \mathbf{x} = \mathbf{c}$ egyenletrendszer egyértelmű megoldása nem lehet **a**. Végül, ha **B** az **A** lineárisan független, l-nél kevesebb, l' oszlopát tartalmazó részmátrixa, akkor tetszőleges l'-méretű **z** vektorral a $\mathbf{B}^T \mathbf{x} = \mathbf{z}$ egyenletrendszernek egynél több megoldása van.

Hibakorlátozás

Most legyen $\mathbf{G}$ egy $[n, k]$-paraméterű MDS-kód generátormátrixa, és $\mathbf{v}$ egy vett szó, amelyben $t + r$-számú hiba van, amelyek közül r-nek ismerjük a helyét. Legyenek az ismert hibahelyek indexei $0 \leq i_0 < \cdots < i_{r-1} < n$, ezen indexek halmaza I, és $\mathbf{G}^{(I)}$ az a mátrix, amelyet $\mathbf{G}$-ből az I-beli indexekhez tartozó oszlopok törlésével kapunk, ekkor $\mathbf{G}^{(I)}$ egy $k \times (n - r)$-méretű mátrix, és $\mathbf{v}^{(I)}$, amelyet $\mathbf{v}$-ből az I-beli indexekhez tartozó komponensek törlésével kapunk, egy $n - r$-méretű vektor. $\mathbf{G}$-ben bármely k oszlop, tehát akkor bármely legfeljebb k oszlop lineárisan független, és ez nyilván igaz lesz $\mathbf{G}^{(I)}$-re is, hiszen ez az eredeti mátrixból oszlopok elhagyásával keletkezett. Ha $n - r < k$, akkor tehát $\mathbf{G}^{(I)}$ oszlopai lineárisan függetlenek, és a ${\mathbf{G}^{(I)}}^T \mathbf{x} = \mathbf{v}^{(I)}$ egyenletrendszernek egynél több megoldása van, vagyis ekkor a dekódolás nem végezhető el. Ebből következik, hogy egyértelmű dekódoláshoz szükséges az $n - r \geq k$ feltétel, vagy másként írva $r \leq n - k = d - 1$. A továbbiakban feltesszük, hogy ez a feltétel teljesül. Legyen J azon indexek halmaza, amely pozíciókon a t-számú további hiba van (természetesen ezeket az indexeket nem ismerjük, de attól még léteznek). Nyilván igaz, hogy I és J diszjunkt halmazok. Legyen még T az n-nél kisebb nemnegatív egész számok halmaza és S a $T \setminus I$ halmaz egy k-elemű részhalmaza. Mivel $\mathbf{G}$ bármely k oszlopa lineárisan független, ezért $\mathbf{G}$-nek az S-beli indexekhez tartozó oszlopaiból álló $\mathbf{G}^{[S]}$ részmátrixa reguláris, és így a ${\mathbf{G}^{[S]}}^T \mathbf{x} = \mathbf{v}^{[S]}$ egyenletrendszernek is van egy és csak egy megoldása, ahol $\mathbf{v}^{[S]}$ a $\mathbf{v}$-nek az S-beli indexekhez tartozó komponenseiből álló vektor. Ha $S \subseteq (T \setminus I) \setminus J$, akkor a megoldásként kapott $\mathbf{c}$ vektor az eredeti üzenet, míg ha $S \cap J \neq \emptyset$, akkor a megoldás biztosan különbözik az eredeti $\mathbf{c}$ üzenettől. Az első eset csak úgy lehetséges, ha $k = |S| \leq |(T \setminus I) \setminus J| = (n - r) - t = n - (t + r)$, azaz ha $t + r \leq n - k = d - 1$, vagyis hibátlan dekódolás is csak ilyen feltétel teljesülése esetén várható. Ekkor $\binom{n-(t+r)}{k}$ olyan k egyenletből álló egyenletrendszer van, amelynek a megoldása a $\mathbf{c}$ üzenet, és bármely más k egyenletből álló egyenletrendszer megoldása ettől különböző. Most tegyük fel, hogy $S \cap J \neq \emptyset$, kérdés, hogy hány olyan egyenletrendszer van, amelynek a megoldása megegyezik az ezen S indexhalmazhoz tartozó egyenletrendszer megoldásával. Ha S_1 és S_2 két olyan, k elemből álló indexhalmaz, hogy a két indexhalmazhoz tartozó egyenletrendszer megoldása azonos, akkor az $S_1 \cup S_2$ indexhalmazhoz tartozó bármely k egyenlet megoldása is az előbbivel megegyező megoldás. Legyen tehát S' a legbővebb olyan indexhalmaz, amelyből vett tetszőleges k egyenlet megoldása azonos az előbb megadott S indexhalmazhoz tartozó megoldással. S' a J bármely elemét tartalmazhatja, ám $(T \setminus I) \setminus J$ -ből legfeljebb csak $k - 1$ elemet, ugyanis ha $|S' \cap ((T \setminus I) \setminus J)| \geq k$, akkor S'-ből kiválasztható k olyan index, amely a hibátlan helyekhez tartozik, és amely által meghatározott egyenletrendszernek a megoldása $\mathbf{c}$ lenne. Ebből következik, hogy $|S'| \leq t + k - 1$, és akkor azon k-egyenletből álló egyenletrendszerek száma, amelyek megoldása megegyezik az S indexhalmazhoz tartozó egyenletekből álló egyenletrendszer megoldásával, legfeljebb $\binom{t+k-1}{k}$. Ha tehát $\binom{n-(t+r)}{k} > \binom{t+k-1}{k}$, vagyis ha $n - (t + r) > t + k - 1$, akkor a $T \setminus I$ indexhalmaz minden k-elemű S részhalmazához tartozó egyenletrendszert megoldva, a helyes megoldást kapjuk a legtöbbször, vagyis ez lesz a dekódolás eredménye. Az előbbi egyenletrendszer alapján ennek az a feltétele, hogy $2t + r \leq d - 1$. Ezen túl még valami megállapítható az eddigi eredményekből. Ha $2t + r \leq d - 1$, akkor

$$n - (t + r) \geq n - \left(\frac{d - 1 - r}{2} + r\right) = \frac{2n - (d - 1) + r - 2r}{2} = \frac{n + k - r}{2},$$

vagyis kell, hogy legyen legalább $\binom{\frac{n+k-r}{2}}{k}$ olyan egyenletrendszer, amelyeknek a megoldása azonos. Ha ez a feltétel nem teljesül, akkor $2t + r > d - 1$, és a helyes javítás nem garantálható.

9. Hamming-kódok

Ebben a részben olyan lineáris kódokat vizsgálunk, amelyek egy hibát javítanak. Ilyen kódot akkor célszerű használni, ha a hibák egymástól függetlenül jelentkeznek, és a hiba valószínűsége lényegesen kisebb a kódszavak hosszának reciprokánál, ekkor ugyanis egy-egy kódszóban legfeljebb egy hiba várható.

Mivel minimális távolságú dekódolás esetén a maximálisan javítható hibaszám $d-1$ felének egészrésze, ezért most d értéke legalább három kell, hogy legyen. Nézzünk egy $[n,k,d]_q$ kódot. A Singleton-korlát alapján $k \leq n-d+1$, és természetesen $k \geq 1$ (hiszen ha $k=0$, akkor a kód egyetlen elemből áll, ami a linearitással együtt éppen a 0), így ha $d=3$, akkor $n \geq k+2 \geq 3$, és ha bevezetjük az $r=n-k$ jelölést, akkor $r \geq 2$. Mivel $[n,k]$-kódban k komponens szükséges az üzenet kódolásához, ezért r az ellenőrző jegyek száma.

Egy lineáris kód akkor egy-hiba javító, ha az ellenőrző mátrix bármely két különböző oszlopa lineárisan független, és pontosan egy hibát javító, ha ezen túl az is teljesül, hogy van három, páronként különböző, lineárisan összefüggő oszlop a $\mathbf{H}$ ellenőrző mátrixban. Adott r-hez keressünk maximális, 3-távolságú, lineáris kódot. Ehhez k, és $k=n-r$ következtében n maximumát kell meghatározni. A feladat tehát az, hogy keressünk $V_q^{(r)}$-ben maximális olyan részhalmazt, amelyben bármely két különböző vektor lineárisan független.

Legyen $2 \leq r \in \mathbb{N}$, és $A \subseteq V_q^{(r)}$ egy ilyen maximális részhalmaz. q és r végessége, valamint $V_q^{(r)} \cong \mathbb{F}_q^{(r)}$ következtében $\left|V_q^{(r)}\right| = q^r$ véges, és véges halmaznak bármilyen tulajdonságra nézve létezik maximális részhalmaza, így A létezik. $V_q^{(r)}$ r-dimenziós tér, így van r-elemű bázisa, és bázis elemei páronként lineárisan függetlenek, ezért A legalább r elemet tartalmaz, A nem üres. Ugyanakkor a $V_q^{(r)}$ tetszőleges nem nulla $\mathbf{u}$ vektorával $e \cdot \mathbf{0} + 0 \cdot \mathbf{u} = \mathbf{0}$ (e az $\mathbb{F}_q$ egységeleme, 0 a test nulleleme), és a bal oldal a $\mathbf{0}$ és $\mathbf{u}$ vektorok nem triviális lineáris kombinációja, ezért a nullvektor nem lehet eleme A-nak, így A a $V_q^{(r)} \setminus \{\mathbf{0}\}$ nem üres részhalmaza. A továbbiakban $V_q^{(r)} \setminus \{\mathbf{0}\}$-t $V_q^{(r)^*}$-gal jelöljük.

Tekintsük a $V_q^{(r)^*} \times V_q^{(r)^*}$ halmazon az alábbi $\sim$ relációt: $\mathbf{u} \in V_q^{(r)^*}$ és $\mathbf{v} \in V_q^{(r)^*}$-ra $\mathbf{u} \sim \mathbf{v}$ akkor és csak akkor, ha van olyan $\mathbb{F}_q$-beli λ, hogy $\mathbf{v} = \lambda \cdot \mathbf{u}$. Mivel $\mathbf{v} \in V_q^{(r)^*}$, így $\mathbf{v} \neq \mathbf{0}$, tehát λ sem lehet 0, $\lambda \in \mathbb{F}_q^*$. A $\sim$ reláció ekvivalencia-reláció $V_q^{(r)^*}$-on. Először is a definíció alapján $\sim$ homogén binér reláció $V_q^{(r)^*}$-on. Tetszőleges $\mathbf{u} \in V_q^{(r)^*}$-ra $\mathbf{u} = e \cdot \mathbf{u}$, ahol e az $\mathbb{F}_q$ egységeleme, így $\sim$ reflexív; ha $\mathbf{u} \sim \mathbf{v}$, akkor alkalmas $\lambda \in \mathbb{F}_q^*$-gal $\mathbf{v} = \lambda \cdot \mathbf{u}$, de $\lambda \neq 0$ következtében létezik a szintén $\mathbb{F}_q^*$-beli, és így $\mathbb{F}_q$-beli λ^{-1}, amellyel $\mathbf{u} = \lambda^{-1} \cdot \mathbf{v}$, a reláció szimmetrikus; végül ha $\mathbf{w} \in V_q^{(r)^*}$ egy harmadik (az előbbi kettőtől nem feltétlenül különböző) vektor úgy, hogy $\mathbf{u} \sim \mathbf{v}$ és $\mathbf{v} \sim \mathbf{w}$, akkor van olyan $\mathbb{F}_q$-beli λ és μ, hogy $\mathbf{v} = \lambda \cdot \mathbf{u}$ és $\mathbf{w} = \mu \cdot \mathbf{v}$, azaz $\mathbf{w} = \mu \cdot (\lambda \cdot \mathbf{u}) = (\lambda\mu) \cdot \mathbf{u} = \nu \cdot \mathbf{u}$, és $\nu = \lambda\mu \in \mathbb{F}_q$, $\mathbf{u} \sim \mathbf{w}$, a reláció tranzitív is. Ekkor $\sim$ egy osztályozást határoz meg $V_q^{(r)^*}$-on: ha $V_q^{(r)^*}$-ra $T_u = \left\{\mathbf{v} \in V_q^{(r)^*} \middle| \mathbf{u} \sim \mathbf{v}\right\}$, akkor az ilyen halmazok egyike sem üres, az uniójuk lefedi $V_q^{(r)^*}$-ot, és közülük bármely kettő vagy azonos, vagy idegen. Mivel $\mathbf{v}$ akkor és csak akkor eleme T_u-nak, ha $\mathbf{v} = \lambda \cdot \mathbf{u}$ egy $\mathbb{F}_q^*$-ból vett λ-val, ezért T_u elemeinek száma legfeljebb $\left|\mathbb{F}_q^*\right| = q-1$, másrészről T_u két eleme, $\mathbf{v}_1 = \lambda_1 \cdot \mathbf{u}$ és $\mathbf{v}_2 = \lambda_2 \cdot \mathbf{u}$ akkor és csak akkor egyenlő, ha $(\lambda_1 - \lambda_2)\mathbf{u} = \mathbf{0}$, ami pontosan akkor teljesül, ha $\lambda_1 - \lambda_2 = 0$, azaz ha $\lambda_1 = \lambda_2$ (mert $\mathbf{u} \neq \mathbf{0}$), ami mutatja, hogy T_u-nak $\mathbf{u}$-tól függetlenül $q-1$ eleme van. Ebből, és abból, hogy $\left|V_q^{(r)^*}\right| = \left|V_q^{(r)}\right| - 1 = q^r - 1$, viszont kapjuk, hogy az osztályok száma, és így bármely reprezentánsrendszer számossága $\frac{q^r-1}{q-1}$.

$V_q^{(r)^*}$ valamely két vektora, $\mathbf{u}$ és $\mathbf{v}$ akkor és csak akkor lineárisan összefüggő, ha azonos osztályban vannak: ha $\lambda\mathbf{u} + \mu\mathbf{v} = \mathbf{0}$ az $\mathbb{F}_q^*$-beli λ-val és $\mathbb{F}_q$-beli μ-vel (tehát egy nem triviális kombinációról

van szó), akkor $\mathbf{u} = (-\lambda^{-1}\mu) \cdot \mathbf{v} = \nu \cdot \mathbf{v}$, és ν is eleme $\mathbb{F}_q$-nak, így $\mathbf{v} \in T_u$, míg a fordított esetben, vagyis ha $\mathbf{v} \in T_u$, akkor $\mathbf{v} = \tau \cdot \mathbf{u}$, ahol $\tau \in \mathbb{F}_q$, és ebből $(-\tau)\mathbf{u} + e\mathbf{v} = \mathbf{0}$, vagyis $\mathbf{u}$ és $\mathbf{v}$ lineárisan összefüggő vektorok (hiszen e és $-\tau$ eleme az alaptestnek, és $e \neq 0$, vagyis az előbbi összeg egy nem triviális lineáris kombinációja a két vektornak).

Legyen $\frac{q^r-1}{q-1} = n$, ekkor $n = \frac{q^r-1}{q-1} = \sum_{i=0}^{r-1} q^i \geq 1 + q \geq 1 + 2 = 3$. Ha R egy reprezentánsrendszer a korábbi ~relációra, akkor R elemeinek száma n, és az előbbi egyenlőtlenség alapján ez a szám legalább három. Azt már tudjuk, hogy R bármely két különböző eleme lineárisan független, míg az azonos osztályban lévő vektorok lineárisan összefüggőek. Válasszunk két reprezentánst, **u**-t, valamint az **u**-tól különböző **v**-t. $\mathbf{z} = \mathbf{u} + \mathbf{v} = \lambda \cdot \mathbf{u}$ ekvivalens a $\mathbf{v} = (\lambda - e) \cdot \mathbf{u} = \mu \cdot \mathbf{u}$ egyenlőséggel, ami **u** és **v** választása folytán még $\lambda = 0$ mellett is lehetetlen, így a **z** összegvektor nem a nullvektor, és sem T_u-nak, sem T_v-nek nem eleme. Ebből az következik, hogy van olyan, mind **u**-tól, mind **v**-től különböző **w** vektor R-ben, amellyel $\mathbf{u} + \mathbf{v} = \lambda \cdot \mathbf{w}$ (mert az osztályok együttesen lefedik a nullától különböző vektorok halmazát), vagyis létezik R-ben három, páronként különböző, lineárisan összefüggő vektor. Ebből látjuk, hogy A-nak választhatjuk az R halmazt.

Jelöljük R elemeit $\mathbf{h}_i$-vel, ahol $n \geq i \in \mathbb{N}^+$, és legyen **H** az az $r \times n$-es $\mathbb{F}_q$ fölötti mátrix, amelynek i-edik oszlopa éppen $\mathbf{h}_i$. **H** sorai lineárisan függetlenek. Valóban: minden $r > t \in \mathbb{N}$-re lesz olyan $n \geq i_t \in \mathbb{N}^+$, hogy $\mathbf{h}_{i_t}$-ben a t-edik és csak a t-edik komponens különbözik nullától, hiszen az ilyen vektorok biztosan páronként függetlenek. Ekkor van **H**-ban r lineárisan független oszlop, de akkor van ugyanennyi lineárisan független sor is. Ez viszont azt jelenti, hogy **H** egy $[n, n-r]_q$-kód ellenőrző mátrixa. Ha $C \leq V_q^{(n)}$ az a kód, amelyet $C = \left\{\mathbf{u} \in V_q^{(n)} \middle| \mathbf{Hu} = \mathbf{0}\right\}$ definiál, akkor a kód paritásellenőrző mátrixának bármely két, különböző indexhez tartozó oszlopa lineárisan független, ugyanakkor létezik három olyan, páronként különböző oszlop, amelyek lineárisan nem függetlenek, így $d(C) = 3$, C egy $[n, n-r, 3]_q$-paraméterű kód, ahol $n = \frac{q^r-1}{q-1}$, és az adott r-hez nem lehet n-nél nagyobb hosszúságú, a minimális távolságú dekódolással legalább egy hibát javító lineáris kódot konstruálni.

9.1. Definíció

$2 \leq r \in \mathbb{N}$ esetén az r ellenőrző jeggyel konstruált, $\mathbb{F}_q$ fölötti, legalább egy hibát javító, maximális hosszúságú lineáris kód az **r-paraméterű q-áris Hamming-kód**.

Δ

9.2. Tétel

Egy $[n, k]_q$-paraméterű kód pontosan akkor Hamming-kód, ha $n = \frac{q^r-1}{q-1}$ és $k = n - r$, ahol $2 \leq r \in \mathbb{N}$. A Hamming-kód pontosan egy hibát javító kód.

Δ

Bizonyítás:
Az előbbi definíció előtti részben bizonyítottuk a tételt.

□

9.3. Tétel

$\mathbb{F}_q$ fölött azonos hosszúságú Hamming-kódok skalárekvivalensek. A Hamming-kód tökéletes.

Δ

Bizonyítás:

1. A lineáris kódot meghatározza az ellenőrző mátrixa. $\mathbb{F}_q$ fölötti bármely két Hamming-kód ellenőrző mátrixának oszlopai a kód konstrukciójának következtében csak sorrendben és egy – oszloponként esetleg más és más – nem nulla $\mathbb{F}_q$-beli szorzóban különbözhetnek. Ekkor ez igaz a generátormátrixra, és így a teljes kódra is, márpedig éppen ez a skalárekvivalencia definíciója.

2. Legyen C egy $[n,k]$-paraméterű q-áris Hamming-kód, ekkor $n=\frac{q^r-1}{q-1}$ és $k=n-r$ alkalmas r pozitív egésszel, és a kód távolsága $d=3$. A kód elemeinek száma $M=q^k=q^{n-r}$. Ezekkel az adatokkal $M\cdot V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right)=M\cdot V_q(n,1)=q^{n-r}\sum_{i=0}^{1}\binom{n}{i}(q-1)^i=q^{n-r}\big(1+n\cdot(q-1)\big)$. n-et az r-rel való megadásával helyettesítve $n\cdot(q-1)=\frac{q^r-1}{q-1}(q-1)=q^r-1$, és ezzel az előző egyenletből $M\cdot V_q\left(n,\left\lfloor\frac{d-1}{2}\right\rfloor\right)=q^{n-r}\big(1+n\cdot(q-1)\big)=q^{n-r}\big(1+(q^r-1)\big)=q^{n-r}q^r=q^n$, ami mutatja, hogy a Hamming-kód valóban tökéletes.

□

Az előbbi tételből következik, hogy nem csak a lineáris kódok, de tetszőleges kódok között is a Hamming-kód biztosítja *r* ellenőrző jeggyel a legbővebb, legalább egy hibát javító kódot.

Most nézzük meg, hogyan lehet Hamming-kód esetén dekódolni. Látni fogjuk, hogy ez **H** alkalmas választása esetén rendkívül egyszerű feladat.

Legyen $\mathbf{u}$ egy ekvivalenciaosztály reprezentánsa. Tudjuk, hogy $\mathbf{u}$ nem a nullvektor. Ekkor van olyan egyértelműen meghatározott t index, hogy $r>t\in\mathbb{N}$ és $u_t\neq 0$, de minden $t<i<r$ indexre $u_i=0$. Mivel az osztály minden eleme $\mathbf{u}$ egy nem nulla konstansszorosa, ezért ez a tulajdonság az osztály valamennyi elemére érvényes. $u_t\neq 0$, ezért van inverze, és $\mathbf{u}$-t ezzel az inverzzel szorozva olyan $\mathbf{v}$ vektort kapunk, amelyben $v_t=e$, és az előbbieknek megfelelően $t<i<r$-re $v_i=0$. A továbbiakban legyen az így meghatározott $\mathbf{v}$ az osztály reprezentánsa, így ez lesz a **H** valamely oszlopa, mondjuk $\tilde{\mathbf{h}}_i$. Nyilvánvaló, hogy kölcsönösen egyértelműen tudjuk a $\tilde{\mathbf{h}}_i$ oszlopokat és az i indexeket egymásnak megfeleltetni.

Tegyük fel, hogy $\mathbf{u}\in C$ és $\mathbf{v}=\mathbf{u}+\boldsymbol{\varepsilon}$, ahol $\boldsymbol{\varepsilon}$ egy $V_q^{(r)}$-beli olyan vektor, amelynek a súlya 1, vagyis $w(\boldsymbol{\varepsilon})=1$, tehát $\boldsymbol{\varepsilon}$-nak pontosan egy komponense különbözik 0-tól. Legyen ez az l indexhez tartozó komponens, és legyen az értéke α, vagyis $\varepsilon_l=\alpha\in\mathbb{F}_q^*$, és az l-től különböző $n\geq i\in\mathbb{N}^+$ indexre $\varepsilon_i=0$. Most $\mathbf{s}=\mathbf{H}\mathbf{v}=\mathbf{H}\boldsymbol{\varepsilon}=\alpha\tilde{\mathbf{h}}_l$, ahol $\mathbf{s}$ a szindróma, vagyis az ismert $\mathbf{v}$-ből számítható $\mathbf{s}$ szindróma a **H** mátrix valamelyik (egyelőre ismeretlen) indexű oszlopának nem nulla konstansszorosa. Ha $\tilde{\mathbf{h}}_l$-ben a t-indexű komponens nem nulla, de minden t-nél nagyobb indexhez tartozó komponens nullával egyenlő, akkor ez igaz lesz $\alpha\tilde{\mathbf{h}}_l$-ben is (mert $\alpha\neq 0$), továbbá a $\tilde{\mathbf{h}}_l$ választása folytán a t-indexű komponens értéke e, tehát $s_t=\alpha$, ami azt jelenti, hogy megkaptuk a hiba értékét. α ismeretében $\tilde{\mathbf{h}}_l$-et is megkapjuk. $\tilde{\mathbf{h}}_l=\alpha^{-1}\mathbf{s}$, és a $\tilde{\mathbf{h}}_i$ és i közötti kölcsönösen egyértelmű meghatározottság alapján l-et is megállapíthatjuk. l és α együttes ismeretében a hiba javítható: az l-től különböző indexekre $u_i=v_i$, míg $u_l=v_l-\alpha$.

H bármely két, különböző indexhez tartozó oszlopának minden, nullától különböző együtthatókkal vett lineáris kombinációja a mátrix valamely, az előző kettőtől különböző oszlopának nem nulla konstansszorosa, így ha pontosan két hiba lép fel az átvitel során, akkor azt úgy érzékeljük, hogy volt hiba, de a megállapított hibahely biztosan különbözik mindkét eredeti hibahelytől, így „javítás" után három hiba lesz a korrigált szóban. Ha a vett szóban három hiba volt, akkor a páronként különböző i, j és l indexszel és nullától különböző α_1, α_2 és α_3 együtthatókkal $\mathbf{s}=\alpha_1\tilde{\mathbf{h}}_i+\alpha_2\tilde{\mathbf{h}}_j+\alpha_3\tilde{\mathbf{h}}_l=\alpha\tilde{\mathbf{h}}_t$. **H**-ban van három lineárisan összefüggő oszlop, így előfordulhat, hogy $\mathbf{s}=\mathbf{0}$, nem érzékeljük a hibát, azt gondoljuk, hogy hibátlan volt az átvitel. Lehetséges, hogy t azonos i, j és l valamelyikével (és csak az egyikkel, hiszen ez a három index páronként különböző), mondjuk i-vel. Ekkor $\alpha\neq\alpha_1$, mert $\tilde{\mathbf{h}}_j$ és $\tilde{\mathbf{h}}_l$ lineárisan független, így ismét nem történik javítás, továbbra is három hiba lesz a "javított" szóban (ez bináris esetben nyilván nem lehetséges). Amennyiben viszont $\alpha\neq 0$, és t különbözik mindhárom hibahelytől, akkor a beavatkozás után négy hiba lesz az új szóban.

Hibakorlátozás

Az előző bekezdésben tárgyalt esetek nyilvánvalóak: a Hamming-kód tökéletes, és korábban beláttuk, hogy d-távolságú tökéletes kód pontosan a $\left\lfloor \frac{d-1}{2} \right\rfloor$-nél nem nagyobb súlyú hibamintákat javítja, vagyis a 3-távolságú Hamming-kódok esetén az egyetlen hibát tartalmazó szavakat.

Bináris esetben különösen egyszerű szerkezetű a paritásellenőrző mátrix és könnyű a javítás. Most minden ekvivalenciaosztály pontosan egy vektort tartalmaz, és $\mathbf{H}$ oszlopai az $n \geq i \in \mathbb{N}^+$ egészek kettes számrendszerben adott felírásai, továbbá rendezhetjük őket olyan sorrendben is, hogy az i-edik oszlopban álló szám értéke éppen i legyen (az oszlopokat 1-től indexelve). Mivel a hiba értéke is csupán 1 lehet, a szindróma mint egy binárisan felírt szám, közvetlenül megadja a hiba helyét.

Nézzünk egy példát. Legyen $q = 2$ és $n = 7$, ekkor $k = 4$ és $\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$. $\mathbf{H}$ sorai lineárisan függetlenek: a számuk három, és $\mathbf{H}$ 1., 2. és 4. oszlopa lineárisan független. Két vektor akkor és csak akkor lineárisan összefüggő, ha egyik a másiknak konstansszorosa, ami $\mathbb{F}_2$ felett azt jelenti, hogy vagy megegyeznek, vagy egyikük a $\mathbf{0}$-vektor, márpedig $\mathbf{H}$-ra egyik feltétel sem teljesül, bármely két oszlop $\mathbf{H}$-ban lineárisan független, a távolság legalább 3. Viszont $\mathbf{H}$ első három oszlopának összege a nullvektor, van három lineárisan összefüggő oszlop, így a kód távolsága pontosan 3, a kód egy hiba javítására alkalmas. Tegyük fel, hogy $\mathbf{c}^T = c_1 \dots c_7$ kódszó, ekkor $\mathbf{Hc} = \mathbf{0}$. Ha átvitelnél egyetlen hiba lép fel, mondjuk az m-edik pozícióban, akkor a vételnél $\mathbf{c}$ helyett egy $\mathbf{c'}$ vektort kapunk, amely $\mathbf{c}$ és $\boldsymbol{\varepsilon}^T = \underbrace{0 \dots 0}_{m-1} 1 \underbrace{0 \dots 0}_{n-m}$ összegének tekinthető. Most $\mathbf{Hc'} = \mathbf{Hc} + \mathbf{H\varepsilon} = \mathbf{H\varepsilon}$, hiszen az első tag $\mathbf{0}$. $\boldsymbol{\varepsilon}$ minden pozíciójában 0 áll az m-ediktől eltekintve, ahol viszont 1 található, ezért $\mathbf{H\varepsilon}$ a $\mathbf{H}$ m-edik oszlopát adja. Figyelmesen megnézve $\mathbf{H}$ oszlopait látható, hogy azokat mint 2-es számrendszerbeli számot olvasva (felül áll a legalacsonyabb helyiértékhez tarozó jegy) éppen az oszlop indexét kapjuk (1-től 7-ig számozva), azaz $\mathbf{Hc'}$ ilyen olvasata pontosan a hiba helyének indexét adja. A javítás tehát abból áll, hogy a $\mathbf{Hc'}$ által meghatározott indexhez tartozó pozícióban a bitet az ellentettjére módosítjuk ($\mathbb{F}_2$ esetén a hiba azt jelenti, hogy 0 helyett 1, 1 helyett 0 áll). Kevés munkával ellenőrizhető, hogy pontosan 2 hiba esetén $\mathbf{Hc'}$ biztosan nem 0 (hiszen bármely két oszlop lineárisan független), és olyan indexet ad, amely különbözik mindkét hiba helyétől, ezért most "javítás" után három hibánk lesz. Ha viszont $\mathbf{c'}$-ben legalább 3 hiba van, akkor lehet, hogy $\mathbf{Hc'} = \mathbf{0}$ (például ha az első három bit és csak ez hibásodik meg), így azt hisszük, hogy nem volt hiba, és lehet, hogy $\mathbf{Hc'} \neq \mathbf{0}$, és ekkor egy addig hibátlan bitet javítunk, amikor a hibák száma nő. Könnyen beláthatóan – mert a kód bináris – most nem fordulhat elő, hogy javításkor valamelyik hibás bitet javítjuk, amikor a hibák száma eggyel csökkenne, de még mindig hibás lenne az adat (viszont mi azt hinnénk, hogy már hibátlan). Ez a kód a [7,4]-paraméterű **bináris Hamming-kód**. A későbbiek kedvéért megmutatjuk, hogy ez a kód nem ciklikus. Legyen $\mathbf{c}^T = 1110000$, ekkor $\mathbf{Hc} = \mathbf{0}$, $\mathbf{c}$ tehát eleme a kódnak. Ugyanakkor az egy pozícióval való ciklikus jobbraléptetéssel kapott $\mathbf{c'}^T = 0111000$ szó nem eleme a kódnak, hiszen $\mathbf{Hc'} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$.

Most nézzük az összellenőrzőjeggyel, vagyis a $c_n = -\sum_{i=0}^{n-1} c_i$ jeggyel kiegészített kódot. Legyen $\widehat{\mathbf{H}}$ a kiterjesztett kód ellenőrző mátrixa, $\mathbf{u}$ az eredeti kódszó, $\mathbf{u'}^T = \mathbf{u}^T|p$ a kiterjesztett kódszó és $\mathbf{v'}^T = \mathbf{v}^T|p'$ a vett szó. Ekkor az $\mathbf{s'} = \widehat{\mathbf{H}}\mathbf{v'}$ szindróma $\mathbf{s'}^T = \mathbf{s}^T|s_p$ alakú, ahol $\mathbf{s} = \mathbf{Hv}$, és s_p a $\mathbf{v'}$ jegyeinek összege. Azt tudjuk, hogy $\mathbf{s} = \mathbf{0}$ $\mathbf{v}$-re vonatkozóan hibátlan esetet vagy legalább három hibát jelent, míg $s_p = 0$ azt jelzi, hogy vagy $\mathbf{v'} = \mathbf{u'}$, tehát egyáltalán nem lépett fel hiba az átvitel során, vagy legalább két jegy hibás $\mathbf{v'}$-ben. Három esetet különböztetünk meg:

a) $\mathbf{s} = \mathbf{0}$. Az előbbiek szerint ez vagy $\mathbf{v} = \mathbf{u}$-t, vagy $\mathbf{v}$-ben legalább három hibát jelent. Mivel feltettük, hogy egy szóban várhatóan legfeljebb egy hiba lehetséges, vagyis nagyon kicsi a hibák valószínűsége, és több hiba valószínűsége az egyes hibák valószínűségének szorzata, így igen nagy valószínűséggel hibátlan volt az átvitel, és ez lesz a döntésünk is, vagyis úgy döntünk, hogy $\mathbf{v} = \mathbf{u}$.

b) $\mathbf{s} \neq \mathbf{0}$ és $s_p = 0$. $\mathbf{s} \neq \mathbf{0}$ csak úgy lehet, ha $\mathbf{u} \neq \mathbf{v}$, vagyis legalább egy hiba történt, és $s_p = 0$ legalább két hibát jelez, ezért tudjuk, hogy legalább két hiba történt az átvitel során. Ezt javítani csak akkor tudjuk, ha **v**-ben egy hiba lépett fel, és a második hiba az összellenőrző jegyben van, minden más esetben korrigálás után is hibás lesz a kódszó. Arra azonban semmilyen lehetőségünk nincs, hogy a kedvező esetet megkülönböztessük a többitől, és két hiba esetén annak valószínűsége, hogy az egyik hiba az összellenőrző jegyben van, nem nagyobb annál a valószínűségnél, hogy mindkét hiba az eredeti részben van, így nem tudunk javítani, de észrevesszük a hibát, tudunk jelezni. Az előbbi állítás pontosabban azt jelenti, hogy ha **v** hossza n, akkor annak a valószínűsége, hogy mindkét hiba erre a részre esik, p-valószínűségű független hiba esetén $\binom{n}{2} p^2 (1-p)^{n-1}$, míg ha csak az egyik hiba van az eredeti részen, akkor a megfelelő valószínűség $np^2(1-p)^{n-1}$, és az előbbi eset valószínűsége $\frac{n-1}{2}$-szerese a második eset valószínűsűgűnek, ami $n > 3$ esetén 1-nél nagyobb.

c) $\mathbf{s} \neq \mathbf{0}$ és $s_p \neq 0$. Ha összesen egy hiba történt, és ez a hiba az eredeti részben van, akkor ezt a kombinációt kapjuk, illetve egy hibával ez a kombináció csak úgy lehet, ha a hiba **v**-ben van. Mivel az a legvalószínűbb, hogy ténylegesen egy hiba keletkezett, ezért ebben az esetben javítunk. Bináris kódnál még jobb a helyzet, hiszen ha egynél több hiba van, akkor legalább 3 helyen hibásodott meg az üzenet, és ebből legalább kettőnek **v**-ben kell lennie. Ekkor ismét nagyságrendekkel az első eset a legvalószínűbb, és ezt tudjuk javítani.

A három eset egybevetéséből látjuk, hogy bináris kódnál két hiba esetén nem fogunk „javítani", tehát csökken a dekódolási hiba. Igaz, hogy bizonyos esetekben olyankor sem javítunk, amikor ez lehetséges lenne, nevezetesen abban az esetben, amikor az üzenetrészben pontosan egy hiba van, és ugyanakkor a paritásjegy is hibás, ám mint láttuk, ennek a valószínűsége kisebb (sőt már nem túl nagy *n* esetén is lényegesen kisebb), mint az, hogy mindkét hiba az üzenetrészben található.

Most megadjuk a Hamming-kód egy lehetséges, speciális elrendezésű paritásellenőrző mátrixát.

9.4. Tétel

A $2 \leq r \in \mathbb{N}$ pozitív egész által meghatározott $[n, k]$-paraméterű q-áris Hamming-kód ellenőrző mátrixa skalárekvivalenciától eltekintve $\mathbf{H}_q^{(2)} = \begin{pmatrix} e & \mathbf{T}_q^{(1)^T} \\ 0 & \mathbf{e}^{(1)^T} \end{pmatrix}$ és $\mathbf{H}_q^{(r+1)} = \begin{pmatrix} \mathbf{H}_q^{(r)} & \mathbf{T}_q^{(r)^T} \\ \mathbf{0}^{(r)^T} & \mathbf{e}^{(r)^T} \end{pmatrix}$ alakú, ahol $n = \frac{q^r-1}{q-1}$, $\mathbf{0}^{(r)}$ a $\frac{q^r-1}{q-1}$ darab 0-ból, $\mathbf{e}^{(r)}$ a q^r darab e-ből álló oszlopvektor, és $\mathbf{T}_q^{(r)}$ a q-elemű test fölötti r dimenziós vektortér vektoraiból mint sorvektorokból álló mátrix.

Δ

A fenti mátrixban balról jobbra először az az oszlop áll, amelyben a 0-indexű elem e, az összes többi 0, majd egymás után az összes olyan vektor, amelyben az 1-indexű elem e, és az 1-nél nagyobb indexűek 0-k, ezután valamennyi olyan vektor jön, amelyben a 2-indexű elem e, a 2-nél nagyobb indexűek értéke 0, stb., végül azok a vektorok következnek, amelyekben a legnagyobb indexű elem e:

$$\begin{pmatrix} e & H_{0,1} & \cdots & H_{0,q-1} & \cdots & H_{0,n-q^{r-1}} & \cdots & H_{0,n-1} \\ 0 & e & \cdots & e & \cdots & H_{1,n-q^{r-1}} & \cdots & H_{1,n-1} \\ 0 & 0 & \cdots & 0 & \cdots & H_{2,n-q^{r-1}} & \cdots & H_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & H_{r-2,n-q^{r-1}} & \cdots & H_{r-2,n-1} \\ 0 & 0 & \cdots & 0 & \cdots & e & \cdots & e \end{pmatrix}.$$

Bizonyítás:

Legyen **u** a korábbi *R* reprezentánsrendszer valamelyik eleme. Ha $\mathbf{u}^T = u_0 u_1 \ldots u_{r-1}$ a megfelelő sorvektor, akkor van olyan $r > t \in \mathbb{N}$ index, hogy $u_t \neq 0$ (mert **u** nem a nullvektor), de minden $t <$

$i < r$ indexre $u_i = 0$. T_u bármely eleme választható reprezentánsnak, és mivel T_u elemei az $\mathbf{u}$ nem nulla konstansszorosai, ezért $\mathbf{u}' = u_t^{-1}\mathbf{u}$ is lehet reprezentánsa a T_u osztálynak. $\mathbf{u}'$ sorvektorában a t-edik komponens a test egységeleme, és továbbra is igaz, hogy a t-nél nagyobb indexű komponensek értéke 0, vagyis a megfelelő sorvektor $u_0 \dots u_{t-1}e0 \dots 0$ alakú. Tegyük fel, hogy már $\mathbf{u}$ ilyen alakú. Ha λ az $\mathbb{F}_q$ 0-tól és e-től különböző eleme, vagyis $\lambda \in \mathbb{F}_q \setminus \{0, e\}$, akkor $u_0 \dots u_{t-1}\lambda 0 \dots 0$ már nem lehet benne R-ben, hiszen ez szintén T_u eleme, de $\mathbf{u}$-tól különbözik. Legyen $\mathbf{v}$ egy másik vektor, és hasonlóan az előbbihez, ebben a vektorban is legyen e a maximális indexű nem nulla komponens. Most $\mathbf{u}$ és $\mathbf{v}$ csak akkor lehet lineárisan összefüggő, ha a két vektor megegyezik, ami azt jelenti, hogy minden lehetséges $n > s \in \mathbb{N}$ és $w_0 \dots w_{s-1}e0 \dots 0$, és csak ezek, előfordulnak $\mathbf{H}$-ban. Az is igaz, hogy ezeket a vektorokat tetszőleges sorrendben választhatjuk, így abban a sorrendben is, hogy ha T_u és T_v reprezentánsában s illetve t az az index, amelyre a vektor megfelelő komponense nem nulla, de amelynél nagyobb indexű valamennyi komponens nulla, és $s < t$, akkor a T_u-t reprezentáló vektor a mátrix kisebb indexű oszlopa, mint a T_v-t reprezentáló. Innen máris kapjuk $r = 2$-re a mátrixot. Ha $r + 1$-re nézzük a $\mathbf{H}$-mátrixot, és t a maximális olyan index egy vektorban, amelyhez nullától különböző komponens tartozik, akkor $t = r$ esetén éppen $\mathbf{T}_q^{(r)}$ transzponáltját kapjuk, míg $t < r$-nél a megfelelő vektorok legmagasabb helyiértékű komponense 0, a többi része pedig olyan, amely $\mathbf{H}_q^{(r)}$-ben is megtalálható, mégpedig ugyanazon sorrendben. Az előbbiekkel viszont kimerítettük $\mathbf{H}_q^{(r+1)}$ oszlopait.

□

Most tegyük fel, hogy egy üzenethalmaz q^k üzenetet tartalmaz, ahol $k \in \mathbb{N}^+$ és q egy prímszám pozitív egész kitevős hatványa, és ehhez keressünk minimális hosszúságú egy-hiba javító lineáris kódot. Ha a megfelelő C kód $[n, k, d]_q$-paraméterű, akkor $d \geq 3$, és az a jó, ha d pontosan 3.

Ahhoz, hogy C legalább egy hibát javítson, szükséges, hogy $q^k\big(1 + n \cdot (q-1)\big) \leq q^n$ legyen, azaz legyen $n \leq \frac{q^{n-k}-1}{q-1}$. Legyen r a legkisebb olyan pozitív egész, amellyel $k + r \leq \frac{q^r-1}{q-1}$, és legyen $n = k + r$. Ilyen n-nel mindenesetre létezik q^k-elemű, 3-távolságú kód, ugyanis megmutatjuk, hogy teljesül a lineáris kódokra vonatkozó Varshamov-Gilbert korlát. $q^k V_q\left(n, \left\lfloor\frac{d-1}{2}\right\rfloor\right) \leq q^n$, ahol $d = 3$, hiszen n-et éppen ennek alapján választottuk. De $\left\lfloor\frac{d-1}{2}\right\rfloor = \left\lfloor\frac{3-1}{2}\right\rfloor = 1 = 3 - 2 = d - 2$, amiből következik, hogy $V_q\left(n, \left\lfloor\frac{d-1}{2}\right\rfloor\right) = V_q(n, d-2)$, és nyilván az is igaz, hogy $V_q(n, d-2) > V_q(n-1, d-2)$ (mert $n \geq d$), így viszont $q^k V_q(n-1, d-2) < q^k V_q\left(n, \left\lfloor\frac{d-1}{2}\right\rfloor\right) \leq q^n$. Másrészről minden pozitív egész k-hoz létezik a megadott egyenlőtlenséget kielégítő n, ugyanis a $\frac{q^x}{1+x(q-1)}$ függvény a 2-nél nem kisebb valós számok halmazán folytonos és felülről nem korlátos, és $x = 2$-ben a függvény értéke kisebb, mint q, tehát mint q^k.

Jelöljük $\frac{q^r-1}{q-1}$-et n'-vel, ekkor $n' \geq n$. n'-höz létezik $[n', n'-r]$-paraméterű q-áris Hamming-kód, legyen egy ilyen C'. Ha $n' = n$, akkor ez a kód teljesíti az előírást, $C = C'$. Nézzük azt az esetet, amikor $n' > n$. Most $k' = n' - r > n - r = k$. Bármely $[n', k']$-kód szisztematikus legalább egy, k' oszlopból álló komponens-rendszerre. Ha rövidítjük a kódot ebből a k' oszlopból vett $k' - k$ oszlopra úgy, hogy a megtartott kódszavak valamennyi komponense ezeken az oszlopokon nulla legyen, akkor az így keletkezett kód lineáris, és a hossza $n' - (k' - k) = n$ lesz, vagyis egy $[n, k]_q$-típusú C^* kódot kapunk. Rövidítésnél a kód távolsága nem csökkenhet (feltéve, hogy a rövidített kód legalább két kódszót tartalmaz, de ez most teljesül), így $d(C^*) \geq d(C) = 3$. Ugyanakkor $d^* = d(C^*) > 3$ nem lehet: ha a távolság nagyobb lenne háromnál, akkor C^*-ot alkalmas $d^* - 3$ helyen átszúrva $[n^{\sim}, k, 3]_q$-paraméterű kódot kapnánk, így érvényes lenne az $n^{\sim} \leq \frac{q^{n^{\sim}-k}-1}{q-1}$ reláció. Ám $n^{\sim} = n - (d^* - 3) < n$-ből $r^{\sim} = n^{\sim} - k < n - k = r$, és így az r-nél kisebb $r^{\sim}$-re is teljesül a $k + r^{\sim} \leq \frac{q^{r^{\sim}}-1}{q-1}$ feltétel, és így r nem lenne minimális. Látjuk tehát, hogy most $C = C^*$ lesz egy megfelelő kód.

9.5. Definíció

Ha az $[n,k]_q$-paraméterű C Hamming-kód szeparábilis valamely k oszlopára, $k > t \in \mathbb{N}^+$, és C' olyan $[n-t, k-t, 3]_q$ kód, amelyet C-ből az előbbi k oszlopból t oszlopon a csupa 0 komponensekre rövidítve kapunk, akkor C' **az** $[n-t,k-t]_q$**-paraméterű** q**-áris rövidített Hamming-kód**.

Δ

Minden Hamming-kód tökéletes, így az elemszáma megegyezik a Hamming-korláttal, amiből következik, hogy egyben optimális is az adott hosszúsággal és kódtávolsággal. Rövidített Hamming-kódra az előbbiekben egyúttal beláttuk a következő tételt.

9.6. Tétel

Ha $n \in \mathbb{N}^+$, q prímhatvány, r a legkisebb egész, amellyel $n \leq \frac{q^r-1}{q-1}$, akkor egy $[n,k,3]_q$-paraméterű kód mérete legfeljebb q^{n-r}, így a megfelelő (rövidített) Hamming-kód optimális lineáris kód.

Δ

Bizonyítás:

A rövidített Hamming-kód konstruálásakor azt mutattuk meg, hogy a k-dimenziós, 3-távolságú lineáris kód hossza legalább $k+r$, ahol r a legkisebb olyan egész, amellyel teljesül a $k+r \leq \frac{q^r-1}{q-1}$ egyenlőtlenség. Legyen most n adott, amelyre a tételben megfogalmazott feltétel érvényes, és $k = n - r$. Ha $k' \geq k$-val létezik $[n,k',3]_q$-paraméterű kód, akkor a Hamming-korlát alapján teljesül a $q^{k'}\big(1+n\cdot(q-1)\big) \leq q^n$, és így az $n \leq \frac{q^{n-k'}-1}{q-1}$ egyenlőtlenség, amely ismét a tétel feltételeivel csak úgy lehet, ha $n-k' \geq r$, vagyis ha $k' \leq n-r = k$, azaz ha $k' = k$.

□

Ha a tételben valódi egyenlőtlenség áll, akkor bár a megfelelő rövidített Hamming-kód optimális lineáris kód, de nem feltétlenül optimális kód. Ha például $2^r \leq n < 3\cdot 2^{r-1}$ egy pozitív egész r-rel, akkor erre az n-re létezik $(n, \lambda\cdot 2^{n-r-1}, 3)_2$-paraméterű kód, ahol $\lambda = \frac{k}{16}$ és $18 \leq k \leq 20$ (n-től függően), vagyis $\lambda > 1$, ugyanakkor az optimális lineáris kód elemszáma az előbbiek szerint 2^{n-r-1}.

Bizonyos Hamming-kód ekvivalens egy azonos paraméterű ciklikus kóddal. Nézzünk például egy $q=2$, $n=7$, $\tau=1$, $\delta=3$-paraméterű BCH-kódot. x^7+1 irreducibilis faktorokra való felbontása $x^7+1 = (x+1)(x^3+x+1)(x^3+x^2+1)$ ($\mathbb{F}_2$ fölött az összeadás egybeesik a kivonással, ezért $x^7-1 = x^7+1$, továbbá 1 az $\mathbb{F}_2$ egységeleme). Egy $\mathbb{F}_2$ fölötti 7-edik primitív egységgyök vagy x^3+x+1, vagy x^3+x^2+1 gyöke, válasszuk az előbbit, ekkor ez lesz α minimálpolinomja. Mivel $\tau=1$ és $\delta=3$, ezért most α-t és α^2-et kell tekintenünk. q-elemű test fölött α és α^q minimálpolinomja azonos, és most $q=2$, ezért $g = x^3+x+1$, ami egy [7,4]-kódot generál. A kód ellenőrző polinomja, h, x^7+1 másik két faktorának szorzata, azaz $h = x^4+x^2+x+1$, így a g-vel generált kód egy ellenőrző mátrixa $\mathbf{H} = \begin{pmatrix} 1\,0\,1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix}$. Ha megnézzük **H** oszlopait mint kettes számrendszerbeli számokat (felül áll a legalacsonyabb helyiérték), akkor látjuk, hogy azok kiadják az 1, 2, 3, 4, 5, 6 és 7 számokat, hasonlóan a [7,4] bináris Hamming-kódhoz. Azt találtuk, hogy ez a kód megkapható az említett Hamming-kódból a bitek pozícióinak egy permutációjával. Ez a permutáció nyilván nem változtatja meg a kód hibajavító tulajdonságait, tehát a két kód ekvivalensnek tekinthető. Ami különbség, hogy a mostani kód ciklikus, így egyetlen polinom ismeretében generálható és az ellenőrzés is elvégezhető, míg a korábban a 88. oldalon ismertetett Hamming-kód nem ciklikus.

Nézzük most általában a kérdést, elsőként a bináris esetet, és legyen $n = 2^m-1$, ahol m 2-nél nagyobb egész. Ha α a 2^m-elemű test primitív eleme, akkor $\mathbb{F}_2$ fölötti minimálpolinomja m-edfokú. α nyilván gyöke az $f = x^n - e \in \mathbb{F}_2[x]$ polinomnak, így $m_\alpha^{(\mathbb{F}_2)}$ osztója f-nek, $m_\alpha^{(\mathbb{F}_2)}$ egy n-hosszúságú C ciklikus kódot generál $\mathbb{F}_2$ fölött. Ha $\mathcal{L}$ a q-elemű $\mathcal{K}$ test bővítése, akkor az L bármely β elemének és

β^q-nak a minimálpolinomja azonos. Most $q = 2$, így α^2 minimálpolinomja is $m_\alpha^{(\mathbb{F}_2)}$, ezért az $m_\alpha^{(\mathbb{F}_2)}$ által generált ciklikus kód egy $\mathbb{F}_2$ fölötti, $n = 2^m - 1$, $t = 1$, $\delta = 3$-paraméterű BCH-kód, ennélfogva $d \geq 3$. Mivel $\deg\left(m_\alpha^{(\mathbb{F}_2)}\right) = m$, ezért a kód $n - m$-dimenziós, a paritásellenőrző mátrix, $\mathbf{H}$, $m \times n$-méretű. $d \geq 3$ következtében $\mathbf{H}$ bármely két oszlopa lineárisan független, vagyis a mátrix oszlopai páronként különbözőek, és nem szerepel közöttük a nullvektor. De az $\mathbb{F}_2$ fölötti m-komponensű, nem nulla vektorok száma $2^m - 1 = n$, így a mátrix valamennyi nem nulla vektort tartalmazza oszlopként, amiből következik, hogy a megkonstruált kód $[n, n-m]_2$-paraméterű Hamming-kód (azt nem állítjuk, hogy minden bináris Hamming-kód ciklikus, ha ugyanis Hamming-kódban a komponensek sorrendjét permutáljuk, akkor ugyanolyan paraméterű Hamming-kódot kapunk, ám a ciklikusság nem invariáns erre a transzformációra, amint az előzőekben a konkrét példában láttuk).

Nem minden r, $n = \frac{q^r-1}{q-1}$ párosra létezik ciklikus Hamming-kód. Legyen például $q = 3$ és $r = 2$ azaz $n = 4$, $k = 2$. Az ellenőrző mátrix oszlopait $\tilde{\mathbf{h}}_j$-vel jelölve, ahol $4 > j \in \mathbb{N}$, egy $j = u$-ra $\tilde{\mathbf{h}}_u^T = 10$ vagy $\tilde{\mathbf{h}}_u^T = 20$, és csak az egyik szerepel $\mathbf{H}$-ban. Hasonlóan, egy alkalmas $v \neq u$-ra a v-edik oszlop vagy $\tilde{\mathbf{h}}_v^T = 01$, vagy $\tilde{\mathbf{h}}_v^T = 02$, ismét kizáró értelemben, ezért a $\mathbf{H}$ által generált altér u és v indexű pozícióján előforul az 10 és 01 kombináció. Ekkor választható a kódhoz olyan $\mathbf{H}$ is, ahol eleve az előbbi kombinációt tartalmazó két vektor a sorvektor. Tegyük fel, hogy a két sor $xy10$ és $zw01$. xz és yw egyike, mondjuk yw, 12 vagy 21 (és csak az egyik lehetséges), míg xz már csak 11 és 22 egyike (és ismét csak egyike) lehet. Ha $yw = 12$, akkor $\mathbf{H}_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$ vagy $\mathbf{H}_2 = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}$, ellenkező esetben a két sort és az első két oszlopot felcserélve kapjuk az előbbi mátrixokat, és a sorcsere nem változtatja meg a kódot, az oszlopcsere pedig csak a kódszavak komponenseinek sorrendjét változtatja. Ha $\mathbf{H}_2$-ben az első sort hozzáadjuk a másodikhoz, és felcseréljük a két sort, akkor ugyanazon kód paritásellenőrző mátrixát kapjuk, és ez a mátrix $\mathbf{H}_3 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 \end{pmatrix}$, ami az oszlopok sorrendjétől eltekintve megegyezik $\mathbf{H}_1$-gyel. Ez azt mutatja, hogy bármely két $[4,2]$-paraméterű ternáris (azaz $\mathbb{F}_3$ fölötti) Hamming-kód csak az oszlopok sorrendjében tér el egymástól. A $\mathbf{H}_1$-hez tartozó $\mathbf{G}_1$ generátormátrix $\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$. A két sor összege, 1110 is eleme a kódnak, ugyanakkor 0-val kezdődő (és nem nulla) kódszó csupán a második sor és annak kétszerese lehet, amelyekben biztosan előfordul a 2, ami mutatja, hogy 1110 ciklikus eltoltja, 0111, nem eleme a kódnak, és ez nem változik az oszlopok cseréjével, így a $[4,2]_3$-kód nem ciklikus. (Csupán az érdekesség kedvéért említjük, hogy amennyiben a ciklikus eltolások után az első komponenst megszorozzuk 2-vel, akkor ismét kódszót kapunk. Általában egy lineáris kód **konstaciklikus**, ha bármely $a_0 \dots a_{n-2}a_{n-1}$ kódszóra $(ca_{n-1})a_0 \dots a_{n-2}$ is kódszó, ahol c a test tetszőleges rögzített, nem nulla eleme. Ha $c = -e$, akkor a kód **negaciklikus**. Az előbbi példa is ilyen, hiszen a három elemű testben $2e = -e$.)

Ezek után nézzük, hogy mi mondható a Hamming-kódok és ciklikus kódok kapcsolatáról.

9.7. Tétel

Ha q egy prímszám pozitív egész kitevős hatványa, r kettőnél nem kisebb pozitív egész, $n = \frac{q^r-1}{q-1}$, és r a $q-1$-hez relatív prím, akkor van $[n, n-r]_q$-paraméterű ciklikus Hamming-kód.

Δ

Bizonyítás:

Mivel $n|q^r - 1$, így van $\mathbb{F}_{q^r}$-ben olyan β, amelynek a rendje $\mathbb{F}_{q^r}^*$-ban n. Elsőként igazoljuk, hogy $(r, q-1) = (n, q-1)$, így $(r, q-1) = 1$-ből adódik, hogy n és $q-1$ is relatív prímek. Valóban,

$$(q-1)\sum_{i=0}^{r-2}(i+1)q^{r-2-i}+r=\sum_{i=0}^{r-2}(i+1)q^{r-1-i}-\sum_{i=0}^{r-2}(i+1)q^{r-2-i}+r$$
$$=\sum_{i=0}^{r-2}(i+1)q^{r-1-i}-\sum_{i=1}^{r-1}iq^{r-1-i}+r$$
$$=q^{r-1}+\sum_{i=1}^{r-2}q^{r-1-i}-(r-1)+r=\sum_{i=0}^{r-1}q^i=\frac{q^r-1}{q-1}=n,$$

vagyis $n=(q-1)\cdot t$+r, és alkalmazva a legnagyobb közös osztókra vonatkozó $(a,ac+b)=(a,b)$ összefüggést látjuk, hogy a mondott két legnagyobb közös osztó megegyezik. Ebből következik, hogy β^{q-1} rendje is n, ami viszont azt jelenti, hogy $n>i\in\mathbb{N}^+$-ra $\beta^{i\cdot(q-1)}\neq e$, ahol e az $\mathbb{F}_q$, és ezzel együtt az $\mathbb{F}_{q^r}$ test egységeleme. Ekkor nincs olyan n-nél kisebb nemnegatív $i\neq j$ kitevő, amelyekhez létezne olyan $\mathbb{F}_q$-beli λ, hogy $\beta^i=\lambda\cdot\beta^j$. Ellenkező esetben ugyanis $e\neq\beta^{i-j}=\lambda\in\mathbb{F}_q$, amihez szükséges, hogy fennálljon a $\beta^{(i-j)\cdot q}=\beta^{i-j}$ egyenlőség, azaz $\beta^{(i-j)\cdot(q-1)}=e$ legyen. De az i-re és j-re tett megszorítás azt jelenti, hogy a különbségükre fennáll az $n>|i-j|\in\mathbb{N}^+$ korlát, így az előbbi hatvány nem lehet az egységelem.

Legyen $\{\alpha_i\in\mathbb{F}_{q^r}|r>i\in\mathbb{N}\}$ az $\mathbb{F}_{q^r}$ egy $\mathbb{F}_q$ fölötti bázisa, $n>j\in\mathbb{N}$-re $\boldsymbol{\beta}_j^T=\beta_{0,j}\dots\beta_{r-1,j}$ a β^j együtthatóinak vektora az előbbi bázissal való felírásban, és $\mathbf{H}$ egy olyan $r\times n$-es mátrix, amelyben az $r>i\in\mathbb{N}$ és $n>j\in\mathbb{N}$ indexekre $H_{i,j}=\beta_{i,j}$. Mivel $\boldsymbol{\beta}_i$ és $\boldsymbol{\beta}_j$ pontosan akkor lineárisan összefüggő, ha van olyan nullától különböző $\mathbb{F}_q$-beli λ, amellyel $\beta^j=\lambda\cdot\beta^i$, ez viszont az adott indexekkel csupán $i=j$ esetén lehetséges, $\mathbf{H}$ oszlopai páronként lineárisan függetlenek, ugyanakkor r és n értékére való tekintettel kell lennie három, páronként különböző, lineárisan összefüggő oszlopnak, $\mathbf{H}$ egy $[n,k]$-paraméterű q-áris Hamming-kódot definiál. De a $\mathbf{Hu}=\mathbf{0}$ egyenlőség ekvivalens az $\hat{u}(\beta)=0$ egyenlőséggel, így ha β $\mathbb{F}_q$ fölötti minimálpolinomja g, akkor a kód a g által generált ciklikus kód.

□

$q=2$ esetén bármely pozitív egész r-re r és $q-1$ relatív prím, ami azt jelenti, hogy minden bináris Hamming-kód generálható ciklikusan, amint korábban láttuk.

Legyen C egy $\mathbb{F}_q$ fölötti, r-paraméterű Hamming-kód. Hamming-kódnál $n-k=r$ és $d=3$, tehát $3=d\leq n-k+1=r+1$, és így $r=2$ esetén $d=n-k+1$, vagyis a kód egy MDS-kód. Ekkor $n=\frac{q^r-1}{q-1}=\frac{q^2-1}{q-1}=q+1$ és $k=n-r=(q+1)-2=q-1$. Az előbbiek szerint a kód egy ellenőrző mátrixa $\begin{pmatrix}e & 0 & \alpha_1 & \cdots & \alpha_{q-1}\\ 0 & e & e & \cdots & e\end{pmatrix}$, ahol $\{\alpha_i|q>i\in\mathbb{N}^+\}=\mathbb{F}_q^*$, és innen $\left(\begin{array}{cc}-\alpha_1 & -e\\ \vdots & \vdots\\ -\alpha_{q-1} & -e\end{array}\middle|\mathbf{I}_{q-1}\right)$ a kód egy generátormátrixa. Ha $q=2$, akkor a kód nem túl érdekes, hiszen ekkor $n=3$ és $k=1$, viszont érdekes lehet a kód $q=2^s$ esetén, ha $1<s\in\mathbb{N}$, ugyanis bármely pozitív egész s esetén 2^s-1 páratlan, tehát relatív prím 2-höz, és így a kód generálható úgy, hogy ciklikus legyen. Az így generált Hamming-kód tehát egy ciklikus MDS-kód.

Most megvizsgáljuk egy Hamming-kód duálisát. Mint ismeretes, a duális kód generátormátrixa az eredeti kód paritásellenőrző mátrixa és fordítva.

Bináris Hamming-kódból indulunk ki. Egy ilyen kódban $n=2^r-1$, ez a hossza a duális kódnak is, így az r-dimenziós duális kód minden vektora egy $n=2^r-1$ hosszúságú bináris sorozat. Bináris Hamming-kód ciklikus, de ciklikus kód duálisa is ciklikus, amelyet $h_0^{-1}h^*=(-g_0)\frac{e-x^n}{g^*}=g^{(D)}$ generál, ha g az eredeti kód generátorpolinomja. Legyen c a duális kódhoz tartozó kódszópolinom. Ekkor $c=ag^{(D)}=\frac{-g_0a}{g^*}(e-x^n)$ egy $\mathbb{F}_2$ fölötti, legfeljebb $r-1$-edfokú a polinommal, majd ebből $S=\frac{c}{e-x^n}=\frac{-g_0a}{g^*}$, és $\deg(g)=r$, így S a g által generált bináris homogén lineáris rekurzív sorozat. De g egy primitív n-edik egységgyök minimálpolinomja, tehát primitív polinom, és így S maximális periódusú sorozat. Ekkor a $g^{(D)}$ által generált bármely nem nulla sorozat egy periódusában az 1-ek száma

2^{r-1}, vagyis a duális kód valamennyi nem nulla vektorának súlya azonos, és értéke 2^{r-1}, a bináris Hamming-kód duálisa **ekvidisztáns**, vagy más elnevezéssel **szimplex kód**.

Most igazoljuk, hogy ez a tulajdonság minden Hamming-kódra igaz. Előtte megadunk egy szükséges feltételt ahhoz, hogy egy kód ekvidisztáns legyen.

9.8. Tétel

Legyen az $[n,k]_q$-paraméterű szimplex kódban n' a 0-tól különböző elemet tartalmazó oszlopok száma. Ekkor $\frac{q^k-1}{q-1}\Big| n'$.

Δ

Bizonyítás:

A 4.15. Tételben láttuk, hogy ha az $[n,k]_q$-kód egy oszlopában van nullától különböző elem, akkor annak az oszlopnak a súlya $(q-1)q^{k-1}$. Mivel n' olyan oszlop van, amely nem csak a nullát tartalmazza, ezért a kód összsúlya $n'(q-1)q^{k-1}$, vagyis a teljes kódban ennyi nullától különböző elem van. A kódszavak száma q^k, és ha minden nem nulla kódszó súlya azonos, akkor egy-egy nem nulla kódszó súlya $w = \frac{n'(q-1)q^{k-1}}{q^k-1}$. De w egész szám és $\left(q^k-1, q^{k-1}\right) = 1$, ezért $q^k-1 \Big| n'(q-1)$, vagyis $\frac{q^k-1}{q-1}\Big| n'$.

□

A Hamming-kód duálisa megfelel a megadott feltételnek, ugyanis a kód dimenziója r, és a kód hossza éppen $\frac{q^r-1}{q-1}$.

9.9. Tétel

Legyen $2 \leq r \in \mathbb{N}$, $q = p^s$, ahol p prímszám és $s \in \mathbb{N}^+$, továbbá $n = \frac{q^r-1}{q-1}$. Az $[n, n-r]$-paraméterű q-áris Hamming-kódhoz tartozó duális kód egy $[n,r,d]_q$-paraméterű szimplex kód, ahol a kód, és így az állandó távolság értéke q^{r-1}.

Δ

Bizonyítás:

Az egyetlen, amit bizonyítani kell az, hogy minden nem nulla kódszó súlya q^{r-1}.

Először belátjuk, hogy az ellenőrző mátrix bármely sorának súlya a fenti érték. Az i-edik sorban lévő nem nulla elemek száma megegyezik az r-dimenziós tér azon vektorainak számával, amelyeknek az i-edik komponense mondjuk a test egységeleme, hiszen a generátormátrix minden oszlopát meg tudjuk szorozni egy olyan nem nulla elemmel, hogy az oszlop adott nem nulla eleme egységelem legyen. Ilyen vektor összesen q^{r-1} van, i-től függetlenül, így a mátrix valamennyi sorának ez a súlya.

Mivel a mátrix sorai lineárisan függetlenek, és így a kód egy bázisának elemei, továbbá a tér bármely nem nulla vektora eleme a tér valamely bázisának, ezért az előbbi megállapítás a kód minden elemére igaz, vagyis valamennyi nem nulla kódszó súlya azonos, és a közös súly q^{r-1}.

□

Bináris esetben a kód hossza 2^r-1, a kód elemeinek száma 2^r, és valamennyi nem nulla vektorban pontosan 2^{r-1} 1-es és $2^{r-1}-1$ 0-ás található, jelöljük ezt a kódot A_n-nel, ahol $n = 2^r$. Ha kiterjesztjük a kódot egy paritásbittel, akkor valamennyi kódszó paritásbitje 0 lesz, hiszen $r > 1$ következtében minden kódszó páros súlyú. Az új kód hossza 2^r, a kódszavak száma nem változott, tehát szintén 2^{r-1}, és a vektorok súlya is változatlan, azaz – nem számítva a nullvektort – ismét 2^{r-1}, vagyis most a csupa nullából álló kódszótól eltekintve mindenegyes vektorban azonos számú 0 és 1 található.

Ez mint kód nem különösebben érdekes, hiszen A_n-nel azonos elemszámmal és hibajavító képességgel rendelkezik, de nagyobb hosszon, azaz nagyobb költséggel. Ha a nullákat 1-re és az egyeseket -1-re cseréljük, akkor egy olyan $n \times n$-es $\mathbf{H}_n$ mátrixot nyerünk, amelyben minden elem 1 vagy -1, és $\mathbf{H}_n\mathbf{H}_n^T = n\mathbf{I}_n$, ahol $\mathbf{I}_n$ az n-edrendű egységmátrix. Az ilyen tulajdonságú mátrixot **n-edrendű Hadamard-mátrix**nak nevezik, segítségükkel képezzük a **Hadamard-kód**okat, azaz az előbbi A_n-t, valamint egy B_n-nel és egy C_n-nel jelölt kódot. Az előbbit úgy kapjuk, hogy A_n-t megnöveljük a kódszavak komplemenseivel, míg az utóbbit hasonló módon, de a kiterjesztett kódból kiindulva (azaz az eredeti kódot meghosszabbítottuk). Könnyű belátni, hogy B_n egy $(2^r - 1, 2^{r+1}, 2^{r-1} - 1)_2$-kód, míg C_n $(2^r, 2^{r+1}, 2^{r-1})_2$-paraméterű kód, és A_n-t az első oszlopon nullára rövidítve $(2^r - 2, 2^{r-1}, 2^{r-1})_2$-paraméterű kódhoz jutunk. A duális Hamming-kód lineáris, ugyanakkor nem minden Hadamard-kód lineáris. (Csak megjegyezzük, hogy Hadamard-mátrix $n = 1$ és $n = 2$-n kívül csupán néggyel osztható n-re létezhet, de azt a sejtést még nem sikerült bizonyítani, hogy minden ilyen n-re létezik is.)

Korábban definiáltuk az önortogonális és önduális kódot, aktualizáljuk most ezeket Hamming- és kiterjesztett Hamming-kódokra valamint ezek duálisára.

Ha egy kód önortogonális, akkor része a saját duális terének, így az eredeti tér dimenziója nem haladhatja meg a duális tér dimenzióját, tehát $k \leq n - k$, azaz $2k \leq n$, és egyben egy kód és duálisa csupán az önduális esetben lehet egyszerre önortogonális. Hamming-kódnál $n = \frac{q^r-1}{q-1}$ és $k = n - r$, így az előbbi feltétel most $\frac{q^r-1}{q-1} \leq 2r$ alakú, és az öndualitáshoz egyenlőségnek kell teljesülnie. Innen $2r \geq \frac{q^r-1}{q-1} = \sum_{i=0}^{r-1} q^i = 2r + \sum_{i=0}^{r-1}(q^i - 2)$, tehát $\sum_{i=0}^{r-1}(q^i - 2) \leq 0$, és ez 2-nél nem kisebb r és q mellett csupán az $r = 2$ és $q = 2$ illetve $r = 2$ és $q = 3$ esetén lehetséges. Közvetlen ellenőrzéssel látjuk, hogy a bináris eset nem jó, ugyanakkor a 2 hosszúságú ternáris Hamming-kód önduális. Kiterjesztett Hamming-kódnál az eltérés az, hogy n helyett $n + 1$ szerepel, és az utolsó összeg értéke 2-nél kell, hogy ne legyen nagyobb. Ezt a feltételt nyilván kielégítik az előző esetek, továbbá $r = 3$, $q = 2$ és $r = 2$, $q = 4$. Újra közvetlen számolással kapjuk, hogy $r = 2$ és $q = 2$ illetve $r = 3$ és $q = 2$ jó, és az utóbbi önduális.

Áttérünk a duális kódokra, a Hamming-kód duálisával kezdve. A kód generátormátrixa az eredeti kód paritásellenőrző mátrixa, és ezt – skalárekvivalencia erejéig – korábban megadtuk. $\mathbf{T}_q^{(r)}$ bármely oszlopának négyzete azonos az első oszlop négyzetével, bármely oszlopának szorzata $\mathbf{e}^{(r)}$-rel azonos az első oszlopnak és $\mathbf{e}^{(r)}$-nek a szorzatával, azaz magával az első oszloppal, végül tetszőleges két különböző oszlop szorzata megegyezik az első két oszlop szorzatával, ezért elég ezeket megvizsgálni. Az első oszlopban a test mindenegyes eleme pontosan q^{r-1}-szer szerepel, így az $\mathbf{e}^{(r)}$-rel vett szorzatban és az önmagával vett szorzatban is minden érték q^{r-1}-szer fordul elő. Ha $r \geq 2$, akkor q^{r-1} osztható q-val, ez pedig a test karakterisztikájával, így ezek az összegek nullát adnak. Hasonlóan láthatjuk be, hogy az első két oszlopban minden lehetséges $\mathbb{F}_q$-beli rendezett pár pontosan q^{r-2}-szer szerepel, és ezért $r \geq 3$ esetén a két oszlop szorzata is 0-t ad. $r = 2$ esetén viszont a skalárszorzat értéke az $\mathbb{F}_q$ elemeiből képzett összes lehetséges $a \cdot b$ szorzat összege, ami azonos a test elemei összegének négyzetével, és $q > 2$ esetén ez is nulla, hiszen legalább kételemű véges testben az elemek összege maga 0. Arra jutottunk, hogy $\mathbf{H}_q^{(r+1)}$ bármely két – nem szükségszerűen különböző – sorának szorzata $r \geq 3$, vagy $r \geq 2$ és $q \geq 3$ esetén azonos $\mathbf{H}_q^{(r)}$ megfelelő két sorának illetve megfelelő sorának és $\mathbf{0}^{(r)}$ transzponáltjának a szorzatával, tehát $\mathbf{H}_q^{(r)}$ megfelelő két sorának szorzatával, hiszen a nullvektorral való szorzás eredménye 0. Ez indukcióval mutatja, hogy adott q mellett bármely r-re akkor és csak akkor lesz a duális Hamming-kód önortogonális, ha $r = 2$, vagy ha $q = 2$, akkor még $r = 3$. $\mathbf{H}_q^{(2)}$ első sorának négyzete az $\mathbb{F}_q$-beli elemek négyzetének összege plusz az egységelem. Az előbbi összeg $q = 2$ esetén e, $q = 3$-ra $-e$, minden más esetben 0, így az első sor négyzete akkor és csak akkor 0, ha $q = 2$ vagy $q = 3$. A második sor négyzete mindig 0, hiszen ebben a sorban q darab egységelem áll. A két sor szorzata viszont éppen a test elemeinek összege, ami mindig nulla. A $q = 2$, $r = 3$ eset közvetlenül ellenőrizhető, és azt adja, hogy bármely két sor skalárszorzata nulla, így kiadódik, hogy a duális Hamming-kód pontosan a bináris és ternáris esetben önortogonális, és ebben a két esetben ez minden r-re igaz. Végül a kiterjesztett Hamming-kód duálisát nézzük. Most a mátrix annyiban különbözik az előzőtől, hogy minden sor végén

szerepel egy nulla, illetve van egy csupa e-ből álló sor. Az előbbi sorok szorzatát nem befolyásolja a kiegészítő 0, ezért ez a kód csak akkor lehet önortogonális, ha a kiterjesztés nélküli kód duálisa is az. Az új sor négyzete $(n+1)e = 2e$, ami viszont csak akkor 0, ha q 2-nek egy hatványa, ezért q már csak 2 lehet. Ezt a sort egy régi sor kiterjesztettjével szorozva az eredeti sorban álló elemek összegét kapjuk, ami 0, mert $\mathbf{T}_q^{(r)}$ oszlopaira és $\mathbf{e}^{(r)}$-re ez igaz, $\mathbf{H}_2^{(2)}$ két sorára is igaz, és ezért indukcióval belátható, hogy minden r-re is igaz. Igazoltuk tehát a következő tételt.

9.10. Tétel

Legyen r kettőnél nem kisebb egész, $n = \frac{q^r-1}{q-1}$, és q egy prímszám pozitív egész kitevős hatványa. Ekkor az $[n,k]$-paraméterű q-áris Hamming-kód akkor és csak akkor önortogonális, ha $r = 2$ és $q = 3$, és ekkor a kód egyben önduális is. A kiterjesztett Hamming-kód akkor és csak akkor önortogonális, ha $q = 2$ és vagy $r = 2$ vagy $r = 3$, és ez utóbbi, és csak ez, egyben önduális is. Minden bináris és ternáris Hamming-kód duálisa valamint kiterjesztett bináris Hamming-kód duálisa önortogonális, és semmilyen más q-ra nincs ilyen típusú önortogonális kód.

Δ

Utolsóként megnézzük a kódsebességet és a hibajavító-képességet. Ismeretes, hogy általában ezek egymás rovására növelhetőek, és az is nyilvánvaló, hogy egy kód csak akkor használható, ha mindkét érték meghalad egy ésszerű alsó korlátot. Sajnos sem a Hamming-kód, sem a duálisa nem jeleskedik ebben a tekintetben.

9.11. Tétel

Legyen q egy prímszám pozitív egész kitevős hatványa, $2 \leq r \in \mathbb{N}$, és $C^{(r)}$ egy $[n, n-r]_q$-paraméterű Hamming-kód. Ekkor r növekedésével $C^{(r)}$ kódsebessége 1-hez és hibajavító képessége 0-hoz, míg a duális kód kódsebessége 0-hoz, hibajavító képessége $1 - \frac{1}{q}$-hoz tart.

Δ

Bizonyítás:

Ha C egy $(n, M, d)_q$-kód, akkor a kódsebesség $\mathcal{R} = n^{-1} \log_q M$, és ez $[n,k,d]_q$-paraméterű lineáris kód esetén $k \cdot n^{-1}$, míg a hibajavító képességre $\delta = d \cdot n^{-1}$ jellemző.

$C^{(r)}$-ben $k = n - r$, így a kódsebesség értéke $\frac{\frac{q^r-1}{q-1}-r}{\frac{q^r-1}{q-1}} = 1 - r\frac{q-1}{q^r-1} > 1 - \frac{r}{q^{r-1}}$, ahol a második tag értéke r növekedésével tetszőleges kis eltéréssel megközelíti a nullát. $\delta_{C^{(r)}}$ számlálója r-től függetlenül 3, míg a nevező korlátlanul nő, így a hányados értéke tart a 0-hoz.

Tetszőleges lineáris kódra érvényes, hogy ha a kód sebessége $\mathcal{R}$, akkor a duális kódé $1 - \mathcal{R}$, hiszen $(n-k) \cdot n^{-1} = 1 - k \cdot n^{-1}$, így a Hamming-kód duálisának sebességére vonatkozó állítás nyilván igaz. Ugyanakkor a duális kód távolsága q^{r-1}, tehát most $\delta = \frac{q^{r-1}}{\frac{q^r-1}{q-1}} = \left(1 - \frac{1}{q}\right) \cdot \left(1 + \frac{1}{q^r-1}\right)$, és a második tényező értéke r növekedésével 1-hez tart.

□

10. Reed-Solomon kódok

Felidézzük a BCH-kódokat. Adott a q-hoz relatív prím n, a τ egész és a 2-nél nem kisebb, de n-nél nem nagyobb δ egész. Ha α egy $\mathbb{F}_q$ fölötti primitív n-edik gyök, és $m_{\alpha^i}^{(\mathbb{F}_q)}$ az α^i $\mathbb{F}_q$ fölötti minimálpolinomja, akkor a $g = \text{lkkt}\left\{m_{\alpha^{\tau+i}}^{(\mathbb{F}_q)} \middle| \delta - 1 > i \in \mathbb{N}\right\}$ polinom által generált ciklikus kód $(n, \tau, \delta)_q$-paraméterű BCH-kód. Ez a kód $[n, k, d]_q$-paraméterű kód, ahol $k = n - \deg(g)$, és $d \geq \delta$, feltéve, hogy $k > 0$.

10.1. Definíció

Az $(n, \tau, \delta)_q$-paraméterű BCH-kód **Reed-Solomon kód**, ha $n|q-1$.

Δ

Mivel $n|q-1$, ezért n és q relatív prím, létezik primitív n-edik egységgyök $\mathbb{F}_q$ fölött. Az $\mathbb{F}_q$ fölötti primitív n-edik egységgyök eleme $\mathbb{F}_q$-nak, így α^i $\mathbb{F}_q$ fölötti minimálpolinomja $x - \alpha^i$, tehát a kód generátorpolinomja $g = \prod_{i=0}^{\delta-2}(x - \alpha^{\tau+i})$. Ekkor $k = n - \deg(g) = n - (\delta - 1) = n - \delta + 1$, és a Singleton-korlát valamint a BCH-kódok távolsága alapján $d \geq \delta = n - k + 1 \geq d$-ből kapjuk, hogy $d = n - k + 1$, vagyis igaz az alábbi tétel.

10.2. Tétel

A Reed-Solomon kódok MDS-kódok.

Δ

A Reed-Solomon kód ellenőrző polinomja $h = \frac{x^n - e}{g} = \frac{\prod_{j=0}^{n-1}(x-\alpha^j)}{\prod_{i=0}^{\delta-2}(x-\alpha^{\tau+i})} = \prod_{i=\delta-1}^{n-1}(x - \alpha^{\tau+i})$, és a duális kód generátorpolinomja $g^{(D)} = h_0^{-1}h^* = \prod_{i=\delta-1}^{n-1}(x - \alpha^{-(\tau+i)})$ (mert $h_0^{-1}h^*$ főpolinom, és reciprok polinom gyökei a polinom nem nulla gyökeinek inverzei). Ez szintén egy Reed-Solomon kód generátorpolinomja, ami igazolja a következő tételt.

10.3. Tétel

Reed-Solomon kód duálisa is Reed-Solomon kód.

Δ

Azt tudjuk, hogy ciklikus kód duálisa ciklikus, most pedig azt láttuk, hogy Reed-Solomon kód duálisa is Reed-Solomon kód. Mivel minden BCH-kód ciklikus, ezért egy BCH-kód duálisa is ciklikus, az azonban általában nem igaz, hogy BCH-kód duálisa BCH-kód. Ha például $n = 8$, $q = 3$, $\tau = 1$ és $\delta = 3$, akkor a kód gyökeinek kitevői egyrészt 1 és 2, másrészt az α és α^2 minimálpolinomjai gyökeinek kitevői. α^j minimálpolinomjának akkor és csak akkor gyöke α^k, ha $k \equiv jq^l\ (n)$ egy alkalmas l kitevővel, vagyis α-hoz tartozik még az 1 kitevőn kívül $3 \cdot 1 = 3$, és más már nem, mert $3 \cdot 3 = 9 \equiv 1\ (8)$, és hasonlóan 2-höz tartozik 2 és 6, mert 18 kongruens 2-vel modulo 8. Ekkor a duális kód gyökeinek kitevői 0, 4, 5 és 7. A 0-hoz nem tartozik más gyök, és hasonlóan a 4 is egyedül áll, míg az 5. és 7. hatvány minimálpolinomja azonos. Ha a duális kód BCH-kód, akkor kell, hogy legyenek egymás utáni kitevőhöz tartozó gyökei úgy, hogy az ezen gyökökhöz tartozó minimálpolinomok gyökei kiadják az előbb felsorolt valamennyi gyököt. Ezek szerint minden minimálpolinomból legalább egy gyöknek szerepelnie kell a sorozatban, tehát a 0. és 4., továbbá az 5. és a 7. legalább egyike (a 0. és a 7. gyök

szomszédosak, mert a 8. hatvány azonos a 0. hatvánnyal!), de bárhogy is választunk ki a megadott módon hármat, vagy mind a négyet, ezek a kiválasztott gyökök nem alkotnak hézagmentes sorozatot, tehát a duális kód nem lehet BCH-kód.

Mint azt a BCH-kódoknál láttuk, ha egy $\delta - 1 > i \in \mathbb{N}$ -re $(\tau + i) \bmod n = 0$, akkor e gyöke a kódnak, vagyis ekkor a kód egy paritáselemes kód.

Most ismét emlékeztetünk a ciklikus kódokra. Ha a kód gyökei az α_i-k, ahol $l > i \in \mathbb{N}$, és $\widetilde{\mathbf{H}}$ az a mátrix, amelyben az $l > i \in \mathbb{N}$, $n > j \in \mathbb{N}$ indexekre $\widetilde{H}_{i,j} = \alpha_i^j$, akkor az $\mathbf{u} \in \mathbb{F}_q^n$ vektor akkor és csak akkor eleme a kódnak, ha $\widetilde{\mathbf{H}}\mathbf{u} = \mathbf{0}$, jóllehet $\widetilde{\mathbf{H}}$ általában nem a kód ellenőrző mátrixa. Ha azonban a kód egy Reed-Solomon kód, akkor az $\alpha_i = \alpha^{\tau+i}$ gyök eleme az alaptestnek, így $\widetilde{\mathbf{H}}$ egy $\mathbb{F}_q$ fölötti mátrix, továbbá $l = n - k$, vagyis most $\widetilde{\mathbf{H}}$ a kód ellenőrző mátrixa, $\widetilde{\mathbf{H}} = \mathbf{H}$, és az $n - k > i \in \mathbb{N}$, $n > j \in \mathbb{N}$ indexpárokra $H_{i,j} = \left(\alpha^{\tau+i}\right)^j$. Legyen $A_{i,j} = \left(\alpha^i\right)^j = \left((\alpha^{-1})^{-i}\right)^j$ az $n \times n$-es $\mathbf{A}_{\alpha^{-1}}$ mátrixban, ekkor $\mathbf{u}$ pontosan akkor eleme a kódnak, ha $\mathbf{A}_{\alpha^{-1}}\mathbf{u}$-ban a $\tau \le i < \tau + n - k$ indexekhez (pontosabban az $i \bmod n$ indexekhez) tartozó komponensek értéke 0. Mivel α rendje n, és $\alpha \in \mathbb{F}_q$, ezért $\mathbf{A}_{\alpha^{-1}}\mathbf{u}$ nem más, mint $\mathbf{u}$-nak az α^{-1}-gyel vett diszkrét Fourier-transzformáltja, vagyis azt kaptuk, hogy az $\mathbb{F}_q$ fölötti n-dimenziós tér egy vektora akkor és csak akkor eleme a kódnak, ha az α^{-1}-gyel vett $\mathbf{U}$ diszkrét Fourier-transzformáltjában a $\tau \le i < \tau + n - k$ indexekre $U_{i \bmod n} = 0$. A diszkrét Fourier-transzformáció bijektíven képezi le az n-dimenziós teret önmagára, így különböző kódszó képe különböző, és az n-dimenziós térben pontosan azon vektorok inverz diszkrét Fourier-transzformáltjai lesznek elemei a kódnak, amelyekben az előbb megadott komponensek mindegyike 0. Mindez azt jelenti, hogy a Reed-Solomon kódot generálhatjuk úgy is, hogy a k-dimenziós tér egy adott elemét mint üzenetet kiegészítjük $n - k$ darab 0-val úgy, hogy a kapott n-komponensű vektorban a fentebb megadott indexekhez tartozzanak ezek a 0-k, és az így kapott vektor α^{-1}-gyel vett inverz Fourier-transzformáltja lesz az üzenethez tartozó kódszó. Ezzel meghatároztuk a Reed-Solomon kód egy lehetséges generátormátrixát, ugyanis ez egy olyan mátrix, amelyet $\mathbf{A}_{\alpha^{-1}}$ inverzéből, vagyis $(ne)^{-1}\mathbf{A}_{\alpha}$-ból kapunk (ne felejtsük el, hogy most a transzformációt generáló primitív n-edik gyök α^{-1}!), ha töröljük ezen mátrix $i \bmod n$ indexekhez tartozó sorait, ahol $\tau \le i < \tau + n - k$. Legyen tehát a kódolandó üzenet $\mathbf{c} \in \mathbb{F}_q^k$, és legyen $k > i \in \mathbb{N}$ -re $U_{(\tau-k+i) \bmod n} = c_i$, míg $\mathbf{U}$ többi komponense legyen 0. Ekkor

$$u_j = (ne)^{-1} \sum_{i=0}^{k-1} U_{(\tau-k+i) \bmod n} \left(\alpha^{-j}\right)^{\tau-k+i}$$
$$= (ne)^{-1} \sum_{i=0}^{k-1} c_i \left(\alpha^{-j}\right)^{\tau-k+i} = (ne)^{-1} \left(\alpha^{-(\tau-k)}\right)^j \hat{c}\left(\alpha^{-j}\right),$$

ahol $c = \sum_{i=0}^{k-1} c_i x^i$, és $c_0 \dots c_{k-1}$ a kódolandó üzenet.

Most legyen $(\tau - k) \bmod n = 0$ és $n = q - 1$. Ekkor $\mathbf{U}$ első k komponense $\mathbf{c}$ megfelelő indexű komponense, így a $\mathbf{c}$-hez és $\mathbf{U}$-hoz tartozó polinom azonos, továbbá $(ne)^{-1} = (-e)^{-1} = -e$ (mert q a karakterisztika egy többszöröse) és $\alpha^{-(\tau-k)} = e$. Ha íly módon generáljuk a kódot azzal a módosítással, hogy a minden kódszóban meglévő $-e$ szorzótól eltekintünk, akkor tehát a $\mathbf{c}$ üzenethez tartozó $\mathbf{u}$ kódszó j-edik komponense $u_j = \hat{c}\left(\alpha^{-j}\right) = \hat{U}\left(\alpha^{-j}\right)$. Szúrjuk át a kódot úgy, hogy összesen m komponens maradjon, ahol $m \ge k$, és legyenek az ezen komponensekhez tartozó gyökök $\alpha_0, \dots, \alpha_{m-1}$. Mivel a Reed-Solomon kód MDS-kód, és MDS-kód átszúrásával kapott kód is MDS-kód, ezért az így kapott kód is MDS-kód, és akkor dekódolható például az MDS-kódoknál megadott többségi eljárással, továbbá mivel k-dimenziós MDS-kód generátormátrixában bármely k oszlop lineárisan független, ezért a kapott kód $[m, k]$-paraméterű lesz. Eredetileg a Reed-Solomon kódot ily módon definiálták, vagyis hogy vesszük a q-elemű test m különböző nem nulla elemét, és a $C_0 \dots C_{k-1}$ üzenethez, ahol $k < m$, azt a $c_0 \dots c_{m-1}$ kódszót rendeljük, ahol $c_i = \sum_{j=0}^{k-1} C_j \alpha_i^j$, a dekódolást pedig a többségi módszerrel végezzük (az így definiált kód egy átszúrt Reed-Solomon kóddal skalárekvivalens, amelyet az átszúrt kód oszlopainak egy permutációjával kapunk, és így általában nem ciklikus). Ennek nyilván speciális esete, amikor $\alpha_i =$

α^{-i}, ahol α a test n-edrendű eleme, és $n \geq m$. Amennyiben az utóbbi esetben még az is igaz, hogy $m = n$, akkor visszajutunk az általunk definiált Reed-Solomon kódhoz.

A Reed-Solomon kód generátormátrixát más módon is megkaphatjuk. Egy lineáris kód generátormátrixa azonos a kód duálisának ellenőrző mátrixával, így elegendő meghatározni ez utóbbi mátrixot. A 10.2 Tétel után láttuk, hogy a duális kód generátotpolinomja $g^{(D)} = \prod_{i=\delta-1}^{n-1}\left(x - \alpha^{-(\tau+i)}\right)$. Kis átalakításokkal $g^{(D)} = \prod_{i=0}^{n-\delta}\left(x - \alpha^{-(\tau+\delta-1+i)}\right) = \prod_{i=0}^{k-1}\left(x - \alpha^{-(\tau+n-k+i)}\right) = \prod_{i=0}^{k-1}\left(x - \alpha^{-(\tau-k+i)}\right)$, vagyis a duális kód gyökei az $\alpha^{-(\tau-k+i)}$ hatványok, ahol $k > i \in \mathbb{N}$. Ennek a kódnak az ellenőrző mátrixa az a $k \times n$-méretű $\mathbf{H}^{(D)}$ mátrix, amelyben $k > i \in \mathbb{N}$-re és $n > j \in \mathbb{N}$ -re $H_{i,j}^{(D)} = \left(\alpha^{-(\tau-k+i)}\right)^j$, és ez egy nem nulla konstans szorzótól eltekintve (ami generátormátrixból generátormátrixot, ellenőrző mátrixból ellenőrző mátrixot ad) azonos $\mathbf{A}_{\alpha^{-1}}^{-1}$ $(\tau - k + i) \bmod n$-indexű sorának j-edik elemével.

A Reed-Solomon kódoknak egy további definícióját is adhatjuk. Legyen $m < q$, $\alpha_0, \dots, \alpha_{m-1}$ a test m különböző, nem 0 eleme, n az α_i-k rendjeinek legkisebb közös többszöröse, $n - 1 > l \in \mathbb{N}^+$, és H olyan $l \times m$-es mátrix, amelyben a τ egésszel $H_{i,j} = \alpha_j^{\tau+i}$, továbbá $C = \left\{\mathbf{c} \in \mathbb{F}_q^m \middle| \mathbf{Hc} = \mathbf{0}\right\}$. Most könyen látható, hogy ez a kód egy n-hosszúságú, $\delta = l + 1$-paraméterű Reed-Solomon kód rövidítéséből kapott kóddal skalárekvivalens kód, amely $m = n$ és $\alpha_i = \alpha^i$ esetén éppen egy, az általunk adott definíciónak megfelelő Reed-Solomon kód.

Térjünk vissza a mi Reed-Solomon kódunkhoz, és nézzük meg, hogy hogyan lehet egy ilyen kódot dekódolni. Mivel ez egy MDS-kód, ezért alkalmazhatjuk a minden MDS-kód esetén működő többségi dekódolást, ám a Reed-Solomon kódok speciális tulajdonságait kihasználva ennél jobb módszerek is léteznek. Ezek egyikével később az alternáns kódoknál foglalkozunk, ugyanis az alternáns kódok a BCH-kódok általánosításai, így minden olyan módszer, amely alkalmazható az alternáns kódokra, nyilván működik a Reed-Solomon kódok esetén is. Itt most egy olyan módszert ismertetünk, amely elsősorban a Reed-Solomon kódok esetén alkalmazható.

Ha $\mathbf{H}$ a Reed-Solomon kód ellenőrző mátrixa, akkor $\mathbf{S} = \mathbf{Hv}$ a $\mathbf{v}$ szóhoz tartozó szindróma (most szándékosan jelöltük a korábbiaktól eltérő módon nagybetűvel a szindrómát). $\mathbf{S}$ az $n - k$-dimenziós tér vektora, és ha $\boldsymbol{\varepsilon}$ a hibavektor, akkor egyben $\mathbf{S} = \mathbf{H}\boldsymbol{\varepsilon}$. Korábban láttuk, hogy $\mathbf{Hv}$ a $\mathbf{v}$ vektor α^{-1}-gyel vett diszkrét Fourier-transzformáltjának a τ-tól kezdődő $n - k$ ciklikusan egymás után következő indexhez tartozó komponense, vagyis ha $\mathbf{A}_{\alpha^{-1}}$ a korábban már bevezetett $n \times n$-es mátrix, akkor $\mathbf{E} = \mathbf{A}_{\alpha^{-1}}\boldsymbol{\varepsilon}$ a hibavektor α^{-1}-gyel vett diszkrét Fourier-transzformáltja, és ennek az előbb megadott indexekhez tartozó szelete a szindróma. Tegyük fel, hogy $w(\boldsymbol{\varepsilon}) = t$, azaz t hiba van, és a hibák a $0 \leq i_0 < \cdots < i_{t-1} < n$ indexhez tartoznak, vagyis $\varepsilon_i \neq 0$ pontosan akkor, ha $i \in J = \{i_l | t > l \in \mathbb{N}\}$. Jelöljük α^{i_l}-et X_l-lel, és legyen $L = \prod_{i=0}^{t-1}(e - X_i x)$. Természetesen L-et nem ismerjük, de ha meg tudnánk határozni, akkor a gyökeiből ismernénk a hibák helyeinek indexeit, ezért ezt a polinomot **hibahely-polinom**nak nevezik. L egy t-edfokú polinom, amelyhez 0 együtthatóval további tagokat kapcsolhatunk, így kapjuk, hogy $L = \sum_{i=0}^{n-1} L_i x^i$. Ha most $\mathbf{L}$ az L együtthatóiból álló n-dimenziós vektor, akkor tekinthetjük ennek α^{-1}-gyel vett $\mathbf{l}$ inverz diszkrét Fourier-transzformáltját. Tudjuk, hogy $l_j = 0$ pontosan akkor, ha $\hat{L}\left(\alpha^{-j}\right) = 0$. Legyen u a polinom egy gyöke, akkor $0 = \hat{L}(u) = \prod_{i=0}^{t-1}(e - X_i u)$, vagyis valamely i indexre $e - X_i u = 0$, ahonnan $u = X_i^{-1} = \alpha^{-j_i}$. Ez azt jelenti, hogy $l_j = 0$ pontosan akkor teljesül, ha $j \in J$, vagyis akkor és csak akkor, ha $\varepsilon_j \neq 0$. Ebből viszont következik, hogy $\mathbf{l} \cdot \boldsymbol{\varepsilon} = \mathbf{0}$, ahol a két vektor szorzatát a komponensenkénti szorzással számoljuk, vagyis $(\mathbf{l} \cdot \boldsymbol{\varepsilon})_i = l_i \varepsilon_i$. De $\mathbf{l} \cdot \boldsymbol{\varepsilon} = \mathbf{0}$ akkor és csak akkor igaz, ha $\mathbf{L} * \mathbf{E} = \mathbf{0}$, ahol $*$ a ciklikus konvolúciót jelöli. A ciklikus konvolúciót kiírva minden $n > i \in \mathbb{N}$ indexre $0 = \sum_{j=0}^{n-1} L_j E_{(i-j)^{(n)}}$, ahol a $j^{(n)} = j \bmod n$ rövidítést alkalmaztuk. Mivel L-ben a t-nél nagyobb indexű együtthatók értéke 0, ezért

$$0 = \sum_{j=0}^{n-1} L_j E_{(i-j)^{(n)}} = \sum_{j=0}^{t} L_j E_{(i-j)^{(n)}} = \sum_{j=0}^{t} L_{t-j} E_{(i-t+j)^{(n)}}.$$

Terjesszük ki az n-komponensű E sorozatot egy végtelen sorozattá a $T_i = E_{(i+\tau)^{(n)}}$ definícióval. Ez a sorozat periodikus az n periódussal, továbbá az $n - k > i \in \mathbb{N}$ indexekre $T_i = E_{(i+\tau)^{(n)}} = S_i$, vagyis a T sorozat első $n - k$ komponense a szindróma, tehát ismert. Most

$$0 = \sum_{j=0}^{t} L_{t-j} E_{(i-t+j)^{(n)}} = \sum_{j=0}^{t} L_{t-j} T_{i-t+j-\tau},$$

de míg korábban az egyenlőség csak az n-nél kisebb i indexekre terjedt ki, addig most ez az összefüggés tetszőleges olyan i-re igaz, amellyel $i - t - \tau$ nemnegatív, vagyis $\sum_{j=0}^{t} L_j^* T_{i+j} = 0$, ahol L^* az L polinom reciproka, és $i \in \mathbb{N}$. Ha még azt is tekintetbe vesszük, hogy $L_t^* = L_0 = \hat{L}(0) = e$, vagyis L^* főpolinom, akkor látjuk, hogy T egy t-edrendű homogén lineáris rekurzív sorozat az L^* karakterisztikus polinommal, amelynek ismerjük az első $n - k$ elemét. Amennyiben $n - k \geq 2t$, akkor viszont az ismert elemek egyértelműen meghatározzák a teljes sorozatot, vagyis ebben az esetben a szindrómából meg tudjuk határozni T-t, de akkor ismerjük **E**-t, és ennek inverz Fourier-transzformálásával megkapjuk az $\boldsymbol{\varepsilon}$ vektort, azaz a hibavektort, és evvel a javított kódszót, $\mathbf{u} = \mathbf{v} - \boldsymbol{\varepsilon}$-t. Az $n - k \geq 2t$ feltétel viszont, mivel Reed-Solomon kódnál $d = n - k + 1$, ekvivalens a $t < \frac{d}{2}$ feltétellel, ami pedig az egyértelmű dekódolhatóság feltétele minimális távolságú dekódolásnál.

Az előbbi eredmény alapján tehát a Reed-Solomon kódok egy lehetséges dekódolása úgy történik, hogy a szindrómát mint egy n-periódusú homogén lineáris rekurzív sorozat első $n - k$ elemét kiegészítjük a periódus további elemeivel. Ezt megtehetjük a lineáris komplexitásnál látott módon, vagy úgy, hogy megoldjuk a $t' = \left\lfloor \frac{n-k}{2} \right\rfloor$ egyenletből álló $\sum_{j=0}^{t'-1} c_j S_{i+j} = S_{i+t'}$ egyenletrendszert, és a megoldásként kapott c_i együtthatókkal meghatározott homogén lineáris rekurzióval kiszámoljuk **E**-t.

A Reed-Solomon kódokat kiterjedten használják olyan helyeken, ahol a véletlen hibákon kívül úgynevezett **csomós hibák** előfordulása is gyakori. A csomós hibára az jellemző, hogy ha valahol fellép egy hiba, akkor a környezetében lévő további jegyek meghibásodása is valószínű. Gondoljunk például egy megkarcolt lemezre, egy kávéval leöntött CD-re, vagy például arra, hogy ha 100 Mbit/s-os sebességgel viszünk át adatokat (nem üvegszál-kábelen), vagyis egy-egy jel időtartama 10 ns, akkor egy légköri elektromos kisülés, amelynek az időtartama ennél lényegesen nagyobb, sok egymás utáni jel értékét változtatja meg. Az ilyen helyzetekre definiáljuk a hibacsomót.

10.4. Definíció

Egy l-hosszúságú **hibacsomó** egy olyan jelsorozat, amelynek az első és utolsó eleme nem 0 (tehát lehetséges, hogy a közbülső helyeken bizonyos jelek hibátlanok).

Δ

A hibacsomókat is javító egyes kódtípusokkal foglalkozunk a következő részben.

Mivel a k-dimenziós Reed-Solomon kód generátormátrixának bármely k oszlopa lineárisan független, ezért a kódot tetszőleges l pozícióján 0-ra rövidítve egy $k - l$-dimenziós, $n - l$ szóhosszúságú MDS-kódot kapunk, feltéve, hogy $l < k$. Az így kapott kódot **rövidített Reed-Solomon kód**nak nevezzük, és a Reed-Solomon kódokra kidolgozott bármely dekódolási eljárással dekódolhatjuk, ha a vett szót a kihagyott pozíciókon 0-val egészítjük ki. Ugyanezen okból a Reed-Solomon kód jól alkalmazható olyan esetekben is, amikor várhatóan bizonyos hibák helye ismert.

A Reed-Solomon kódok felhasználhatóak a kriptográfiában titokmegosztásra. Titokmegosztásnál n résztvevő mindegyike rendelkezik egy olyan adattal, amelyből akkor lehet megismerni a titkos adatot, ha legalább k résztvevő adata rendelkezésre áll. A kód tulajdonságainak köszönhetően a segítségével megosztott titkot akkor is helyesen kapjuk vissza, ha néhányan hamis adatot szolgáltatnak.

A CD-ken (mind a zenei, mind az adatokat tartalmazó lemezeken) rövidített Reed-Solomon kódokat alkalmaznak, de egyrészt a következő fejezetben tárgyalt direkt szorzat kód formájában, másrészt a blokk-kódnál bonyolultabb konvolúciós kód részeként.

11. Kódkonstrukció II.

Az alábbiakban három konstrukciós eljárást ismertetünk. Előtte azonban lássunk két tételt a hibacsomóról.

11.1. Tétel

Egy $[n,k]_q$-paraméterű C kód hibacsomó-javító képességére fennáll, hogy $l \leq \left\lfloor \frac{n-k}{2} \right\rfloor$, ahol l a javítható hibacsomó hossza.

Δ

Bizonyítás:

Tekintsünk egy tetszőleges nemzérus kódszót, s abban a leghosszabb, nemzérussal kezdődő, s nemzérussal végződő részsorozatot, másként csomót. Tegyük fel, hogy az összes nemzérus kódszót tekintve a legrövidebb ilyen részsorozat hossza $b+1$. Ekkor egy adott kódszópozícióban kezdődő, legfeljebb b hosszú hibacsomóknak megfelelő hibavektorok a szindróma-dekódolás standard elrendezési táblázatában különböző sorokba (mellékosztályokba) kell, hogy essenek, ellenkező esetben két ilyen hibavektor különbsége kódszó lenne, ami ellentmondásra vezetne. Mivel a táblázat sorainak száma q^{n-k}, továbbá a különböző, legfeljebb b-hosszúságú hibacsomók száma q^b, ezért $q^b \leq q^{n-k}$, ahonnan $b \leq n-k$ adódik. Tehát van a kódban olyan kódszó, amelyben a leghosszabb csomó hossza legfeljebb $n-k+1$. Ha ezen kódszóban ezen csomót szétvágjuk két rövidebb csomóra, és az egyiknek vesszük a -1-szeresét, akkor az azoknak megfelelő hibavektorok azonos mellékosztályba kell, hogy essenek, hiszen ezen vektorok különbsége kódszó. Ennélfogva csak egyikük választható mellékosztály-vezetőnek, vagyis javítható hibamintának. Innen már következik, hogy garantálhatóan legfeljebb az $\left\lfloor \frac{n-k}{2} \right\rfloor$-hosszúságú hibacsomók javíthatók.

□

11.2. Megjegyzés

A csomót és hibacsomót ciklikusan tekintjük, vagyis egy b-hosszúságú csomó elhelyezkedhet úgy is a kódszóban, hogy a kódszó utolsó $0 < m < b$ pozícióján, valamint a szó kezdő, $b-m$ pozícióján lévő jegyek alkotják.

Δ

A tételbeli korlát **Reiger-korlát** néven ismert. Azon hibacsomó-javító kódot, amelyre $l = \left\lfloor \frac{n-k}{2} \right\rfloor$ fennáll, **Reiger-optimális**nak hívjuk.

11.3. Tétel

MDS-kód Reiger-optimális.

Δ

Bizonyítás:

MDS-kódban $d = n-k+1$, azaz a kód maximum $\left\lfloor \frac{n-k}{2} \right\rfloor$ egyedi hibát képes javítani. Másrészről, ha egy kód képes t (egyedi) hibát javítani, akkor nyilván ki tud javítani bármilyen, legfeljebb t-hosszúságú hibacsomót. Ezt alkalmazva, MDS-kód esetén $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor \leq l \leq \left\lfloor \frac{n-k}{2} \right\rfloor$, és ebből már közvetlenül adódik az állítás.

□

Ezek után nézzük a következő, elsősorban csomós hibák javítására szolgáló kódkonstukciókat.

Átfűzéses kód

Adott egy $(n, M, d)_q$-paraméterű C kód, valamint a λ pozitív egész szám. A C tetszőleges λ kódszavát egymás alá írva, majd oszlopfolytonosan kiolvasva kapjuk az új kód egy kódszavát:

$$\begin{pmatrix} u_0^{(0)} & \cdots & u_j^{(0)} & \cdots & u_{n-1}^{(0)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ u_0^{(i)} & \cdots & u_j^{(i)} & \cdots & u_{n-1}^{(i)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ u_0^{(\lambda-1)} & \cdots & u_j^{(\lambda-1)} & \cdots & u_{n-1}^{(\lambda-1)} \end{pmatrix} \rightarrow$$

$$\rightarrow \mathbf{u}^T = u_0^{(0)} \dots u_0^{(i)} \dots u_0^{(\lambda-1)} \dots u_j^{(0)} \dots u_j^{(i)} \dots u_j^{(\lambda-1)} \dots u_{n-1}^{(0)} \dots u_{n-1}^{(i)} \dots u_{n-1}^{(\lambda-1)},$$

vagyis $u_{\lambda j+i} = u_j^{(i)}$, ahol $\lambda > i \in \mathbb{N}$ és $n > j \in \mathbb{N}$. Ha a kapott C' kód paraméterei $(n', M', d')_{q'}$, akkor az rögtön látszik, hogy $n' = \lambda n$ és $q' = q$, továbbá az is világos, hogy $M' = M^\lambda$, hiszen a λ sorba egymástól függetlenül a C bármely eleme választható. Ebből az is következik, hogy

$$\mathcal{R}' = \frac{1}{n'} \log_{q'} M' = \frac{1}{\lambda n} \log_q M^\lambda = \frac{1}{n} \log_q M = \mathcal{R},$$

vagyis az új kód sebessége megegyezik az alapkód sebességével. Nézzük még a kód távolságát. Mivel λ pozitív egész szám, ezért M^λ akkor és csak akkor nagyobb, mint 1, ha M is legalább 2, vagyis az új kódnak pontosan akkor van távolsága, ha az eredeti kódnak is volt, tegyük tehát fel, hogy $M \geq 2$. Ha $\mathbf{u}$ és $\mathbf{v} \neq \mathbf{u}$ C' két különböző eleme, akkor legalább egy i-re és j-re $u_j^{(i)} \neq v_j^{(i)}$. De ha $u_j^{(i)} \neq v_j^{(i)}$, akkor $\mathbf{u}^{(i)} \neq \mathbf{v}^{(i)}$, és mivel C távolsága d, ezért $\mathbf{u}^{(i)}$ és $\mathbf{v}^{(i)}$ legalább d helyen különbözik, amiből következik, hogy $\mathbf{u}$ és $\mathbf{v}$ távolsága is legalább d, tehát $d' \geq d$. Most legyen $\mathbf{u}^{(0)}$ és $\mathbf{v}^{(0)}$ a C két olyan eleme, amelyek távolsága d, és legyen $\mathbf{u}$ és $\mathbf{v}$ többi eleme azonos. Ekkor $\mathbf{u}$ és $\mathbf{v}$ távolsága d, vagyis van a kódban két olyan szó, amelyek távolsága d, amiből következik, hogy $d' \leq d$, azaz C' távolsága megegyezik C távolságával, $d' = d$, és C' egy $\left(\lambda n, M^\lambda, d\right)_q$-paraméterű kód.

Felmerül a kérdés, hogy mire jó egy olyan kód, amelyben nagyobb kódhosszúsághoz azonos távolság, vagyis azonos számú javítható hiba tartozik, azaz amelynek a relatív hibajavítóképessége kisebb. Nyilván semmire. Vegyük azonban tekintetbe, hogy bár t-hiba javító kód esetén λ kódszóban összesen λt hiba kijavítható, de ez nem jelenti azt, hogy egymás után küldött λ kódszóban közvetlenül egymás után következő λt számú hibát tudunk javítani. Az új kód azonban képes bármely $l \leq \lambda t$- hosszúságú hibacsomó javítására, ugyanis amennyiben a vett szóban legfeljebb λt hosszú hibacsomó van, akkor ezt a szót oszlopfolytonosan írva a $\lambda \times n$ méretű mátrixba, a hiba minden sorban legfeljebb t egymás melletti elemet érint. Valóban, legyen a hibacsomó első elemének indexe r_1, az utolsóé r_2, a csomó két eleme tartozzon az s_1 és az $s_2 \geq s_1$ indexekhez, és legyen a csomó hossza legfeljebb λt. Ekkor $s_2 - s_1 \leq r_2 - r_1 < \lambda t$. Tegyük fel, hogy az előbbi két hibahely a mátrix azonos, mondjuk az i indexű sorához tartozik. Ekkor $\lambda t > s_2 - s_1 = (\lambda j_2 + i) - (\lambda j_1 + i) = \lambda(j_2 - j_1)$, és mivel $\lambda > 0$, ezért $j_2 - j_1 < t$, vagyis egy-egy eredeti szóban legfeljebb t hiba van, amit az eredeti kód képes kijavítani, és így a teljes vett szót ki tudjuk javítani. Ezzel beláttuk, hogy igaz a következő tétel.

11.4. Tétel

t-hiba javító kódból λ-szoros átfűzéssel kapott kód λt hosszúságú hibacsomót javító kód.

Δ

Most tegyük fel, hogy C egy $[n,k,d]_q$-paraméterű lineáris kód. Ekkor $M = q^k$, míg a λ-szoros átfűzés után $M' = M^\lambda = \left(q^k\right)^\lambda = q^{\lambda k}$. Legyen $\mathbf{u}$ és $\mathbf{v}$ C', a és b a test két eleme. $\lambda n > i \in \mathbb{N}$-re $au_i + bv_i \in \mathbb{F}_q$, így $a\mathbf{u} + b\mathbf{v} \in \mathbb{F}_q^{\lambda n}$. Legyen $a\mathbf{u} + b\mathbf{v} = \mathbf{w}$ és $a\mathbf{u}^{(i)} + b\mathbf{v}^{(i)} = \mathbf{z}^{(i)}$. C lineáris, ezért $\lambda > i \in \mathbb{N}$-re $\mathbf{z}^{(i)} \in C$. Ha $n > j \in \mathbb{N}$ és $l = \lambda j + i$, akkor $w_l = au_l + bv_l = au_j^{(i)} + bv_j^{(i)} = z_j^{(i)}$, vagyis $\mathbf{w}$-t oszlopfolytonosan a mátrixba írva, annak minden sora eleme C-nek, és így $\mathbf{w}$ eleme C'-nek, C' lineáris. De ha C' lineáris, és $M' = q^{\lambda k}$, ahol q a test elemszáma, akkor C' egy λk-dimenziós kód, azaz C' egy $[\lambda n, \lambda k, d]_q$-paraméterű kód.

Végül tegyük fel, hogy C a g generátorpolinommal generált ciklikus kód, és nézzük meg, hogy milyen szót kapunk, ha C' egy elemét ciklikusan egy hellyel jobbra léptetjük.

$$u_0^{(0)} \dots u_0^{(i)} \dots u_0^{(\lambda-1)} \dots u_j^{(0)} \dots u_j^{(i)} \dots u_j^{(\lambda-1)} \dots u_{n-1}^{(0)} \dots u_{n-1}^{(i)} \dots u_{n-1}^{(\lambda-2)} u_{n-1}^{(\lambda-1)}$$
$$\downarrow$$
$$u_{n-1}^{(\lambda-1)} u_0^{(0)} \dots u_0^{(i)} \dots u_0^{(\lambda-1)} \dots u_j^{(0)} \dots u_j^{(i)} \dots u_j^{(\lambda-1)} \dots u_{n-1}^{(0)} \dots u_{n-1}^{(i)} \dots u_{n-1}^{(\lambda-2)},$$

vagy a táblázatos alakban

$$\begin{pmatrix} u_0^{(0)} & \cdots & u_j^{(0)} & \cdots & u_{n-2}^{(0)} & u_{n-1}^{(0)} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ u_0^{(i)} & \cdots & u_j^{(i)} & \cdots & u_{n-2}^{(i)} & u_{n-1}^{(i)} \\ u_0^{(i+1)} & & u_j^{(i+1)} & & u_{n-2}^{(i+1)} & u_{n-1}^{(i+1)} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ u_0^{(\lambda-2)} & \cdots & u_j^{(\lambda-2)} & \cdots & u_{n-2}^{(\lambda-2)} & u_{n-1}^{(\lambda-2)} \\ u_0^{(\lambda-1)} & \cdots & u_j^{(\lambda-1)} & \cdots & u_{n-2}^{(\lambda-1)} & u_{n-1}^{(\lambda-1)} \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} u_{n-1}^{(\lambda-1)} & u_0^{(\lambda-1)} & \cdots & u_j^{(\lambda-1)} & \cdots & u_{n-2}^{(\lambda-1)} \\ u_0^{(0)} & \cdots & u_j^{(0)} & \cdots & u_{n-2}^{(0)} & u_{n-1}^{(0)} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ u_0^{(i-1)} & & u_j^{(i-1)} & & u_{n-2}^{(i-1)} & u_{n-1}^{(i-1)} \\ u_0^{(i)} & \cdots & u_j^{(i)} & \cdots & u_{n-2}^{(i)} & u_{n-1}^{(i)} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ u_0^{(\lambda-2)} & \cdots & u_j^{(\lambda-2)} & \cdots & u_{n-2}^{(\lambda-2)} & u_{n-1}^{(\lambda-2)} \end{pmatrix}$$

Látjuk, hogy a 0. sor az 1. sor helyére került változatlan formában, az i-edik sor az $i+1$-edik helyére, és a $\lambda-2$-edik sor a $\lambda-1$-edik helyére szintén minden változás nélkül, ugyanakkor az utolsó, $\lambda-1$-edik sor felkerült a 0. sor helyére, de ciklikusan egy hellyel jobbra tolva. Mivel az eredeti táblázat minden sora egy-egy C-beli kódszó, és C ciklikus, vagyis bármely kódszavának ciklikus eltoltja is kódszó, ezért a második táblázat valamennyi sorában is C egy-egy kódszava áll, és így ez a táblázat is, oszlopfolytonosan kiolvasva, C' egy kódszava, ami éppen azt jelenti, hogy C' is ciklikus.

Az előbbi eredmény algebrai úton is kijön. A kód egy $\mathbf{u}$ kódszavához tartozó kódszó-polinom az oszlopfolytonos kiolvasásnál

$$u = \sum_{l=0}^{\lambda n-1} u_l x^l = \sum_{i=0}^{\lambda-1}\sum_{j=0}^{n-1} u_{\lambda j+i} x^{\lambda j+i} = \sum_{i=0}^{\lambda-1}\sum_{j=0}^{n-1} u_j^{(i)} x^{\lambda j+i}$$
$$= \sum_{i=0}^{\lambda-1} x^i \sum_{j=0}^{n-1} u_j^{(i)} \left(x^\lambda\right)^j = \sum_{i=0}^{\lambda-1} x^i \left(u^{(i)} \circ x^\lambda\right).$$

Ekkor a polinom eltoltja

$$u_\rightarrow = xu \bmod \left(x^{\lambda n} - e\right) = x \sum_{i=0}^{\lambda-1} x^i \left(u^{(i)} \circ x^\lambda\right) \bmod \left(x^{\lambda n} - e\right)$$
$$= \sum_{i=0}^{\lambda-1} \left(x^{i+1} \left(u^{(i)} \circ x^\lambda\right) \bmod \left(x^{\lambda n} - e\right)\right)$$
$$= \sum_{i=1}^{\lambda-1} \left(x^i \left(u^{(i-1)} \circ x^\lambda\right) \bmod \left(x^{\lambda n} - e\right)\right) + \left(x^\lambda \left(u^{(\lambda-1)} \circ x^\lambda\right) \bmod \left(\left(x^\lambda\right)^n - e\right)\right)$$
$$= \sum_{i=1}^{\lambda-1} x^i \left(u^{(i-1)} \circ x^\lambda\right) + \left(xu^{(\lambda-1)} \bmod \left(x^n - e\right)\right) \circ x^\lambda$$
$$= \sum_{i=1}^{\lambda-1} x^i \left(u^{(i-1)} \circ x^\lambda\right) + x^0 \left(u_\rightarrow^{(\lambda-1)} \circ x^\lambda\right) = \sum_{i=0}^{\lambda-1} x^i \left(v^{(i)} \circ x^\lambda\right),$$

ahol $\mathbf{v}^{(0)} = \mathbf{u}_\rightarrow^{(\lambda-1)}$, és $\lambda > i \in \mathbb{N}^+$-ra $\mathbf{v}^{(i)} = \mathbf{u}^{(i-1)}$. De ha C ciklikus, akkor $\mathbf{v}^{(0)} = \mathbf{u}_\rightarrow^{(\lambda-1)} \in C$, így $\mathbf{u}_\rightarrow \in C'$, a C' kód ciklikus.

Határozzuk meg C' generátorpolinomját, g'-t (a vessző nem a deriválást jelenti). C' egy $[\lambda n, \lambda k, d]_q$-paraméterű ciklikus kód, amelyben a generátorpolinom az egyetlen $\lambda n - \lambda k = \lambda(n-k)$-adfokú főpolinom, tehát ha megadunk egy ilyen polinomot, akkor az lesz a kód generátorpolinomja. Legyen $u^{(0)} = g$, ahol g a C generátor-polinomja, és legyen $\lambda > i \in \mathbb{N}^+$-ra $u^{(i)} = 0$. Ekkor

$$u = \sum_{i=0}^{\lambda-1} x^i \left(u^{(i)} \circ x^\lambda\right) = u^{(0)} \circ x^\lambda = g \circ x^\lambda,$$

tehát u főpolinom, és a fokszáma $\lambda(n-k)$, vagyis $g' = g \circ x^\lambda$. Beláttuk tehát a következőt.

11.5. Tétel

$[n, k, d]_q$-paraméterű C kód λ-szoros átfűzésével kapott C' kód $[\lambda n, \lambda k, d]_q$-paraméterű kód, és ha C ciklikus a g generátorpolinommal, akkor C' is ciklikus a $g' = g \circ x^\lambda$ generátorpolinommal.

Δ

Direkt szorzat kód

Legyen adott egy M_A-elemű A és egy M_B-elemű B üzenethalmaz, egy $(n_1, M_1, d_1)_{q_1}$-paraméterű C_1 kód az S_1 ábécé felett, és egy $(n_2, M_2, d_2)_{q_2}$-paraméterű C_2 kód az S_2 ábécé felett, továbbá egy q-elemű S ábécé, és tegyük fel, hogy $M_A \le q^{k_A} \le M_1$, $M_B \le q^{k_B} \le M_2$, $q_1^{k_A} \le M_1$ és $q_2^{k_B} \le M_2$, ahol k_A és k_B pozitív egész szám. Mivel $M_A \le q^{k_A}$, ezért az A-beli üzeneteket felírhatjuk az S ábécé feletti k_A-hosszúságú szavakként, és ezeket kódolhatjuk a C_1 kóddal, hiszen $q^{k_A} \le M_1$. Most csináljuk azt, hogy k_B számú üzenetet kódolunk az előbb leírt módon, és írjuk egymás mellé a kapott, oszlopként írt kódszavakat, ekkor egy S_1 fölötti $n_1 \times k_B$-méretű táblázatot kapunk:

$$\begin{matrix} u_0^{(0)} & \cdots & u_0^{(j)} & \cdots & u_0^{(k_B-1)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ u_i^{(0)} & \cdots & u_i^{(j)} & \cdots & u_i^{(k_B-1)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ u_{n_1-1}^{(0)} & \cdots & u_{n_1-1}^{(j)} & \cdots & u_{n_1-1}^{(k_B-1)} \end{matrix}.$$

Itt valamennyi $u_i^{(j)}$ eleme S_1-nek, és $q_2^{k_B} \leq M_2$ következtében az előbbi táblázat egy-egy sora kódolható C_2-vel, vagyis egy-egy S_1 feletti, k_B hosszúságú sorozathoz egyértelműen hozzárendelhető egy S_2 fölötti n_2-hosszúságú sorozat, így $u_i^{(0)} \dots u_i^{(j)} \dots u_i^{(k_B-1)}$-et $v_0^{(i)} \dots v_j^{(i)} \dots v_{n_2-1}^{(i)}$-gyel kódolva a

$$\begin{matrix} v_0^{(0)} & \cdots & v_j^{(0)} & \cdots & v_{n_2-1}^{(0)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ v_0^{(i)} & \cdots & v_j^{(i)} & \cdots & v_{n_2-1}^{(i)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ v_0^{(n_1-1)} & \cdots & v_j^{(n_1-1)} & \cdots & v_{n_2-1}^{(n_1-1)} \end{matrix}$$

táblázatot kapjuk. Ha most ezt a táblázatot kiolvassuk úgy, hogy minden eleme egyszer és csak egyszer forduljon elő, akkor az A^{k_A} halmazt egy C_A kóddal kódoltuk. Ez a kód a q_2-elemű S_2 fölötti kód, szóhosszúsága $n = n_1 n_2$, és elemszáma $M_A^{k_B}$. Meg kell még határoznunk a kód távolságát.

Ha A-nak egyetlen eleme van, akkor C_A-ban is csak egy elem van, a kódnak nincs távolsága. Ellenkező esetben tegyük fel, hogy A^{k_A} két különböző elemét kódoljuk. Ekkor a kiinduló két táblázat legalább egy helyen különbözik, és így a C_1-gyel való kódolás után a q_B számú kódszópárok legalább egyike eltérő. Mivel C_1 távolsága d_1, ezért ez a két kódszó legalább d_1 helyen különböző. Ha most a sorokat C_2-vel kódoljuk, akkor azok a kódszópárok, amelyek az előbbi eltérő helyekhez tartoznak, szintén különbözőek, és akkor egy-egy ilyen kódszópár minimum d_2 helyen tér el, hiszen ez a C_2 kód távolsága. Mindebből az következik, hogy a C_A-beli két kódszó eltérése legalább $d_1 d_2$, és így a C_A kód távolsága $d_A \geq d_1 d_2$.

Kiindulhatunk B-ből is. Írjuk fel B elemeit az S betűiből alkotott k_B hosszú szavakként, és írjunk egymás alá k_A ilyen szót. $q^{k_B} \leq M_2$, ezért egy-egy szót kódolhatunk a C_2 kóddal, és így, továbbra is egymás alá írva ezeket a kódszavakat, egy S_2 feletti $k_A \times n_2$ méretű táblázatunk van. Mivel $q_1^{k_A} \leq M_1$, ezért a táblázat egy-egy oszlopa kódolható C_1-gyel, és kódolás után egy S_1 feletti $n_1 \times n_2$-méretű táblázatot kapunk, amelyet valamilyen sorrendben kiolvasva, egy $n_1 n_2$ hosszúságú, S_1 feletti kódszót nyerünk. Az előbbihez hasonlóan kapjuk, hogy így egy $\left(n_1 n_2, M_B^{k_A}, d_B\right)_{q_1}$-paraméterű C_B kódot konstruáltunk, ahol $d_B \geq d_1 d_2$.

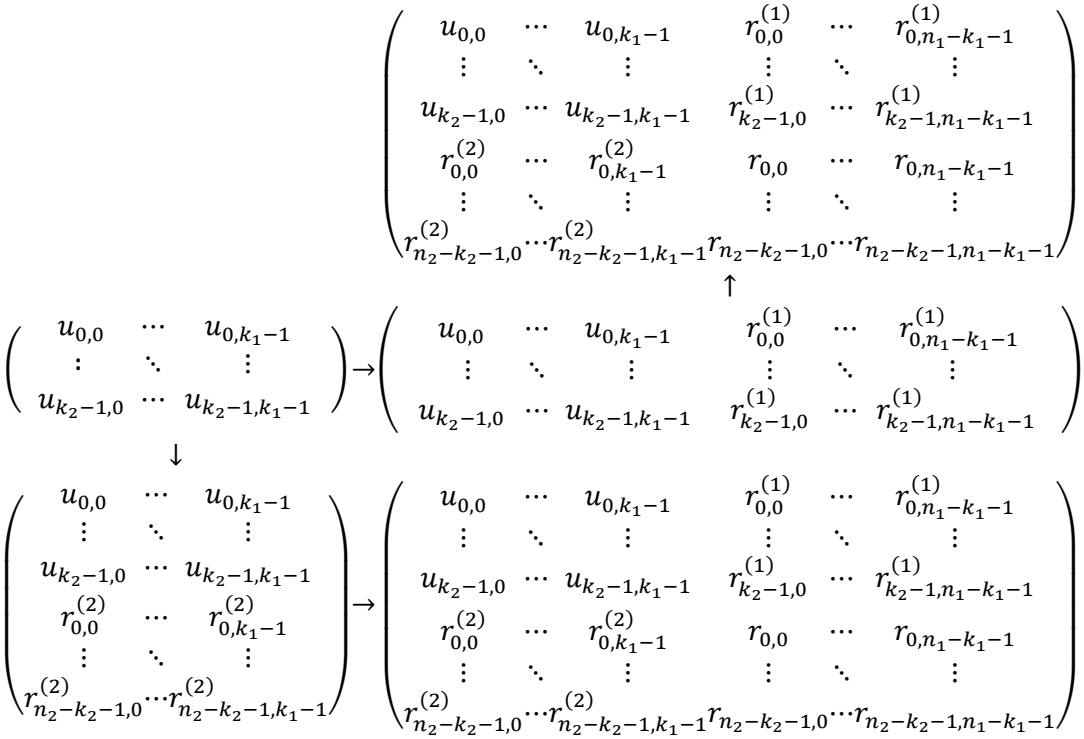
Most nézzük meg a két kód sebességét.

$$\mathcal{R}_A = \frac{1}{n_1 n_2} \log_{q_2} M_A^{k_B} = \frac{k_B}{n_1 n_2} \log_{q_2} M_A \leq \frac{k_B}{n_1 n_2} \log_{q_2} M_1 = \frac{k_B}{n_1 n_2} \frac{\log_{q_1} M_1}{\log_{q_1} q_2}$$
$$= \frac{k_B}{n_2} \log_{q_2} q_1 \frac{1}{n_1} \log_{q_1} M_1 = \mathcal{R}_1 \frac{1}{n_2} \log_{q_2} q_1^{k_B} \leq \mathcal{R}_1 \frac{1}{n_2} \log_{q_2} M_1 = \mathcal{R}_1 \mathcal{R}_2,$$

és teljesen hasonlóan kapjuk, hogy $\mathcal{R}_B \leq \mathcal{R}_1 \mathcal{R}_2$.

Legyen $t_1 = \left\lfloor \frac{d_1 - 1}{2} \right\rfloor$ és $t_2 = \left\lfloor \frac{d_2 - 1}{2} \right\rfloor$. Tegyük fel, hogy A-ból indultunk ki, és a kódolás eredményeképpen kapott táblázatot oszlopfolytonosan olvassuk ki. Amennyiben az átvitel során egy legfeljebb $n_1 t_2$-hosszúságú hibacsomó lép fel, és ezen kívül még olyan véletlen hibák vannak, amelyeket soronként C_2 képes javítani, akkor oszlopfolytonosan visszaírva a vett szót a táblázatba, és C_2-vel kijavítva a véletlen hibákat, a táblázat minden sorában legfeljebb t_2 hiba lesz, amit a C_2 kód képes javítani.

Ugyanígy, ha B-t kódoljuk, és sofolytonos a kiolvasás illetve beírás, akkor a kód képes egy maximum $n_2 t_1$ hosszú hibacsomó, valamint a C_1-gyel javítható további véletlen hibák javítására.



8. ábra

Az előbbieket specializáljuk lineáris kódokra. Legyen adott a q-elemű test fölötti $[n_1, k_1, d_1]_q$-paraméterű C_1 és $[n_2, k_2, d_2]_q$-paraméterű C_2 kód, $\mathbf{G}_1$ és $\mathbf{H}_1$ a C_1, $\mathbf{G}_2$ és $\mathbf{H}_2$ a C_2 kód generátor- és ellenőrző mátrixa, továbbá legyen az üzenethalmaz $q^{k_1 k_2}$-elemű. Ekkor az üzenetek tekinthetőek az $\mathbb{F}_q$ fölötti $k_1 \times k_2$-méretű mátrixoknak (ezt persze úgy is felfoghatjuk, hogy az üzenethalmaz a q-elemű test fölötti k_2-dimenziós tér, és ennek a térnek k_1 üzenetét kódoljuk, illetve a q-elemű test fölötti k_1-dimenziós tér mint üzenettér k_2 elemét kódoljuk). Egy ilyen $\mathbf{U}$ mátrix egy-egy sora kódolható a C_2 kóddal, és $\mathbf{UG}_2$ egy $k_1 \times n_2$-méretű mátrix, amelynek minden sora egy-egy C_2-beli kódszó. Ugyanakkor $\mathbf{UG}_2$ minden oszlopa $\mathbb{F}_q$ fölötti k_1-dimenziós vektor, amely kódolható C_1-ben. Ez a kódolás a $\mathbf{G}_1$-gyel való szorzással végezhető el, és a szorzás után a $\mathbf{V} = ((\mathbf{UG}_2)^T\mathbf{G}_1)^T = \mathbf{G}_1^T\mathbf{UG}_2$ mátrixot kapjuk mint az $\mathbf{U}$ üzenet kódját. De ugyanezt a kódot kapjuk, ha először az $\mathbf{U}$ oszlopait kódoljuk a $\mathbf{G}_1$ mátrixszal, és utána az így kapott mátrix sorait $\mathbf{G}_2$-vel: ebben az esetben az első lépésben az $\mathbf{U}^T\mathbf{G}_1$, majd a második lépés után az $(\mathbf{U}^T\mathbf{G}_1)^T\mathbf{G}_2 = \mathbf{G}_1^T\mathbf{UG}_2$ mátrixot kapjuk, ami éppen az előbbi $\mathbf{V}$ mátrix. Ebből következik, hogy a végső mátrix oszlopai C_1-beli, míg sorai C_2-beli kódszavak. Ez onnan is látszik, hogy $\mathbf{H}_1\mathbf{V} = \mathbf{H}_1(\mathbf{G}_1^T\mathbf{UG}_2) = (\mathbf{H}_1\mathbf{G}_1^T)(\mathbf{UG}_2) = \mathbf{0}$ és $\mathbf{H}_2\mathbf{V}^T = \mathbf{H}_2(\mathbf{G}_1^T\mathbf{UG}_2)^T = (\mathbf{H}_2\mathbf{G}_2^T)(\mathbf{U}^T\mathbf{G}_1) = \mathbf{0}$.

Standard alakú generátormátrixszal az előbbieket a 8. ábra szemlélteti.

Ha $\mathbf{U}_1$ és $\mathbf{U}_2$ két üzenet, és a_1 valamint a_2 az $\mathbb{F}_q$ két eleme, akkor $a_1\mathbf{U}_1 + a_2\mathbf{U}_2$ is $\mathbb{F}_q$ fölötti $k_1 \times k_2$-méretű mátrix, és $\mathbf{G}_1^T(a_1\mathbf{U}_1 + a_2\mathbf{U}_2)\mathbf{G}_2 = a_1\mathbf{G}_1^T\mathbf{U}_1\mathbf{G}_2 + a_2\mathbf{G}_1^T\mathbf{U}_2\mathbf{G}_2$, tehát a kapott kód is lineáris. Meg kell határozni ezen C kód paramétereit. A kódszavak $n_1 \times n_2$-méretű $\mathbb{F}_q$ fölötti mátrixok, így a kódhossz $n = n_1 n_2$. Mivel az üzenetek az $\mathbb{F}_q$ fölötti $k_1 \times k_2$-méretű mátrixokkal reprezentálhatóak, ezért a kód az $\mathbb{F}_q$ fölötti $n_1 n_2$-dimenziós tér $k_1 k_2$-dimenziós altere, $k = k_1 k_2$. A kód távolságához elegendő a kód súlyának meghatározása, hiszen a kód lineáris (feltesszük, hogy az eredeti mindkét kód legalább egydimenziós, és így az eredő kód is tartalmaz nem nulla kódszót). Ha $\mathbf{V}$ nem nulla, akkor a mátrix legalább egy eleme nem nulla. Ha az i-edik oszlopban van nem nulla elem, akkor az i-edik oszlop a C_1 kód nem nulla eleme, és mivel a C_1 távolsága d_1, ezért az i-edik oszlopban legalább d_1 nullától

különböző elem áll, vagyis a mátrixban legalább d_1 nullától különböző sor van. Ezek a sorok C_2-beli nem nulla kódszavak, és így a súlyuk legalább akkora, mint a C_2 kód távolsága, azaz legalább d_2. Ez azt jelenti, hogy legalább d_1 olyan sor van, amelyek mindegyikében legalább d_2 nem nulla elem található, tehát egy nem nulla kódszóban minimum $d_1 d_2$ nullától eltérő elem áll, vagyis a két kódból keletkezett C kód d távolsága legalább $d_1 d_2$. Most legyen $\mathbf{u}^{(1)}$ a C_1 kód egy d_1-súlyú eleme, és $\mathbf{u}^{(2)}$ egy C_2-beli, d_2-súlyú kódszó, továbbá legyen $\mathbf{V}$ egy olyan $n_1 \times n_2$-es mátrix, amelyben $V_{i,j} = u_i^{(1)} u_j^{(2)}$. A $\mathbf{V}$ j-edik oszlopában álló elemek esetén $u_j^{(2)}$ állandó, tehát ez az oszlop az $\mathbf{u}^{(1)}$ C_1-beli kódszó $u_j^{(2)}$-szerese, és így maga is C_1-beli kódszó. Hasonlóan láthatjuk, hogy a mátrix i-edik sora a C_2-beli $\mathbf{u}^{(2)}$ kódszó $u_i^{(1)}$-szerese, tehát C_2-beli kódszó. Mindebből következik, hogy ez a $\mathbf{V}$ eleme C-nek. $V_{i,j} = u_i^{(1)} u_j^{(2)}$ akkor és csak akkor nem nulla, ha mind $u_i^{(1)}$, mind $u_j^{(2)}$ nullától különböző. Összesen d_1 olyan i index van, amelyre $u_i^{(1)} \neq 0$, és azon j indexek száma, amelyekre $u_j^{(2)} \neq 0$, d_2, így $\mathbf{V}$ súlya $d_1 d_2$, amiből következik, hogy a kód súlya legfeljebb ekkora. Mivel korábban azt találtuk, hogy a kód súlya legalább $d_1 d_2$, ezért $d = d_1 d_2$, tehát C egy $[n_1 n_2, k_1 k_2, d_1 d_2]_q$-paraméterű lineáris kód. Beláttuk tehát a következő tételt.

11.6. Tétel

Legyen C_1 egy $[n_1, k_1, d_1]_q$-paraméterű kód a $\mathbf{G}_1$ és C_2 egy $[n_2, k_2, d_2]_q$-paraméterű kód a $\mathbf{G}_2$ generátormátrixszal. Ekkor az $\mathbb{F}_q^{k_1 \times k_2}$ elemein az $\mathbf{U} \mapsto \mathbf{G}_1^T \mathbf{U} \mathbf{G}_2$ szabállyal értelmezett C kód egy $[n_1 n_2, k_1 k_2, d_1 d_2]_q$-paraméterű lineáris kód.

Δ

11.7. Definíció

Legyen C_1 a $\mathbf{G}_1$ és C_2 a $\mathbf{G}_2$ generátormátrixszal generált kód, és legyen $\mathbf{U} \in \mathbb{F}_q^{k_1 \times k_2}$. Ekkor az $\mathbf{U} \mapsto \mathbf{G}_1^T \mathbf{U} \mathbf{G}_2$ szabállyal értelmezett C kód a C_1 **és** C_2 **direkt szorzata**, egy **direkt szorzat kód**.

Δ

Mivel a direkt szorzat kódban a kódszavak olyan mátrixoknak tekinthetőek, amelyeknek mind a sorai, mind az oszlopai egy-egy kód elemei, ezért megpróbálhatjuk a hibajavítást oly módon, hogy először például soronként javítunk a C_2 kód alapján, majd az ily módon javított mátrix oszlopait javítjuk a C_1-beli döntési függvény alapján. Ilyen módszerrel azonban nem használjuk ki az összetett kód hibajavító képességét. A C_2 kód távolsága d_2, így soronként $t_2 = \left\lfloor \frac{d_2 - 1}{2} \right\rfloor$ hiba javítható, míg az oszloponként javítható hibák száma $t_1 = \left\lfloor \frac{d_1 - 1}{2} \right\rfloor$, hiszen a C_1 kód távolsága d_1, vagyis összességében a soronként és oszloponként elkülönítetten történő hibajavítás esetén $t_1 t_2$ hiba javítható. Ennél valamivel jobb a helyzet. Ha ugyanis a hibák száma kisebb, mint $(t_1 + 1)(t_2 + 1)$, akkor ez soronkénti és oszloponkénti javítással kijavítható. Ekkor ugyanis az olyan sorok száma, amelyben t_2-nél több hiba van, legfeljebb t_1, így a soronkénti javítás után legfeljebb t_1 sorban marad hiba (nem feltétlenül az eredeti pozíciókban). Ez viszont azt jelenti, hogy minden oszlopban legfeljebb t_1 hiba van, amelyeket az oszloponkénti javítással meg lehet szüntetni.

Most legyen $\mathbf{u}^{(1)}$ a C_1 egy d_1-súlyú, míg $\mathbf{u}^{(2)}$ a C_2 egy d_2-súlyú kódszava, és legyen $\mathbf{v}^{(1)}$ az $\mathbf{u}^{(1)}$ valamely $\left\lfloor \frac{d_1}{2} \right\rfloor$, $\mathbf{v}^{(2)}$ pedig az $\mathbf{u}^{(2)}$ valamely $\left\lfloor \frac{d_2}{2} \right\rfloor$ karakterének 0-val való helyettesítésével előálló szó. $\mathbf{v}^{(1)}$ a C_1 kód $\mathbf{0}$ kódszavából $d_1 - \left\lfloor \frac{d_1}{2} \right\rfloor = \left\lceil \frac{d_1}{2} \right\rceil$ hibával keletkező szó. Páratlan d_1-nél ez $t_1 + 1$ hiba, és mivel a test bármely nullától különböző c eleme esetén $c\mathbf{u}^{(1)}$ $c\mathbf{v}^{(1)}$-től vett távolsága csak t_1, ezért $c\mathbf{v}^{(1)}$ esetén a kód $c\mathbf{u}^{(1)}$-re dönt, vagyis a dekódolás eredményeként nem az elküldött kódszót kapjuk, a dekódolás hibás eredményt ad. Ha d_1 páros, akkor mind az eredeti kódszó, $\mathbf{0}$, mind $\mathbf{u}^{(1)}$ azonos távolságra van $\mathbf{v}^{(1)}$-től, és ez az azonos, nem nulla konstansszorosokra is igaz, ezért a dekódoló vagy nem dönt, vagy, ha dönt, akkor bármelyikre (de adott rendszeren belül mindig ugyanúgy) dönt. Tegyük fel, hogy

most a dekódoló dönt, és $\mathbf{u}^{(1)}$-re, illetve a megfelelő konstansszorosára dönt, ekkor a helyzet ugyanaz, mint a páratlan távolság esetén. Ha a szorzatkód üzenete a csupa 0-ból álló mátrix, és a vett szó, visszaírva a mátrixba, olyan, hogy az (i,j) indexpárhoz tartozó elem $v_i^{(1)}v_j^{(2)}$, akkor a mátrix i-edik sorában a $\mathbf{v}^{(2)}$ szó $v_i^{(1)}$-szerese lesz, vagyis t_1+1 sor lesz a csupa 0-t tartalmazó sortól eltérő sor. Ezen sorok „javítása" után a mátrixunk (i,j)-indexű helyén $v_i^{(1)}u_j^{(2)}$ lesz, hiszen a nem $\mathbf{0}$ sorokban $v_i^{(1)}\mathbf{v}^{(2)}$-nél a dekódoló $v_i^{(1)}\mathbf{u}^{(2)}$-re dönt. A sorkorrekciók után a mátrx minden sora $\mathbf{u}^{(2)}$ egy konstansszorosa (különböző indexű sor általában más és más konstanssal), az i-edik sor az $\mathbf{u}^{(2)}$ $v_i^{(1)}$-szerese, ezért a mátrix minden oszlopa a $\mathbf{v}^{(1)}$ konstansszorosa, közelebbről a j-edik oszlop a $\mathbf{v}^{(1)}$ $u_j^{(2)}$-szerese lesz. Az oszloponkénti javítás során ebből az oszlopból $\mathbf{u}^{(1)}u_j^{(2)}$ lesz, a végeredményként kapott mátrix tehát az i-edik sor j-edk oszlopában $u_i^{(1)}u_j^{(2)}$-t tartalmazza. Ebben a mátrixban minden sor és minden oszlop az adott kód kódszava, tehát egy olyan mátrix, amelyben a hibák száma minden sorban és minden oszlopban nulla. Ugyanakkor a nullától különböző elemek száma nem nulla (pontosan d_1d_2, de a lényeg csak annyi, hogy nagyobb, mint 0), a dekódolás eredményeként nem az eredeti kódszót kapjuk, a dekódolás helytelen eredményt ad. A vett mátrixban a hibák száma a nullától különböző elemek száma, tehát $(t_1+1)(t_2+1)$ volt, ezt a hibamintát a dekódoló nem az eredeti kódszóra módosította, vagyis ez a hibaminta a soronkénti és oszloponkénti külön javítással nem javítható, így van olyan $(t_1+1)(t_2+1)$ hibát tartalmazó hibaminta, amelyet a szeparált javítással nem lehet javítani. Ez mutatja, hogy van olyan $(t_1+1)(t_2+1)$ hibát tartalmazó hibaminta, amely a külön-külön soronként és oszloponként végrehajtott javítással nem javítható.

Ugyanakkor a direkt szorzat kód távolsága $d=d_1d_2$, ennélfogva ez a kód $t=\left\lfloor\frac{d-1}{2}\right\rfloor=\left\lfloor\frac{d_1d_2-1}{2}\right\rfloor$ hibát képes javítani minimális távolságú dekódolással, tehát, ha $t\geq(t_1+1)(t_2+1)$, akkor a soronkénti-oszloponkénti javítással nem használjuk ki teljes mértékben a kód hibajavító képességét. Az előbbi egyenlőtlenség másként $t+1>(t_1+1)(t_2+1)$. Legyen $d_1=2k_1+\varepsilon_1$ és $d_2=2k_2+\varepsilon_2$, ahol k_1 és k_2 nemnegatív egész szám, és ε_1 valamint ε_2 egyaránt $\{0,1\}$ eleme. Ha $\varepsilon\in\{0,1\}$, akkor könnyűű ellenőrzésel kapjuk, hogy $\varepsilon=\left\lfloor\frac{\varepsilon+1}{2}\right\rfloor$. Most $t+1=\left\lfloor\frac{d_1d_2+1}{2}\right\rfloor=2k_1k_2+k_1\varepsilon_2+k_2\varepsilon_1+\varepsilon_1\varepsilon_2$, és hasonló módon $(t_1+1)(t_2+1)=\left\lfloor\frac{d_1+1}{2}\right\rfloor\cdot\left\lfloor\frac{d_2+1}{2}\right\rfloor=(k_1+\varepsilon_1)(k_2+\varepsilon_2)=k_1k_2+k_1\varepsilon_2+k_2\varepsilon_1+\varepsilon_1\varepsilon_2$ lesz., így az eredeti egyenlőtlenség a $k_1k_2>0$ feltételre egyszerűsödik, ami pontosan akkor teljesül, ha a bal oldalon mindkét tényező legalább 1. Azt kaptuk tehát, hogy $t\geq(t_1+1)(t_2+1)$ pontosan akkor igaz, ha mindkét kód távolsága legalább 2.

Ha például egy n darab m-bites bináris szóból álló adatblokk minden szavát kiegészítjük egy-egy paritásbittel, és a blokk valamennyi, az egyes szavakban azonos pozíción álló bitekből álló oszlopát is megtoldjuk egy paritásbittel, akkor ha mindkét irányban párosra egészítünk ki, a keletkezett kód lineáris, és az eredeti szavak paritásbitjeiből álló oszlop ellenőrzőbitje megegyezik az oszlopok ellenőrző bitjeiből álló szó paritásbitjével. Most mind a soronként, mind az oszloponként alkalmazott kód távolsága 2, vagyis külön-külön egyik sem alkalmas hibajavításra, ugyanakkor a direkt szorzat kód távolsága 4, tehát képes egy hiba javítására és két hiba jelzésére. Az egy hiba úgy javítható, hogy egyetlen hiba esetén pontosan egy sorban és egy oszlopban kapunk hibajelzést, és a jelzett sor és jelzett oszlop metszéspontjában áll a hibás bit, amelyet az ellentettjére változtatva kijavítottuk a hibát. Ám ha két hiba van, akkor legalább két sorban, vagy minimum két oszlopban kapunk hibajelzést, ami mutatja, hogy legalább két hiba lépett fel, amit a kód már nem tud (és nem is kell, hogy tudjon) javítani.

Másik példaként legyen mindkét kód 7-hosszúságú bináris Hamming-kód. Ha mondjuk a 0. és 1. sorban a 0. és 1. oszlopban lép fel hiba, azaz összesen négy hiba keletkezik, akkor a soronkénti „javítás" megváltoztatja a 0. és 1. sor 2. oszlopában álló biteket, majd az oszloponkénti „javítás" során invertáljuk a 0., 1. és 2. oszlop 2. sorának bitjeit, vagyis az eredeti négy hiba helyett kilenc hiba lesz a blokkban, ám ez a módosított táblázat már olyan, amelynek minden sora és minden oszlopa kódszó, vagyis maga a hétszer hetes táblázat is kódszó. Most tehát a négy hibát tartalmazó szót rosszul javítottuk, holott a kód képes lenne négy hibát javítani, hiszen az eredeti két kód távolsága 3, vagyis a direkt szorzat kód távolsága 9. Ennek ellenére gyakran alkalmazzuk a szeparált dekódolást, de iterálva. Azt tudjuk, hogy sor-oszlop javítással biztosan javítható $2\times2-1=3$ hiba, és van olyan négy hibából álló hibaminta,

amelyet a kód nem tud javítani. Ez azonban nem jelenti azt, hogy egyetlen négy hibából álló hibaminta sem javítható sor-oszlop javítással. Nézzük például az előbbi két kódból konstruált direkt szorzat kódot a következő hibamintával:

$$\begin{pmatrix} 1&1&0&0&0&0&0\\ 0&1&0&1&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0 \end{pmatrix}$$

Most ismét négy hiba van. Kezdjük a dekódolást soronként. Ekkor a következő táblázatot kapjuk:

$$\begin{pmatrix} 1&1&1&0&0&0&0\\ 0&1&0&1&0&1&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0 \end{pmatrix}$$

majd az oszloponkénti javítás után

$$\begin{pmatrix} 0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0 \end{pmatrix}$$

Most még három hiba van, és a soronkénti ellenőrzésnél nem mindegyik szindróma értéke 0. Ám ha ismét javítunk soronként, akkor ez a három hiba eltűnik, hiszen minden sorban legfeljebb egy hiba van, és olyan táblánk lesz, amely sem a sorokban, sem az oszlopokban nem tartalmaz hibát, és valóban a hibákat javítottuk ki. Ha a dekódolást az oszlopokkal kezdenénk, akkor már csak egy oszlopban maradna hiba, tehát soronként legfeljebb csak egy hibát kellene javítani, amire az eredeti kód képes.

A direkt szorzat kód, mint korábban az általános esetben láttuk, jól használható hibacsomó javítására. Az adatátvitel során a kétdimenziós kódszó jeleit általában sorosan továbbítják, így a táblázatot általában – de nem mindig, mint azt később látjuk – soronként vagy oszloponként olvassuk ki, és a vétel helyén hasonlóan töltjük fel a táblázatot a javítás előtt. Most tegyük fel, hogy az oszlopfolytonos olvasást alkalmazzuk, és az átvitel során egy t_2n_1-nél nem hosszabb hibacsomó lépett fel. Ekkor a táblázatba való beírás után az egyes sorokban legfeljebb t_2 hiba van. Amennyiben más hiba nincs, akkor a sorirányú javítás esetén a teljes hibát ki tudjuk javítani, vagyis a kód oszlopfolytonos átvitel esetén képes bármely legfeljebb t_2n_1 hosszú hibacsomó javítására. Hasonlóan kapjuk, hogy sorfolytonos alkalmazás esetén a t_1n_2-nél nem hosszabb hibacsomókat tudjuk a kóddal javítani, így a megfelelő irányú működéssel $\max\{t_2n_1, t_1n_2\}$-hosszúságú hibacsomó javítására alkalmas a kód.

A lineáris direkt szorzat kód kódsebessége könnyen meghatározható, hiszen

$$\mathcal{R} = \frac{1}{n_1n_2}\log_q M = \frac{1}{n_1n_2}\log_q q^{k_1k_2} = \frac{k_1k_2}{n_1n_2} = \frac{k_1}{n_1}\frac{k_2}{n_2} = \mathcal{R}_1\mathcal{R}_2.$$

Végül vizsgáljuk a kód ciklikusságát. Sor- illetve oszlopfolytonos működés esetén hiába ciklikus mindkét kód, a direkt szorzat kód nem ciklikus. Ha mondjuk oszlopfolytonos a kiolvasás, akkor az egy hellyel való ciklikus jobbraléptetés során például a második oszlopban álló kódszó úgy módosul, hogy az utolsó jegye elvész, míg az elejére az első oszlop utolsó jegye kerül, és ez a jelsorozat általában nem kódszó (a sorokkal a helyzet ugyanaz, mint az átfűzéses kódnál, vagyis az egyes sorok egy sorral lejjebb kerülnek, míg az utolsó sor a 0. sor helyére megy, egy hellyel ciklikusan jobbra léptetve, tehát sorirányban nincs probléma, ám a direkt szorzat kódban oszloponként is kódszavaknak kell állnia, és ez nem teljesül a teljes kód egy hellyel való elléptetése esetén, ha a kódot oszlopfolytonosan olvassuk – és nyilván a sorirány sérülne sorfolytonos kiolvasásnál). Próbáljuk megállapítani, hogy van-e olyan kiolvasás, amikor ciklikus kódokból ciklikus kódot kapunk. Az természetesen feltétel, hogy a kiolvasásnál minden $n_1 > i \in \mathbb{N}$ és $n_2 > j \in \mathbb{N}$ indexpár egy és csak egy $n_1 n_2 > l \in \mathbb{N}$ indexnek feleljen meg.

Amennyiben mindkét kód valamennyi kódszava konstans, vagyis minden kódszóban egy adott elem és csak ez az elem fordul elő (ez az ismétléses kód), akkor a szorzatkód is ilyen tulajdonságú, és ekkor bármely olyan kiolvasásnál, ahol minden jegy pontosan egyszer szerepel, az összetett kód is ciklikus. Legyen a kiolvasott szóban az l indexhez tartozó elem a táblázat (i,j)-indexű eleme, és legyen $l' = (l+1)^{(n_1 n_2)}$ a következő elem a kiolvasás sorrendjében, ahol $a^{(b)} = a \bmod b$. Ez az elem az (i',j') helyen áll. Ha minden (i,j) indexpárra teljesül, hogy az $\left((i+1)^{(n_1)}, j\right)$ helyen álló elemet az $\left((i'+1)^{(n_1)}, j'\right)$ pozícióra eső elem követi, míg az $\left(i, (j+1)^{(n_2)}\right)$ rácsponthoz tartozó elemet követő elem indexpárja $\left(i', (j'+1)^{(n_2)}\right)$, akkor tetszőleges, rögzített (i_0, j_0) és bármilyen r valamint s egész szám esetén $\left((i_0+r)^{(n_1)}, (j_0+s)^{(n_2)}\right)$ után az $\left((i_0'+r)^{(n_1)}, (j_0'+s)^{(n_2)}\right)$ indexpár következik. Ez azt jelenti, hogy $(i_0', (j_0+s)') = (i_0', j_0'+s)$, vagyis az eltolás után a mátrix i_0' indexű sorában az eredeti mátrix i_0 indexű sorának ciklikus eltoltja, tehát a C_2 kód egy kódszava áll, hiszen most C_2 ciklikus. Ugyanilyen megfontolással a j_0 indexű oszlop ciklikus eltoltja az eltolással átkerül a j_0' indexű oszlopba, ahol most a C_1 kód egy kódszava lesz, hiszen ez a kód is ciklikus. Ha tehát a kiolvasás olyan, hogy jobb szomszédot jobb szomszéd, alsó szomszédot alsó szomszéd követ a mátrix minden pozícióján, akkor ciklikus kódok szorzata is ciklikus.

Ha az előbb említett feltétel teljesül, akkor bármely (r,s) egész számpár esetén teljesül, hogy $\left((i_0'+r)^{(n_1)} - (i_0+r_1)^{(n_1)}\right)^{(n_1)} = (i_0' - i_0)^{(n_1)}$ és $\left((j_0'+s)^{(n_2)} - (j_0+s)^{(n_2)}\right)^{(n_2)} = (j_0' - j_0)^{(n_2)}$, vagyis minden (i,j)-re $(i',j') = \left((i+r)^{(n_1)}, (j+s)^{(n_2)}\right)$ az $r = (i_0' - i_0)^{(n_1)}$ és $s = (j_0' - j_0)^{(n_2)}$ jelöléssel. Tegyük tehát fel, hogy egy elem kiolvasása után a tőle s pozícióval jobbra és r pozícióval lejjebb álló elem következik, ahol a jobbra illetve lefelé lépést egyaránt ciklikusan értjük, vagyis ha egy adott l-re $u_l = u_{i,j}$, akkor ezen l esetén $u_{l+1} = u_{(i+r)^{(n_1)}, (j+s)^{(n_2)}}$. Ha most minden elemre teljesül, hogy jobb oldali szomszédjának, illetve az alatta álló elemnek a rákövetkezője az ő utána következő elem jobb oldali szomszédja illetve alatta álló elem (természetesen ismét mindenütt ciklikusan értve), akkor tehát a szorzatkód kódszavának egy hellyel való ciklikus elléptetésekor a táblázat bármely sora egyetlen sorba megy át s hellyel ciklikusan jobbra léptetve, és minden oszlop egyetlen oszlopba megy át r pozícióval való lefelé léptetéssel, amint a 9. ábra (111. oldal) mutatja. Ekkor, mivel a táblázat minden sora és minden oszlopa egy-egy ciklikus kód eleme, az áthelyezés után is olyan táblázatot kapunk, amelynek minden sora és minden oszlopa benne van a megfelelő kódban, vagyis az elléptetett kódszó eleme a szorzatkódnak, a direkt szorzat ciklikus kód. Kérdés, mi a feltétele, hogy minden elem szomszédjára (jobbra és lefelé) következő elem a rákövetkező elem megfelelő szomszédjába kerüljön. Ez nyilván teljesül, ha valamennyi elemre igaz, hogy a kiolvasás során a következő elemet az ettől az elemtől jobbra s és lefelé r pozícióval álló helyről vesszük, vagyis minden l indexre teljesül, hogy ha $u_l = u_{i,j}$, akkor $u_{l+1} = u_{(i+r)^{(n_1)}, (j+s)^{(n_2)}}$. Ennek szükséges és elégséges, hogy pontosan $n_1 n_2$ lépés után érjünk először egy olyan elemhez, amelyben már jártunk, és akkor ez az elsőként ismétlődő elem éppen a kiinduló elem lesz. A feltétel tehát az, hogy $n_1 n_2$ legyen az a legkisebb pozitív egész m szám, amellyel $i + mr \equiv i\ (n_1)$ és $j + ms \equiv j\ (n_2)$ teljesül, azaz m legyen a legkisebb pozitív egész, hogy $n_1 | mr$ és $n_2 | ms$. Innen $\frac{n_1}{(n_1,r)} \Big| m$ és $\frac{n_2}{(n_2,s)} \Big| m$, és ekkor $m = \left[\frac{n_1}{(n_1,r)}, \frac{n_2}{(n_2,s)}\right]$. $[a,b] = \frac{ab}{(a,b)} \leq ab$, és egyenlőséget akkor kapunk, ha $(a,b) = 1$, így $m = n_1 n_2$ pontosan akkor lehetséges, ha $\frac{n_1}{(n_1,r)} = n_1$ és $\frac{n_2}{(n_2,s)} = n_2$, vagyis ha $(n_1, r) = 1$ és $(n_2, s) = 1$, valamint $(n_1, n_2) = 1$. Tehát ha n_1 és n_2 relatív prímek, akkor tetszőleges, az n_1-hez relatív prím r-rel és az n_2-höz relatív prím s-sel ciklikus lesz a direkt szorzat kód, ha egy

kiolvasott elem után a tőle ciklikusan s pozícióval jobbra és r pozícióval lefelé álló elemet olvassuk ki. A tetszőleges, de rögzített (i_0, j_0) indextől kezdve a kiolvasást $u_l = u_{(i_0+lr) \bmod n_1,(j_0+ls) \bmod n_2}$ szerint végezzük, ahol $n_1 n_2 > l \in \mathbb{N}$.

$$\begin{pmatrix} & u_{0,j} & & \\ & \vdots & & \\ u_{i,0} \cdots & u_{i,j} & \cdots \cdots \cdots \cdots \cdots \cdots & u_{i,n_1-s-1}\ u_{i,n_1-s} \cdots u_{i,n_1-1} \\ & \vdots & & \\ & \vdots & & \\ & \vdots & & \\ & \vdots & & \\ & \vdots & & \\ & \vdots & & \\ & u_{n_2-r-1,j} & & \\ & u_{n_2-r,j} & & \\ & \vdots & & \\ & u_{n_2-1,j} & & \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} & & u_{n_2-r,j} & & \\ & & \vdots & & \\ & & \vdots & & \\ & & \vdots & & \\ & & u_{n_2-1,j} & & \\ & & u_{0,j} & & \\ & & \vdots & & \\ u_{i,n_1-s} \cdots \cdots \cdots u_{i,n_1-1}\ u_{i,0} \cdots & & u_{i,j} & \cdots \cdots \cdots \cdots u_{i,n_1-s-1} & \leftarrow i+r \\ & & \vdots & & \\ & & \vdots & & \\ & & \vdots & & \\ & & \vdots & & \\ & & u_{n_2-r-1,j} & & \end{pmatrix}$$

$$\uparrow$$

$$j+s$$

9. ábra

Az előbbi kiolvasási sorrend nem változtat a hibacsomó-javító képességen. Ha a hibacsomó hossza L, akkor a soronkénti hibák száma $\left\lfloor \frac{L}{n_1} \right\rfloor \leq h_s \leq \left\lceil \frac{L}{n_1} \right\rceil$, míg az oszloponkénti hibák száma az előbbihez hasonlóan $\left\lfloor \frac{L}{n_2} \right\rfloor \leq h_o \leq \left\lceil \frac{L}{n_2} \right\rceil$, ez pedig éppen azt jelenti, hogy ha $L \leq t_2 n_1$, akkor soronkénti, $L \leq t_1 n_2$ esetén pedig oszloponkénti javítással meg tudjuk szüntetni a hibát.

1 minden egészhez relatív prím, ezért mind r, mind s lehet 1, azaz a táblázat bal felső sarkából indulva mindig az eggyel jobbra és eggyel lejjebb álló elem következik (természetesen ciklikusan értve).

Ha például $n_1 = 7$ és $n_2 = 5$, akkor az alábbi kiolvasással ciklikus kódot kapunk, feltéve, hogy az eredeti két kód ciklikus volt:

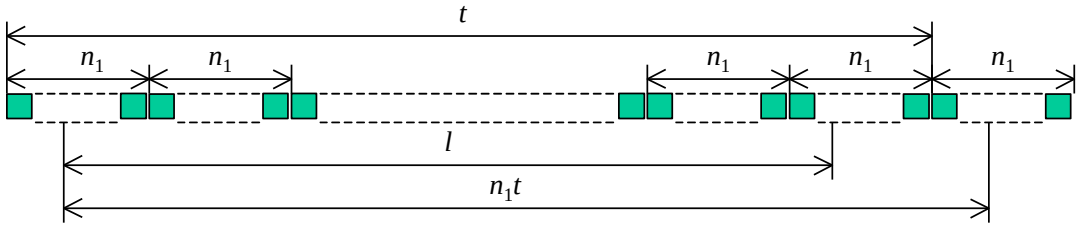
$$\begin{pmatrix} 0 & 15 & 30 & 10 & 25 & 5 & 20 \\ 21 & 1 & 16 & 31 & 11 & 26 & 6 \\ 7 & 22 & 2 & 17 & 32 & 12 & 27 \\ 28 & 8 & 23 & 3 & 18 & 33 & 13 \\ 14 & 29 & 9 & 24 & 4 & 19 & 34 \end{pmatrix}$$

Kaszkád kód

Ismét két kódból alkotunk egy újat, amely alkalmas hibacsomók javítására. Legyen C_1 a q_1-elemű S_1 ábécé feletti $(n_1, M_1, d_1)_{q_1}$-paraméterű, C_2 a q_2-elemű S_2 ábécé feletti $(n_2, M_2, d_2)_{q_2}$-paraméterű kód, és A egy M-elemű üzenethalmaz, ahol $M \leq q_2 \leq q_1^{k_1} \leq M_1$, $M^{k_2} \leq M_2$ valamilyen k_1 és k_2 pozitív egésszel. Ekkor megadhatunk egy $\varphi: S_2 \to S_1^{k_1}$ injekcót, valamint egy olyan $\psi: M \to S_1^{k_1}$ injektív leképezést, hogy $\mathrm{Im}(\psi) \subseteq \mathrm{Im}(\varphi)$. Most legyen $\mathbf{u}^T = u^{(0)} \dots u^{(k_2-1)} \in M^{k_2}$, és kódoljuk külön-külön $\mathbf{u}$ valamennyi komponensét ψ-vel, így egy S_1 fölötti k_1k_2-hosszúságú szót kapunk. Egy-egy k_1-hosszúságú szakasznak feleltessük meg azt az S_2-beli betűt, amelynek a képe éppen ez az S_1 feletti k_1-hosszúságú szó, ily módon egy S_2 feletti k_2-hosszúságú szót nyerve. Mivel $M^{k_2} \leq M_2$, ezért az ilyen szavak kódolhatóak C_2-vel, vagyis u-hoz hozzárendelhetjük C_2 elemeit. A hozzárendelés eredménye egy S_2 feletti n_2-hosszúságú szó. Ha most ennek a szónak mindenegyes betűjét leképezzük φ-vel, akkor egy-egy betű képét kódolva a C_1 kóddal, egy S_1 feletti n_1n_2-hosszúságú szó keletkezik, vagyis A^{k_2} elemeit S_1 feletti n_1n_2 hosszúságú szavakkal kódoltuk, azaz egy C kódot kaptunk.

Határozzuk meg az új kód paramétereit. A kód kódszavainak hossza n_1n_2, a kód mérete M^{k_2}, tehát C egy $\left(n_1n_2, M^{k_2}, d\right)_{q_1}$-paraméterű kód, ahol d még ismeretlen. Ha A^{k_2} két különböző elemét kódoljuk, akkor az első, C_2-vel való kódolás eredményeként két különböző kódszót kapunk, amelyek legalább d_2 helyen különböznek, vagyis a két kódszóban legalább d_2 különböző betű van. Mivel különböző betűknek különböző C_1-beli kódszó felel meg, és két eltérő C_1-beli kódszó minimum d_1 helyen tér el, ezért a két üzenet kódjának távolsága legalább d_1d_2, a C kód távolsága $d \geq d_1d_2$.

A távolságok alapján C_2 ki tud javítani bármely $t = \left\lfloor \frac{d_2-1}{2} \right\rfloor$-nél nem több hibát minimális távolságú dekódolással. Amennyiben egy kódszó az átvitel során úgy sérül meg, hogy az egyes n_1-hosszúságú szakaszokat mint C_1-beli kódszavakat javítva, egy legfeljebb $n_1(t-1)+1$-hosszúságú hibacsomó marad, akkor az n_1 hosszú szakaszokat visszaírva az eredeti k_1 hosszúságú S_1 feletti szavakká, majd ezeket a megfelelő S_2-beli betűvel helyettesítve, egy olyan S_2 feletti n_2-hosszúságú szót kapunk, amely legfeljebb t hibát tartalmaz, és ezt C_2 képes javítani, vagyis C ki tud javítani egy legfeljebb $n_1(t-1)+1$ hosszúságú hibacsomót (10. ábra):



10. ábra

A kódolás most a 11. ábra szerint néz ki. Az ábra alapján érthető, hogy C_1-et belső, míg C_2-t külső kódnak nevezik.

11. ábra

11.8. Definíció

Ha egy üzenetet egy C_2 kóddal kódolva, a kódszavak betűit egy C_1 kóddal kódoljuk, akkor az így kapott C kód egy **kaszkád kód**, ahol C_2 a **külső kód**, és C_1 a **belső kód**.

Δ

Állapítsuk meg a kaszkád kód kódsebességét.

$$\mathcal{R} = \frac{1}{n_1 n_2}\log_{q_1} M^{k_2} \le \frac{1}{n_1 n_2}\log_{q_1} M_2 = \frac{1}{n_1 n_2}\log_{q_2} M_2 \log_{q_1} q_2$$
$$= \left(\frac{1}{n_1}\log_{q_1} q_2\right)\left(\frac{1}{n_2}\log_{q_2} M_2\right) = \left(\frac{1}{n_1}\log_{q_1} q_2\right)\mathcal{R}_2 \le \left(\frac{1}{n_1}\log_{q_1} M_1\right)\mathcal{R}_2 = \mathcal{R}_1\mathcal{R}_2$$

tehát az $\mathcal{R}_1$ sebességű C_1 és $\mathcal{R}_2$ sebességű C_2 kódból konstruált kaszkád kód sebessége $\mathcal{R} \le \mathcal{R}_1\mathcal{R}_2$.

Egyszerű a helyzet, ha C_2 egy $[n_2, k_2, d_2]_{q_2}$-, míg C_1 egy $[n_1, k_1, d_1]_{q_1}$-paraméterű kód, ahol $q_2 = q_1^{k_1}$. Ha most $\mathbb{F}_{q_1}^{k_1 k_2}$ az üzenettér, akkor egy-egy üzenet az $\mathbb{F}_{q_1}$ elemeiből álló $k_1 k_2$-hosszúságú sorozat. Ennek minden k_1-hosszúságú szakasza kölcsönösen egyértelműen leképezhető $\mathbb{F}_{q_2}$-be, és a leképezés után egy $\mathbb{F}_{q_2}$ feletti k_2-hosszúságú szót kapunk, amely C_2-vel szintén egy $\mathbb{F}_{q_2}$ feletti n_2-hosszúságú szóba kódolható. Ennek a szónak minden betűje visszaírható egy $\mathbb{F}_{q_1}$ fölötti k_1-hosszúságú szóba, és ez C_1-gyel kódolva $\mathbb{F}_{q_1}$ fölötti n_1-hosszúságú szót ad, vagyis végeredményként az $\mathbb{F}_{q_1}$ test fölötti $k_1 k_2$-hosszúságú üzenetet egy $\mathbb{F}_{q_1}$ fölötti $n_1 n_2$-hosszúságú kódszóba kódoltunk, tehát így egy $[n_1 n_2, k_1 k_2, d]_{q_1}$-paraméterű C kódot kapunk. Azt a korábbiak során már láttuk, hogy a kód távolsága legalább $d_1 d_2$, vagyis $d \ge d_1 d_2$. Ennél többet azonban most sem mondhatunk, ugyanis ha az üzenetet első lépésben a C_2 egy minimális súlyú kódszavába kódoltuk, akkor utána az egyes betűk C_1-beli kódja általában nem minimális súlyú, vagyis általában nincs C-ben $d_1 d_2$ súlyú kódszó. Végül a lineáris kódokból összeállított kaszkád kód kódsebessége $\mathcal{R} = \frac{k_1 k_2}{n_1 n_2} = \frac{k_1}{n_1}\frac{k_2}{n_2} = \mathcal{R}_1\mathcal{R}_2$, amint az könnyen belátható. Igazoltuk tehát a következőt.

11.9. Tétel

Az $\mathbb{F}_{q_1}$ fölötti $[n_1, k_1, d_1]_{q_1}$-paraméterű, $\mathcal{R}_1$ sebességű C_1 kódból mint belső kódból és az $\mathbb{F}_{q_1^{k_1}}$ fölötti $[n_2, k_2, d_2]_{q_1^{k_1}}$-paraméterű $\mathcal{R}_2$ sebességű C_2 kódból mint külső kódból konstruált kaszkád kód egy $\mathbb{F}_{q_1}$ fölötti $[n_1 n_2, k_1 k_2, d]_{q_1}$-paraméterű, $\mathcal{R} = \mathcal{R}_1\mathcal{R}_2$ sebességű C kód, ahol $d \ge d_1 d_2$.

Δ

A kaszkád kód általában nem ciklikus, hiszen ha egy kódszót egy pozícióval ciklikusan jobbra tolunk, akkor az egyes n_1-hosszúságú szakaszok mint C_1-beli kódszavak úgy változnak, hogy a jobb szélső betű kicsúszik, viszont a bal oldalon az előtte lévő kódszó utolsó betűje jelenik meg első betűként, és általában egy ilyen szó nem eleme a C_1 kódnak (ha például C_1 egy paritásbites bináris kód, akkor jobbról lehagyva egy bitet és balról kiegészítve egy másik kódszó utolsó bitjével, a kapott szóban az egyesek száma akár páros, akár páratlan is lehet).

Végezetül gondoljuk meg, hogy milyen kódot kapunk akkor, ha előbb a C_1 kóddal kódolunk, majd az így kapott n_1-hosszúságú kódszavakat $\mathbb{F}_{q_1^{n_1}}$ elemeinek tekintve, k_2 egymás utáni kódszóra alkalmazzuk a C_2 kódot, végül egy ilyen kódszó minden betűjét visszaírjuk $\mathbb{F}_{q_1}$-be. Az eredmény egy $\mathbb{F}_{q_1}$ fölötti $n_1 n_2$-hosszúságú kódszó lesz, ugyanúgy, mint az előbb, és a kód mérete, valamint a sebessége sem változik. Más a helyzet azonban a kód távolságával. Ha egy nullától különböző üzenetet kódolunk, akkor első lépésben legalább egy nem nulla kódszót kapunk. Az így kapott kódszavak az átírás után egy nem nulla üzenetet adnak a C_2 bemenetére, amelyet kódolva egy legalább d_2-súlyú kódszót kapunk. Ha azonban most ezt a kódszót visszaírjuk $\mathbb{F}_{q_1}$-be, akkor csak annyit állíthatunk biztosan, hogy a nem nulla elemek nem nulla $\mathbb{F}_{q_1}$ fölötti n_1-hosszúságú sorozatot adnak, azonban hogy egy-egy ilyen sorozatban hány nem nulla elem van, azt nem tudhatjuk (szélső esetben az ilyen elemek száma akár egy is lehet). Mindössze tehát annyit tudunk, hogy a konstruált kódban egy nem nulla kódszó legalább d_2 nem nulla elemet tartalmaz, azaz a kód súlya $d' \ge d_2$.

A kaszkád kód egy elterjedt használata, amikor a bináris üzenetet külső kódként egy 2^r-elemű test fölötti Reed-Solomon kóddal (vagy rövidített Reed-Solomon kóddal) kódolunk. Az ilyen kódot **binárisba fejtett Reed-Solomon kód**nak nevezik. Az elterjedt használatban $r = 8$, vagyis a külső kód betűi bájtok, míg a belső kód többnyire egy paritásbites kód, vagyis a Reed-Solomon kódból kapott bájtokat egy paritásbittel egészítjük ki.

12. Euklideszi algoritmus

Emlékeztetünk rá, hogy az $\mathcal{R}$ integritási tartomány akkor euklideszi gyűrű, ha létezik olyan $\varphi: R^* \to \mathbb{N}$ leképezés (az euklideszi norma), hogy tetszőleges $u \in R$ és $v \in R^*$ esetén $u = qv + r$, ahol $q \in R$, $r \in R$, és $r = 0$, vagy $r \neq 0$ és $\varphi(r) < \varphi(v)$. Ekkor a gyűrű egységelemes, bármely két elemének létezik asszociálttól eltekintve egyértelműen meghatározott legnagyobb közös osztója, és ez a legnagyobb közös osztó meghatározható az euklideszi algoritmussal. Az algoritmus a következő. Vezessük be az $r_{-1} = u$, $r_0 = v$ jelölést. Ekkor van olyan $n \in \mathbb{N}$, hogy minden $n \geq i \in \mathbb{N}$ indexre

$$r_{i-1} = q_i r_1 + r_{i+1}$$

úgy, hogy $r_i \neq 0$ és $r_{n+1} = 0$, továbbá ha $i < n$, akkor $\varphi(r_{i+1}) < \varphi(r_i)$. Ekkor $d = r_n$ az u és v legnagyobb közös osztója, és minden $-1 \leq i \leq n$ indexre van R-nek olyan a_i és b_i eleme, amellyel $r_i = a_i u + b_i v$. Ezeket az együtthatókat is meghatározhatjuk az euklideszi algoritmussal. $a_{-1} = e$ és $b_{-1} = 0$-ra nyilván igaz, hogy $r_{-1} = u = a_{-1}u + b_{-1}v$ és az $a_0 = 0$, $b_0 = e$ együtthatókkal a hasonló $r_0 = v = a_0 u + b_0 v$ egyenlőség. Ha most $r_{i-1} = a_{i-1}u + b_{i-1}v$ és $r_i = a_i u + b_i v$ az $n > i \in \mathbb{N}$ indexre, akkor $a_{i+1} = a_{i-1} - q_i a_i$, $b_{i+1} = b_{i-1} - q_i b_i$ jelöléssel

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i = (a_{i-1}u + b_{i-1}v) - q_i(a_i u + b_i v) \\ &= (a_{i-1} - q_i a_i)u + (b_{i-1} - q_i b_i)v = a_{i+1}u + b_{i+1}v, \end{aligned}$$

vagyis $i + 1$-re is teljesül az összefüggés.

Igazolható, hogy euklideszi gyűrűben mindig van olyan euklideszi norma, amelynél $uv \neq 0$ esetén $\varphi(uv) \geq \varphi(u)$. A továbbiakban feltételezzük, hogy az euklideszi norma teljesíti ezt a feltételt.

Legyen $u \neq 0$ és $\varphi(u) < \varphi(v)$. Ekkor

$$r_{-1} = u = 0 \cdot v + u = q_0 r_0 + r_1,$$

ahol $r_1 = u \neq 0$ és $\varphi(r_1) = \varphi(u) < \varphi(v) = \varphi(r_0)$, majd

$$v = r_0 = q_1 r_1 + r_2.$$

Ugyanide jutunk, ha $r_{-1} = v$ és $r_0 = u$, de eggyel kevesebb lépésből áll az algoritmus, elmarad az első, felesleges lépés. Emiatt a továbbiakban azt is feltesszük, hogy ha $u \neq 0$, akkor $\varphi(u) \geq \varphi(v)$.

Mint tudjuk, test fölötti polinomgyűrű euklideszi, ahol a nem nulla f polinomra $\varphi(f) = \deg(f)$ euklideszi norma, amely kielégíti a fenti megkötést.

Az alábbiakban az euklideszi algoritmus néhány további tulajdonságát vizsgáljuk.

12.1. Tétel

Legyen $\mathcal{R}$ euklideszi gyűrű az e egységelemmel és φ normával, amelynél $\varphi(ab) \geq \varphi(a)$, valahányszor $ab \neq 0$, és legyen $u \in R$ és $v \in R^*$ úgy, hogy $u = 0$, vagy $u \neq 0$ és $\varphi(u) \geq \varphi(v)$. Ekkor

1. ha $u|v$, akkor $v|u$;

ha az euklideszi algoritmusban $(u, v) = d = r_n$, akkor

2. $n = 0$ akkor és csak akkor, ha $v|u$;
3. ha $u = 0$, akkor $q_0 = 0$, egyébként $n \geq i \in \mathbb{N}$ esetén $q_i \neq 0$;

4. $n \geq i \in \mathbb{N}^+$ esetén $a_i \neq 0$, $b_i \neq 0$;
5. ha $n \geq i \in \mathbb{N}$, akkor $a_{i-1}b_i - a_i b_{i-1} = (-1)^i e$;
6. ha $-1 \leq i \leq n$, akkor $(a_i, b_i) = e$, míg $n \geq i \in \mathbb{N}$-re $(a_{i-1}, a_i) = e$ és $(b_{i-1}, b_i) = e$;
7. $n \geq i \in \mathbb{N}$-re $r_i a_{i-1} - r_{i-1}a_i = (-1)^i v$ és $r_{i-1}b_i - r_i b_{i-1} = (-1)^i u$.

Ha $\mathcal{R}$ egy $\mathcal{K}$ test feletti polinomgyűrű az $f \neq 0$ polinomokra a $\varphi(f) = \deg(f)$ normával, akkor az f és g nem nulla polinomokra

8. $n \geq i \in \mathbb{N}$ esetén $\deg(q_i) = \deg(r_{i-1}) - \deg(r_i)$, és ha $i > 0$, akkor $\deg(q_i) > 0$;
9. $-1 \leq i \leq n$-re $\deg(q_i) = \deg(f) - \sum_{j=0}^{i} \deg(q_j)$;
10.
   a) $\deg(b_0) \leq \deg(b_1)$, és $n > i \in \mathbb{N}^+$-re $\deg(a_i) < \deg(a_{i+1})$, $\deg(b_i) < \deg(b_{i+1})$;
   b) az $n \geq i \in \mathbb{N}$ indexekre $\deg(b_i) = \deg(f) - \deg(r_{i-1}) < \deg(f)$, és ha az index pozitív, akkor $\deg(a_i) = \deg(g) - \deg(r_{i-1}) < \deg(g)$.

Δ

Bizonyítás:

Az euklideszi algoritmus szerint $n \geq i \in \mathbb{N}$-re $r_{i-1} = q_i r_i + r_{i+1}$. Innen $q_i r_i = r_{i-1} - r_{i+1}$, másrészt $r_{i+1} = r_{i-1} - q_i r_i$. Ezt a két összefüggést többször alkalmazzuk.

1. Ha $u|v$, akkor $u \neq 0$ (mert $v \neq 0$) és $v = q'u$, így

$$u = qv + r = qq'u + r,$$

ahol $r = 0$, vagy $r \neq 0$ és $\varphi(r) < \varphi(u)$. A fenti egyenlőségből $r = (e - qq')u = q''u$, és ha $r \neq 0$, akkor ebből következik, hogy $\varphi(u) \leq \varphi(r) < \varphi(u)$, ami nyilvánvalóan lehetetlen, így $r = 0$, és akkor $u = qv$, tehát $v|u$.

2. Tegyük fel, hogy $v|u$. Ekkor

$$r_{-1} = u = qv = qv + 0 = q_0 r_0 + r_1,$$

vagyis ekkor $n = 0$ és $d = r_0 = v$. Fordítva, ha $n = 0$, akkor

$$u = r_{-1} = q_0 r_0 + r_1 = q_0 r_0 + 0 = q_0 r_0 = qv,$$

ami azt jelenti, hogy $v|u$.

3. Ha $u = 0$, akkor $u = 0 \cdot v + 0$, tehát $q_0 = 0$, és mivel ekkor $v|u$, ezért $n = 0$. Most tegyük fel, hogy $u \neq 0$. Ekkor $q_i = 0$ esetén $r_{i-1} = r_{i+1}$, ami lehetetlen, mert $r_{i-1} \neq 0$, és vagy $r_{i+1} = 0$, vagy ha nem, akkor $\varphi(r_{i-1}) \geq \varphi(r_i) > \varphi(r_{i+1})$.

4. Ha $n > i \in \mathbb{N}^+$-ra $a_i = 0$, akkor $0 \neq r_i = b_i v$, és így $\varphi(v) = \varphi(r_0) > \varphi(r_i) \geq \varphi(v)$, míg $b_i = 0$-val $0 \neq r_i = a_i u$, így $u \neq 0$, és ekkor $\varphi(u) \geq \varphi(v) = \varphi(r_0) > \varphi(r_i) \geq \varphi(u)$, ami mindkét esetben lehetetlen.

5. $a_{-1}b_0 - a_0 b_{-1} = e \cdot e - 0 \cdot 0 = e$, és ha $n > i \in \mathbb{N}$ -re $a_{i-1}b_i - a_i b_{i-1} = (-1)^{i+1} e$, akkor

$$\begin{aligned} a_i b_{i+1} - a_{i+1} b_i &= a_i(b_{i-1} - q_i b_i) - (a_{i-1} - q_i a_i) b_i \\ &= -(a_{i-1}b_i - a_i b_{i-1}) = -(-1)^{i+1} e = (-1)^{(i+1)+1} e. \end{aligned}$$

6. 5. szerint $a_{i-1}b_i - a_i b_{i-1} = \pm e$, és ez csak a tétel legnagyobb közös osztóival lehetséges, hiszen a felsorolt legnagyobb közös osztók mindegyike szükségszerűen osztója a jobb oldalnak, e-nek.

7. Ha $i = -1$ vagy $i = 0$, akkor

$$\begin{aligned} r_0 a_{-1} - r_{-1} a_0 &= v \cdot e - u \cdot 0 = v = (-1)^0 v \\ r_1 a_0 - r_0 a_1 &= r_1 \cdot 0 - v \cdot e = -v = (-1)^1 v, \end{aligned}$$

valamint

$$r_{-1}b_0 - r_0b_{-1} = u \cdot e - v \cdot 0 = u = (-1)^0u$$
$$r_0b_1 - r_1b_0 = r_0(-q_0) - r_1e = -(q_0r_0 + r_1) = -r_{-1} = -u = (-1)^1u,$$

ami mutatja, hogy a fentebb megadott két indexre érvényesek az egyenlőségek. Most tegyük fel, hogy $0 \leq j \leq i < n$ esetén $r_ja_{j-1} - r_{j-1}a_j = (-1)^jv$ és $r_{j-1}b_j - r_jb_{j-1} = (-1)^ju$. Ekkor

$$\begin{aligned} r_{i+1}a_i - r_ia_{i+1} &= r_{i+1}a_i - r_i(a_{i-1} - q_ia_i) = (r_{i+1} + q_ir_i)a_i - r_ia_{i-1} \\ &= -(r_ia_{i-1} - r_{i-1}a_i) = -(-1)^iv = (-1)^{i+1}v, \end{aligned}$$

$$\begin{aligned} r_ib_{i+1} - r_{i+1}b_i &= r_i(b_{i-1} - q_ib_i) - r_{i+1}b_i = -(r_{i+1} + q_ir_i)b_i + r_ib_{i-1} \\ &= -(r_{i-1}b_i - r_ib_{i+1}) = -(-1)^iu = (-1)^{i+1}u, \end{aligned}$$

tehát valamennyi tekintetbe vett indexre érvényes az állított egyenlőség.

A polinomokra vonatkozó állítások bizonyításánál felhasználjuk, hogy test fölötti nem nulla polinomok szorzatának foka a tényezők fokainak összege, és különböző fokú polinomok összegének és különbségének foka a tagok fokszámainak maximuma.

8. $n \geq i \in \mathbb{N}$-re $q_i \neq 0$ és $r_{i-1} \neq 0 \neq r_i$, ezért $q_ir_i = r_{i-1} - r_{i+1} \neq 0$, $\deg(r_{i-1}) \geq \deg(r_i)$, $r_{i+1} = 0$ (az $i = n$ esetben) vagy $r_{i+1} \neq 0$ és $\deg(r_i) > \deg(r_{i+1})$, így

$$\deg(q_i) = \deg(r_{i-1} - r_{i+1}) - \deg(r_i) = \deg(r_{i-1}) - \deg(r_i),$$

és ez nagyobb nullánál, ha $i > 0$.

9. $\deg(f) - \sum_{j=0}^{-1} \deg(q_j) = \deg(f) = \deg(r_{-1})$. Ha $n \geq i \in \mathbb{N}$, akkor $\deg(q_j)$-t az előző pontból helyettesítve

$$\sum_{j=0}^{i} \deg(q_j) = \sum_{j=0}^{i} \Big(\deg(r_{j-1}) - \deg(r_j)\Big) = \deg(r_{-1}) - \deg(r_i) = \deg(f) - \deg(r_i),$$

és ebből átrendezéssel kapjuk r_i fokát.

10.Azt tudjuk, hogy az a_i és b_i együtthatók és a q_i hányadosok egyike sem 0, és a pozitív indexekre $\deg(q_i) > 0$. Legyen n pozitív egész.

a) $b_{-1} = 0 = a_0$, $b_0 = e = a_1$, így $\deg(b_0) = 0 = \deg(a_1)$, és $b_1 = b_{-1} - q_0b_0 = -q_0$, tehát $\deg(b_1) = \deg(q_0) \geq 0 = \deg(b_0)$. Legyen $n > 1$. $\deg(a_2) = \deg(q_1) > 0 = \deg(a_1)$, hiszen $a_2 = a_0 - q_1a_1 = -q_1$, és ha $\deg(b_i) \geq \deg(b_{i-1})$ és $\deg(a_i) > \deg(a_{i-1})$, akkor a rekurziós összefüggésből és $\deg(q_i) > 0$-ból $\deg(b_{i+1}) > \deg(b_i)$ és $\deg(a_{i+1}) > \deg(a_i)$.

b) Az előbbi pontot felhasználva

$$\deg(b_0) = 0 = \deg(f) - \deg(f) = \deg(f) - \deg(r_{-1}) = \deg(f) - \deg(r_{0-1})$$

és

$$\deg(a_1) = 0 = \deg(g) - \deg(g) = \deg(g) - \deg(r_0) = \deg(g) - \deg(r_{1-1}).$$

A továbbiakban tegyük fel, hogy $i < n$ esetén egy nemnegatív i-re $\deg(b_i) = \deg(f) - \deg(r_{i-1})$ és $\deg(a_i) = \deg(g) - \deg(r_{i-1})$, ha az i pozitív. Ekkor

$$\begin{aligned} \deg(b_{i+1}) &= \deg(q_i) + \deg(b_i) = \deg(r_{i-1}) - \deg(r_i) + \deg(f) - \deg(r_{i-1}) \\ &= \deg(f) - \deg(r_i) = \deg(f) - \deg\big(r_{(i+1)-1}\big) \end{aligned}$$

valamint

$$\deg(a_{i+1}) = \deg(q_i) + \deg(a_i) = \deg(r_{i-1}) - \deg(r_i) + \deg(g) - \deg(r_{i-1})$$
$$= \deg(g) - \deg(r_i) = \deg(g) - \deg\left(r_{(i+1)-1}\right),$$

mert ha $i < n$, akkor $\deg(r_i) > \deg(r_{i+1}) \geq 0$. Még azt kell belátnunk, hogy $\deg(b_i) < \deg(f)$ valamint $\deg(a_i) < \deg(g)$. Ellenkező esetben $\deg(r_{i-1}) = 0$. Ekkor $\deg(r_i) = 0$ is igaz, mert a maradékok fokszáma nem növekedhet, és a fokszámok egyenlősége is csak akkor lehetséges, ha $i = 0$, ami most nem igaz, hiszen i pozitív egész.

□

A továbbiakban elsősorban az $n > i \in \mathbb{N}$ indexekkel talált

$$\deg(d) = \deg(r_n) < \deg(r_i) < \deg(g) \leq \deg(f)$$

$$\deg(b_i) = \deg(f) - \deg(r_{i-1})$$

egyenlőtlenségekre, valamint arra lesz szükségünk, hogy az a_i és b_i polinomok relatív prímek valamennyi, a $-1 \leq i \leq n$ feltételnek megfelelő indexre.

13. Alternáns kódok

Először megismétlünk néhány dolgot a ciklikus kódoknál tanultakból.

Legyen C egy $[n,k,d]_q$ ciklikus kód az $\mathbb{F}_q$ test fölött, ahol k pozitív egész, és g a kód generátorpolinomja. Ekkor $0 \neq g \in \mathbb{F}_q[x]$, $\deg(g) = n-k$, g osztója az $x^n - e$ polinomnak, ahol e az $\mathbb{F}_q$ egységeleme, továbbá az $\mathbb{F}_q$ fölötti legfeljebb $n-1$-edfokú c polinom akkor és csak akkor kódszópolinom a C kóddal, ha g osztója c-nek. Ha g gyökei egyszeresek, és biztosan ez a helyzet, ha n és q relatív prímek, akkor az előbbi feltétel pontosan akkor teljesül, ha g minden gyöke gyöke c-nek. Legyen g $\mathbb{F}_q$ fölötti irreducibilis felbontása $g = \prod_{i=1}^{s} m^{(i)}$. Ha $\alpha^{(i)}$ gyöke $m^{(i)}$-nek, és $\deg\left(m^{(i)}\right) = n_i$, akkor ${\alpha^{(i)}}^{q^j}$ is gyöke $m^{(i)}$-nek, ahol $0 \leq j < n_i$, ezek a gyökök páronként különbözőek, és nincs más gyöke $m^{(i)}$-nek. De $\alpha^{(i)}$ akkor és csak akkor gyöke c-nek, ha a $[0..n_i - 1]$ intervallumba eső legalább egy j kitevőre ${\alpha^{(i)}}^{q^j}$ gyöke c-nek, így az előbbi feltétel úgy is igaz, hogy c akkor és csak akkor kódpolinom a C kóddal, ha minden $m^{(i)}$ legalább egy-egy gyöke gyöke c-nek. Legyen $A^{(i)} = \left\{ {\alpha^{(i)}}^{q^j} \middle| n_i > j \in \mathbb{N} \right\}$, és $\{\alpha_l | n-k \geq t > l \in \mathbb{N}\} = B \subseteq A = \bigcup_{i=1}^{s} A^{(i)}$ g gyökeinek olyan halmaza, amely valamennyi $m^{(i)}$ legalább egy gyökét tartalmazza, vagyis $|B| = t \leq n-k$ és $\forall (s \geq i \in \mathbb{N})$: $B \cap A^{(i)} \neq \emptyset$, továbbá $\mathbf{H}$ egy olyan $t \times n$-méretű mátrix, amelyben a $0 \leq i < t$ és $0 \leq j < n$ indexekre $H_{i,j} = \alpha_i^j$, ahol $\alpha_i \in B$. Mivel c pontosan akkor kódszó, ha $0 = \hat{c}(\alpha_i) = \sum_{j=0}^{n-1} c_j \alpha_i^j = \sum_{j=0}^{n-1} H_{i,j} c_j = (\mathbf{Hc})_i$ minden $t > i \in \mathbb{N}$ indexre, ezért c akkor és csak akkor kódszó, ha $\mathbf{Hc} = \mathbf{0}$.

Mivel g osztója $x^n - e$-nek, ezért g valamennyi gyöke az $x^n - e$-nek is gyöke. Az utóbbi polinom gyökei $\mathbb{F}_q$ fölötti n-edik egységgyökök, és ha $(n,q) = 1$, akkor ezek a gyökök egy $\mathbb{F}_q$ fölötti α primitív n-edik egységgyök n-nél kisebb nemnegatív egész kitevős hatványai. Tegyük fel, hogy n és q relatív prímek. Legyen az A halmaz valamely B_1 részhalmaza olyan, hogy a B_1-ben lévő gyökök az α egymás után következő hatványai, vagyis $B_1 = \{\alpha^{\tau+l} | \delta - 1 > l \in \mathbb{N}\}$, ahol $\tau \in \mathbb{Z}$ tetszőleges egész, és $n - k + 1 \geq \delta \in \mathbb{N}$ (nem kötjük ki, hogy B_1 a g minden faktorának tartalmazza legalább egy gyökét), és legyen $\mathbf{H}$ olyan mátrix, amelyben az i-edik sor j-edik eleme $\left(\alpha^{\tau+i}\right)^j$, ahol $\delta - 1 > i \in \mathbb{N}$ és $n - 1 > j \in \mathbb{N}$. Ekkor $H_{i,j} = \left(\alpha^{\tau+i}\right)^j = \alpha^{\tau j}\left(\alpha^j\right)^i = h_j \beta_j^i$, ahol $h_j = \alpha^{\tau j}$ és $\beta_j = \alpha^j$. Ha most $\mathbf{H}'$ a $\mathbf{H}$ tetszőlegesen kiválasztott, páronként különböző $\delta - 1$ oszlopából álló részmátrix, akkor $\mathbf{H}'$ egy $\delta - 1$ -edrendű kvadratikus mátrix. Legyen D a $\mathbf{H}'$ determinánsa. A determináns j_l-indexű oszlopából, ahol $\delta - 1 > l \in \mathbb{N}$ és $n > j_l \in \mathbb{N}$, kiemelhető a 0-tól különböző h_{j_l}, és ha minden oszlopból kiemeltük ezt a szorzót, és a kiemelés utáni determinánst D'-vel jelöljük, akkor $D = D' \prod_{l=0}^{\delta-2} h_{j_l}$. Mivel a D' mögött álló szorzat nem nulla, ezért D pontosan akkor nulla, ha D' nulla. De D' egy olyan Vandermonde-determináns, amelyben a generátorelemek páronként különbözőek, hiszen $D'_{1,l} = \alpha^{j_l}$, az α primitív n-edik egységgyök és a j_l indexek csupa különböző, n-nél kisebb nemnegatív egészek. Ebből következik, hogy $\mathbf{H}'\mathbf{c} = \mathbf{0}$ csak úgy lehet, ha $\mathbf{c}$ a nullvektor, vagy $w(\mathbf{c}) \geq \delta$, és így a kód súlya legalább δ.

A BCH-kódot az előbbieknek megfelelően konstruáljuk. Legyen n a q prímhatványhoz relatív prím pozitív egész, τ tetszőleges egész, és δ 1-nél nagyobb egész, továbbá α egy $\mathbb{F}_q$ fölötti primitív n-edik egységgyök, végül g az $\alpha^{\tau+i}$-k $\mathbb{F}_q$ fölötti minimálpolinomjainak legkisebb közös többszöröse, ahol $\delta - 1 > i \in \mathbb{N}$. Ekkor a g által generált ciklikus kód dimenziója $k = n - \deg(g)$, és távolsága legalább δ, feltéve, hogy $k > 0$ (ellenkező esetben a kód csupán a nullvektort tartalmazza, így a kód távolsága nincs értelmezve). A konstrukcióból látszik, hogy ha τ-t tetszőleges, vele $\mathrm{modulo}\ n$ kongruens egésszel helyettesítjük, akkor ugyanazt a kódot kapjuk, továbbá ha δ nem kisebb n-nél, akkor g δ -tól függetlenül $x^n - e$, így kiköthetjük, hogy $n > \tau \in \mathbb{N}$ és $n \geq \delta \in \mathbb{N}$.

A BCH-kódnak $\delta - 1 > i \in \mathbb{N}$-re $\alpha^{\tau+i}$ gyöke, és a kód valamennyi gyöke az előbbi gyökök minimálpolinomjainak gyöke, tehát az $\mathbb{F}_q$ fölötti legfeljebb $n-1$-edfokú c polinom akkor és csak akkor eleme ennek a BCH-kódnak, ha az előbbi $\alpha^{\tau+i}$-k mindegyike gyöke c-nek, vagyis ha $\mathbf{Hc} = \mathbf{0}$, ahol $\mathbf{H}$ $(\delta - 1) \times n$-méretű, és $H_{i,j} = \left(\alpha^{\tau+i}\right)^j$ $(\delta - 1 > i \in \mathbb{N}$ és $n > j \in \mathbb{N})$. Hogy ennek a kódnak a távolsága

legalább δ, az azon múlott, hogy a **H** bármely $\delta - 1$-rendű kvadratikus részmátrixa, az oszlopokból egy-egy alkalmas nem nulla értéket kiemelve, reguláris Vandermonde-determinánst határoz meg. Ebből viszont következik, hogy ha **H** tetszőleges olyan, $r \times n$-méretű mátrix, amelynek bármely r-edrendű kvadratikus részmátrixához tartozó determinánsa az oszlopokból való alkalmas, nullától különböző elem kiemelése után reguláris Vandermonde-determináns, akkor mindazok az $\mathbb{F}_q$ fölötti n-dimenziós vektorok, amelyeknek **H**-val vett szorzata $\mathbf{0}$, egy olyan kódot adnak, amelynek a távolsága legalább $r + 1$.

13.1. Definíció

Legyen m, r és az r-nél nagyobb n pozitív egész, $n > j \in \mathbb{N}$-re h_j az $\mathbb{F}_{q^m}$ nem nulla elemei, ugyanezen indexekre az α_j-k az $\mathbb{F}_{q^m}$ páronként különböző elemei, és $C = \{\mathbf{c} \in \mathbb{F}_q^n | \mathbf{Hc} = \mathbf{0}\}$, ahol **H** az $\mathbb{F}_{q^m}$ fölötti olyan $r \times n$-méretű mátrix, amelyben $H_{i,j} = h_j \alpha_j^i$ $(r > i \in \mathbb{N}, n > j \in \mathbb{N})$. Ekkor C egy $\mathbb{F}_q$ fölötti **alternáns kód**. Ezt az alternáns kódot $A(q, m, r, \mathbf{h}, \boldsymbol{\alpha})$, vagy ha q, m és r ismert, akkor $A(\mathbf{h}, \boldsymbol{\alpha})$ jelöli.

Δ

Egy BCH-kód nyilván alternáns: ha a kód hossza n, és a kezdő értéket megadó paraméter τ, akkor $h_j = \alpha^{\tau j}$ és $\alpha_j = \alpha^j$.

Az rögtön látszik, hogy az alternáns kód lineáris, és a kódszavak hossza n, továbbá a kód konstrukciója következtében a kód d távolsága legalább $r + 1$. Korábban azt is láttuk, hogy a fenti **H** mátrix, amennyiben $m > 1$, általában nem ellenőrző mátrixa a kódnak, hiszen **H** nem minden eleme van benne feltétlenül $\mathbb{F}_q$-ban. Ha megadjuk $\mathbb{F}_{q^m}$-nek egy $\mathbb{F}_q$ fölötti bázisát, akkor $\mathbb{F}_{q^m}$ minden eleme bijektíven megfeleltethető egy $\mathbb{F}_q$ fölötti m-dimenziós vektornak, ahol a vektor komponensei az $\mathbb{F}_{q^m}$ adott elemének az előbbi bázisban való felírásánál kapott együtthatói. Ha a **H** minden elemét helyettesítjük a neki megfelelő vektor oszlopmátrixával, akkor már egy **H** fölötti $mr \times n$-méretű mátrixunk lesz. Ennek a mátrixnak azonban lehetnek lineárisan összefüggő sorai. Kiválasztva maximális számú lineárisan független sort, az így kapott mátrix lesz a kód ellenőrző mátrixa. A lineárisan független sorok száma legalább r, hiszen az eredeti mátrix sorai lineárisan függetlenek, és így van benne r lineárisan független oszlop, de akkor az új mátrixnak is legalább r oszlopa lineárisan független, és maximum rm, így a kód k dimenziójára azt kapjuk, hogy $n - mr \leq k \leq n - r$, és C egy $\mathbb{F}_q$ fölötti, $[n, k, d]_q$-paraméterű kód. Meg kell jegyezni, hogy ez a kód általában nem ciklikus (ugyanakkor minden BCH-kód alternáns, vagyis léteznek ciklikus alternáns kódok).

Most egy másik kódot definiálunk, amelyről kiderül, hogy szintén alternáns. A definíció előtt szükségünk lesz egy egyszerű tényre. Ha g egy $\mathcal{K}$ test fölötti r-edfokú polinom, ahol r nagyobb nullánál, és $u \in K$ olyan, hogy $\hat{g}(u) \neq 0$, vagyis u nem gyöke g-nek, akkor g és $x - u$ relatív prímek. Test fölötti polinomgyűrű euklideszi, így létezik, és asszociálttól eltekintve egyértelmű a legnagyobb közös osztó. $x - u$ mint elsőfokú polinom, irreducibilis a $\mathcal{K}[x]$ gyűrűben, így az előbbi legnagyobb közös osztó, asszociálttól eltekintve, csupán e vagy $x - u$ lehet, ahol e a test egységeleme. De ha a legnagyobb közös osztó $x - u$, akkor $x - u$ osztója g-nek, ami ekvivalens azzal, hogy u gyöke g-nek. Mivel $\hat{g}(u) \neq 0$, ezért a legnagyobb közös osztó csak e lehet. Euklideszi gyűrűben a legnagyobb közös osztó felírható a megadott elemek olyan lineáris kombinációjaként, ahol az együtthatók a gyűrűből vannak, így létezik olyan $g^{(u)}$ és $t^{(u)}$ $\mathcal{K}$ fölötti polinom, hogy $e = g^{(u)} \cdot (x - u) + t^{(u)} g$. $g^{(u)}$ nem nulla, mert $r > 0$, és mindig megválasztható úgy, hogy a foka kisebb legyen, mint g foka. Ha ugyanis f_1 és f_2 nem konstans polinomok, amelyek relatív prímek, és $e = h_1 f_1 + h_2 f_2$, akkor $f_2 \neq 0$, így $h_1 = q f_2 + r$, ahol $r = 0$, vagy $r \neq 0$ és $\deg(r) < \deg(f_2)$. Innen behelyettesítés és átrendezés után $e = r f_1 + (q f_1 + h_2) f_2 = t_1 f_1 + t_2 f_2$, és $t_1 = r \neq 0$ ismét azért, mert f_2 nem konstans.

Az $e = g^{(u)} \cdot (x - u) + t^{(u)} g$ felírásból látjuk, hogy $g | e - g^{(u)} \cdot (x - u)$, amit úgy is írhatunk, hogy $e \equiv g^{(u)} \cdot (x - u)$ (g), vagy hogy $g^{(u)} \equiv (x - u)^{-1}$ (g), és azt mondjuk, hogy $g^{(u)} \cdot (x - u)$ kongruens e-vel modulo g, illetve hogy $g^{(u)}$ modulo g inverze $x - u$-nak. Általánosan, ha egy test

fölötti polinomgyűrűben az f_1 és f_2 polinom különbsége osztható a g polinommal, akkor f_1 és f_2 kongruens modulo g, és azt írjuk, hogy $f_1 \equiv f_2\ (g)$, míg ha $h_1 h_2 \equiv e\ (g)$, ahol a bal oldali szorzat két tényezője ugyanezen polinomgyűrű két eleme, és e a test egységeleme, akkor h_2 a h_1 modulo g inverze, jelölésben $h_2 \equiv h_1^{-1}\ (g)$.

Ezek után lássuk a kódot.

13.2. Definíció

Legyen m és n pozitív egész, $0 \neq g \in \mathbb{F}_{q^m}[x],\ n > j \in \mathbb{N}$-re az α_j-k az $\mathbb{F}_{q^m}$ páronként különböző olyan elemei, amelyek nem gyökei g-nek, végül $C = \left\{\mathbf{c} \in \mathbb{F}_q^n \middle| \sum_{i=0}^{n-1} c_i (x-\alpha_i)^{-1} \equiv 0\ (g)\right\}$. Ekkor C egy $\mathbb{F}_q$ fölötti **Goppa-kód**, amelyet $\Gamma(q, m, g, \boldsymbol{\alpha})$, vagy röviden $\Gamma(g, \boldsymbol{\alpha})$ jelöl.

Δ

13.3. Tétel

$\mathbb{F}_q$ fölötti Goppa-kód $\mathbb{F}_q$ fölötti alternáns kód.

Δ

Bizonyítás:

A $g^{(j)} \equiv \left(x-\alpha_j\right)^{-1}\ (g)$ polinom könnyen megadható. Egységelemes kommutatív $\mathcal{R}$ gyűrű (tehát bármely test) fölötti g polinomra, és az előbbi gyűrű u elemére $g = (x-u)h + \hat{g}(u)$ egy alkalmas, $\mathcal{R}$ fölötti h polinommal, így $g - \hat{g}(u)$ osztható $x-u$-val, és $h = \frac{g-\hat{g}(u)}{x-u}$. Ha $\hat{g}(u)$ invertálható $\mathcal{R}$ -ben (és így u nem gyöke g-nek), akkor $g = (x-u)h + \hat{g}(u)$-ból $\left(\hat{g}(u)\right)^{-1}$-gyel való szorzással és átrendezéssel $e = \left(\hat{g}(u)\right)^{-1}(g - (x-u)h) = \left(-\left(\hat{g}(u)\right)^{-1}\frac{g-\hat{g}(u)}{x-u}\right)(x-u) + \left(\hat{g}(u)\right)^{-1} g$, és innen közvetlenül leolvasható, hogy $g^{(j)} = -\left(\hat{g}(\alpha_j)\right)^{-1}\frac{g-\hat{g}(\alpha_j)}{x-\alpha_j}$.

Legyen $g = \sum_{l=0}^{r} g_l x^l$, ahol $g_r \neq 0$, és így $g \neq 0$ és $\deg(g) = r$. $\sum_{i=0}^{n-1} c_i (x-\alpha_i)^{-1} \equiv 0\ (g)$ ekvivalens azzal, hogy $g \middle| \sum_{i=0}^{n-1} c_i g^{(i)}$. Ha $g \middle| \sum_{i=0}^{n-1} c_i g^{(i)}$, ahol a c_i-k $\mathbb{F}_q$ elemei, akkor $\sum_{i=0}^{n-1} c_i g^{(i)} = 0$, hiszen a $g^{(i)}$-k $r-1$-edfokúak, ezért az összegük is legfeljebb $r-1$-edfokú. De egy legfeljebb $r-1$-edfokú polinom csak úgy lehet osztható egy r-edfokú polinommal, ha 0, ahonnan kapjuk az előbbi egyenlőséget. Ebből következik, hogy $\mathbf{c} \in \mathbb{F}_q^n$ akkor és csak akkor eleme C-nek, ha $\sum_{i=0}^{n-1} c_i g^{(i)} = 0$. A rövidség kedvéért legyen $h_k = -\left(\hat{g}(\alpha_k)\right)^{-1}$, és nézzük a $\sum_{i=0}^{n-1} c_i g^{(i)} = 0$ feltételt.

$$
\begin{aligned}
0 &= \sum_{k=0}^{n-1} c_k g^{(k)} = \sum_{k=0}^{n-1} c_k \left(-\left(\hat{g}(\alpha_k)\right)^{-1}\frac{g-\hat{g}(\alpha_k)}{x-\alpha_k}\right) = \sum_{k=0}^{n-1} c_k \left(h_k \frac{g-\hat{g}(\alpha_k)}{x-\alpha_k}\right) \\
&= \sum_{k=0}^{n-1} c_k h_k \frac{\sum_{j=1}^{r} g_j\left(x^j - \alpha_k^j\right)}{x-\alpha_k} = \sum_{k=0}^{n-1} c_k h_k \sum_{j=1}^{r} g_j \frac{x^j - \alpha_k^j}{x-\alpha_k} = \sum_{k=0}^{n-1} c_k h_k \sum_{j=1}^{r} g_j \sum_{i=0}^{j-1} \alpha_k^{j-1-i} x^i \\
&= \sum_{i=0}^{r-1} x^i \sum_{k=0}^{n-1} \sum_{j=i+1}^{r} g_j h_k \alpha_k^{j-1-i} c_k = \sum_{i=0}^{r-1} x^i \sum_{k=0}^{n-1} \sum_{j=0}^{r-1-i} g_{i+1+j} h_k \alpha_k^j c_k \\
&= \sum_{i=0}^{r-1} x^i \sum_{k=0}^{n-1} \sum_{j=0}^{r-1} g_{i+1+j} h_k \alpha_k^j c_k = \sum_{i=0}^{r-1} x^{r-1-i} \sum_{k=0}^{n-1} \sum_{j=0}^{r-1} g_{r-i+j} h_k \alpha_k^j c_k,
\end{aligned}
$$

ahol $g_l = 0$, ha $r < l \in \mathbb{N}$. Vezessünk be néhány új jelölést. Az $r > i \in \mathbb{N}$, $r > j \in \mathbb{N}$ és $n > k \in \mathbb{N}$ indexekre legyen $x_i = x^{r-1-i}$, $G_{i,j} = g_{r-i+j}$ és $H_{j,k} = h_k \alpha_k^j$, továbbá $\mathbf{x}$, $\mathbf{G}$ és $\mathbf{H}$ a megfelelő vektor

illetve mátrix. Az x_i-k lineárisan függetlenek, hiszen az x^i polinomok a polinomgyűrű egy bázisát képezik, így az $\mathbf{x}$ komponenseinek csak a triviális lineáris kombinációja a nullvektor. Ha $j > i$, akkor $r - i + j > r$, ezért $\mathbf{G}$ alsó háromszögmátrix. $\mathbf{G}$ főátlójában $g_{r-i+i} = g_r$ áll, amely nem nulla, ennélfogva $\mathbf{G}$ determinánsa nem nulla, $\mathbf{G}$ reguláris, és ha $\mathbf{A}$ egy r sorból álló mátrix, akkor $\mathbf{GA} = \mathbf{0}$ akkor és csak akkor igaz, ha $\mathbf{A} = \mathbf{0}$. A bevezetett jelölésekkel a fenti összefüggést folytatva

$$0 = \sum_{i=0}^{r-1} x^{r-1-i} \sum_{k=0}^{n-1} \sum_{j=0}^{r-1} g_{r-i+j} h_k \alpha_k^j c_k$$
$$= \sum_{i=0}^{r-1} \left(x_i \left(\sum_{k=0}^{n-1} \left(\sum_{j=0}^{r-1} G_{i,j} H_{j,k} \right) c_k \right) \right) = \mathbf{x}^T \big(\mathbf{G}(\mathbf{Hc}) \big).$$

De $\mathbf{x}^T \big(\mathbf{G}(\mathbf{Hc}) \big) = 0$ akkor és csak akkor, ha $\mathbf{G}(\mathbf{Hc}) = \mathbf{0}$, ez pedig pontosan akkor teljesül, ha $\mathbf{Hc} = \mathbf{0}$. Viszont $\mathbf{H}$ olyan $r \times n$-es mátrix, amelyben $H_{i,j} = h_j \alpha_j^i$, $h_j = -\left(\hat{g}(\alpha_j) \right)^{-1} \neq 0$, és az α_j-k páronként különbözőek, így a Goppa-kód valóban alternáns kód.

□

Az előbbiekből következik, hogy a fenti Goppa-kód távolsága legalább $r + 1$, a kód lineáris, és $n - mr \leq k \leq n - r$, ahol k a kód dimenziója.

Egy BCH-kódot **szűkebb értelemben vett** BCH-**kód**nak nevezünk, ha $\tau = 1$. Szűkebb értelemben vett BCH-kód Goppa-kód. Most ugyanis $H_{i,j} = \alpha^j \left(\alpha^j \right)^i$, ahol $\delta - 1 > i \in \mathbb{N}$, és δ a kód tervezett távolsága. $\mathbf{H}$ sorait fordított sorrendben írva $H_{i,j} = \alpha^j \left(\alpha^j \right)^{\delta-2-i} = -\left(-\left(\alpha^{-j} \right)^{\delta-1} \right)^{-1} \left(\alpha^{-j} \right)^i$, így ha $g = -x^{\delta-1}$ és $\alpha_i = \alpha^{-i}$, akkor $\hat{g}(\alpha_i) \neq 0$, hiszen g-nek a 0 és csak a 0 a gyöke, és egységgyök nem nulla, és $H_{i,j} = -\left(\hat{g}(\alpha_j) \right)^{-1} \alpha_j^i$. Ugyanakkor egy BCH-kód általában nem Goppa-kód.

Ezek után vizsgáljuk meg a **bináris**, vagyis az $\mathbb{F}_2$ fölötti **Goppa-kód**okat. Egy ilyen kódhoz tartozó kódszóban minden elem 0 vagy 1. Az alábbiakban kihasználjuk, hogy egy $\mathbb{F}_{2^r}$ fölötti polinom deriváltja teljes négyzet. Legyen ugyanis $h = \sum_{i=0}^{t} h_i x^i \in \mathbb{F}_{2^r}[x]$, ekkor

$$h' = \sum_{i=1}^{t} i h_i x^{i-1} = \sum_{i=0}^{t-1} (i+1) h_{i+1} x^i = \sum_{i=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} h_{2i+1} x^{2i}$$
$$= \sum_{i=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} f_i^2 x^{2i} = \left(\sum_{i=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} f_i x^i \right)^2 = f^2,$$

ahol $f = \sum_{i=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} h_{2i+1}^{\frac{1}{2}} x^i$. Az átalakításnál kihasználtuk, hogy ha i páratlan, akkor $i + 1$ páros, így páratlan indexre $\mathbb{F}_{2^r}$-ben $(i+1)h_{i+1} = 0$, azt, hogy p-karakterisztikájú testben bármely pozitív egész l-re minden elemnek van egyértelműen meghatározott p^l-edik gyöke, tehát h_{i+1}-nek is van egy és csak egy f_i négyzetgyöke $\mathbb{F}_{2^r}$-ben, végül hogy p-karakterisztikájú testben egy összeg p^k-kitevős hatványa, ahol k nemnegatív egész, a tagok p^k-adik hatványainak összege, ezért $\mathbb{F}_{2^r}$ fölötti összeg négyzete a tagok négyzeteinek összege.

A másik tulajdonság, amit felhasználunk, a következő. Legyen $t \in \mathbb{N}$, az u_i-k, ahol $t \geq i \in \mathbb{N}^+$, egy $\mathcal{K}$ test elemei, és $h = \prod_{i=1}^{t} (x - u_i)$, ekkor

$$h' = \sum_{i=1}^{t} \prod_{\substack{j=1 \\ j\neq i}}^{t} (x-u_j) = \sum_{i=1}^{t} \frac{\prod_{j=1}^{t}(x-u_j)}{x-u_i} = \sum_{i=1}^{t} \frac{h}{x-u_i}.$$

Tegyük fel, hogy az u_i-k egyike sem gyöke a $\mathcal{K}$ fölötti g polinomnak. Ekkor mindegyik i indexre létezik a $g^{(i)} \equiv (x-u_i)^{-1}\ (g)$ polinom, és $h' = \sum_{i=1}^{t} \frac{h}{x-u_i} \equiv \sum_{i=1}^{t} hg^{(i)} = h\sum_{i=1}^{t} g^{(i)}\ (g)$. Mivel h-nak az u_i-k és csak az u_i-k a gyökei, amelyek egyike sem gyöke g-nek, ezért g és h relatív prímek, így g akkor és csak akkor osztója a $\sum_{i=1}^{t} g^{(i)}$ polinomnak, ha osztója h'-nek. De $h' = f^2$. Legyen g irreducibilis felbontása a $\mathcal{K}$ valamely bővítése fölött $g = \prod_{i=1}^{s} m^{(i)^{k_i}}$, ahol az $m^{(i)}$ polinomok páronként különbözőek (a bővítés lehet triviális is, azaz maga $\mathcal{K}$, vagy lehet a $\mathcal{K}$ felbontási teste, de a $\mathcal{K}$ bármely más bővítése is). Ha valamely i-re $k_i = 2l-1$, akkor $m^{(i)^{2l-1}} \Big| f^2 = f\cdot f$-ből, és abból, hogy $m^{(i)}$ irreducibilis, következik, hogy $m^{(i)^{l}} \Big| f$, és ekkor $m^{(i)^{2l}} \Big| f^2 = h'$. Mivel ez mindegyik i-re igaz, ezért g pontosan akkor osztója $\sum_{i=1}^{t} g^{(i)}$-nek, ha ez utóbbi polinom osztható $\tilde{g} = \prod_{i=1}^{s} m^{(i)^{\left\lceil \frac{k_i}{2} \right\rceil}}$ négyzetével. Könnyű látni, hogy amennyiben valamennyi i-re $k_i = 1$, vagyis ha g minden gyöke egyszeres (például ha g irreducibilis $\mathcal{K}$ fölött, és $\mathcal{K}$ véges, vagy 0-karakterisztikájú), akkor $\tilde{g} = g$.

Igaz tehát a következő tétel.

13.4. Tétel

Legyen C egy $\Gamma(g, \boldsymbol{\alpha})$ Goppa-kód, $g = \prod_{i=1}^{s} m^{(i)^{k_i}}$ a g irreducibilis felbontása az $\mathbb{F}_2$ valamely bővítése fölött, és $\tilde{g} = \prod_{i=1}^{s} m^{(i)^{\left\lceil \frac{k_i}{2} \right\rceil}}$. Ekkor $\Gamma(g, \boldsymbol{\alpha}) = \Gamma(\tilde{g}^2, \boldsymbol{\alpha})$.

Δ

Bizonyítás:
A tétel előtt belátott tényekkel már könnyű a bizonyítás. $\mathbf{c} \in \mathbb{F}_2^n$ akkor és csak akkor eleme C-nek, ha $g \Big| \sum_{i=0}^{n-1} c_i g^{(i)}$. Most c_i csak 0 és 1 lehet, így ha J azon indexek halmaza, amelyekre $c_i = 1$, és $h = \prod_{i\in J}(x-\alpha_i)$, akkor $\sum_{i=0}^{n-1} c_i g^{(i)} = \sum_{i\in J} g^{(i)}$, és g akkor és csak akkor osztója $\sum_{i\in J} g^{(i)}$-nek, ha $\tilde{g}^2$ osztója az összegnek.

□

$\tilde{r} = \deg(\tilde{g}^2) \geq \deg(g) = r$, és a tétel alapján C távolsága legalább $\tilde{r}+1$. Ha g gyökei egyszeresek, akkor $\tilde{r} = \deg(\tilde{g}^2) = \deg(g^2) = 2r$, vagyis ekkor $d = d(C) \geq 2r+1$.

A 69., majd a 76. oldalon definiáltuk a jó kódot, valamint az olyan kódot, amely aszimptotikusan kielégíti a Varshamov-Gilbert korlátot. Most igazoljuk a következő eredményt.

13.5. Tétel

Létezik Goppa-kódok olyan családja, amely aszimptotikusan eléri a Varshamov-Gilbert korlátot.

Δ

Bizonyítás:
A Varshamov-Gilbert korlát szerint $A_q(n,d) \geq \frac{q^n}{V_q(n,d-1)}$, ahol $V_q(n,t) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$, és a $\delta = \frac{d}{n}$ jelöléssel a megfelelő aszimptotikus korlát $a_q(\delta) = \overline{\lim_{n\to\infty}} \left(n^{-1} A_q(n, \delta n) \right) \geq 1 - H_q^*(\delta)$, ha teljesül a $\delta \leq 1 - q^{-1}$ feltétel. A jobb oldalon álló függvény $H_q^*(\delta) = \delta \log_q(q-1) + H_q(\delta)$, és ebben $H_q(\delta) = -\delta \log_q(\delta) - (1-\delta)\log_q(1-\delta)$ a Shannon-féle entrópia. Felhasználjuk még a bizonyítás

során, hogy tetszőleges pozitív egész r-re a q-elemű test fölötti r-edfokú irreducibilis főpolinomok száma $I_q(r) = \frac{1}{r}\sum_{d|r}\mu(d)q^{\frac{r}{d}}$, és ha $r > 1$, akkor

$$\sum_{d|r}\mu(d)q^{\frac{r}{d}} > q^r - \sum_{i=0}^{\left\lfloor\frac{r}{2}\right\rfloor} q^d = q^r - \frac{q^{\left\lfloor\frac{r}{2}\right\rfloor+1}-1}{q-1} > q^r\left(1-q^{-\frac{r}{2}+1}\right) \geq 0,$$

azaz $I_q(r) > \frac{1}{r}q^r\left(1-q^{-\frac{r}{2}+1}\right)$.

Ezek után megmutatjuk, hogy bármely véges test fölött meg tudunk adni a tételben megfogalmazott tulajdonságú kódcsaládot.

Legyen $m, r \geq 2$ és d pozitív egész szám, q egy prím pozitív egész kitevős hatványa, $n = q^m$, továbbá $\boldsymbol{\alpha} = \mathbb{F}_{q^m} = \{a_i | n > i \in \mathbb{N}\}$. Ha az r-edfokú $g \in \mathbb{F}_{q^m}[x]$ polinom irreducibilis $\mathbb{F}_{q^m}$ fölött, akkor teljesül az a feltétel, hogy $\boldsymbol{\alpha}$ egyetlen eleme sem gyöke g-nek, így kapunk egy $\Gamma(g, \boldsymbol{\alpha})$ Goppa-kódot $\mathbb{F}_q$ fölött. g-t úgy szeretnénk megválasztani, hogy a kód távolsága legalább d legyen. A generált C kód $\mathbb{F}_q^n$ azon $\mathbf{c}$ elemeinek összessége, amelyekre $g \left| \sum_{i=0}^{n-1}\frac{c_i}{x-a_i} = \sum_{c_i\neq 0}\frac{c_i}{x-a_i}\right.$. Ha $0 < w(\mathbf{c}) = t$, akkor az előbbi összeg a közös nevezővel $\sum_{c_i\neq 0}\frac{c_i}{x-a_i} = \frac{f}{h}$, ahol h a páronként különböző $x - a_i$ polinomok szorzata, tehát egy t-edfokú polinom, míg a számlálóban álló f polinom $t-1$-edfokú polinomok $\mathbb{F}_q$-beli együtthatós lineáris kombinációja. f és h relatív prímek, mivel h bármely gyöke az f-et alkotó összeg egy és csak egy tagjának nem gyöke, és így magának f-nek sem gyöke. $g \left|\frac{f}{h}\right.$-ból $hg|f$, azaz $g|f$, így $\mathbf{c}$ akkor és csak akkor eleme a kódnak, ha g osztója f-nek, vagyis $\mathbf{c}$ pontosan akkor nincs benne a kódban, ha g nem faktora f-nek. f-nek legfeljebb $\left\lfloor\frac{t-1}{r}\right\rfloor$ r-edfokú irreducibilis osztója van. A kód távolsága biztosan nem kisebb d-nél, ha teljesül, hogy valahányszor $1 \leq t < d$, mindannyiszor a t-súlyú $\mathbf{c}$ nem eleme $\Gamma(g, \boldsymbol{\alpha})$-nek. Lesz tehát d-távolságú kódunk, ha meg tudjuk g-t választani úgy, hogy minden ilyen esetben a megfelelő f polinomnak nem faktora. A pontosan t-súlyú szavak száma $\mathbb{F}_q^n$-ben $\binom{n}{t}(q-1)^t$, minden ilyen esetén maximum $\left\lfloor\frac{t-1}{r}\right\rfloor$ irreducibilis főpolinomot kell kizárnunk, tehát a nem alkalmas polinomok száma összesen $\sum_{t=1}^{d-1}\left\lfloor\frac{t-1}{r}\right\rfloor\binom{n}{t}(q-1)^t < \frac{d}{r}V_q(n, d-1)$. Az eddigi eredmények alapján tehát biztosan konstruálható a q-elemű test fölötti, n szóhosszúságú, legalább d távolságú kód, ha teljesül a $\frac{d}{r}V_q(n,d) < \frac{1}{r}q^{mr}\left(1-q^{-\frac{mr}{2}+1}\right)$, másként a $dV_q(n,d) < q^{mr}\left(1-q^{-\frac{mr}{2}+1}\right)$ egyenlőtlenség. Áttérve a logaritmusokra a feltétel $n^{-1}\left(\log_q(\delta n) + \log_q V_q(n, \delta n)\right) < \frac{mr}{n} + n^{-1}\left(\log_q\left(1-q^{-\frac{mr}{2}+1}\right)\right)$ alakú. Amennyiben $\delta \leq 1 - q^{-1}$, akkor $n \to +\infty$ esetén határértékben $H_q^*(\delta) \leq \lim_{n\to\infty}\frac{mr}{n}$-et, vagy kis átalakítással $1 - H_q^*(\delta) \geq 1 - \lim_{n\to\infty}\frac{mr}{n}$-et kapunk. r-edfokú polinommal generált Goppa-kódban $k \geq n - mr$ és $d \geq r + 1$, így a kód $\mathcal{R}_n$ sebessége legalább $1 - \frac{mr}{n}$. r-et meg tudjuk úgy választani, hogy határértékben teljesüljön az $1 - H_q^*(\delta) = 1 - \lim_{n\to\infty}\frac{mr}{n}$, vagyis az $a(\delta) = 1 - H_q^*(\delta)$ egyenlőség, ami az aszimptotikus Varshamov-Gilbert korlát, .

Mivel $m = \log_q n$, ezért tudunk ennélfogva ez a sorozat eléri az aszimptotikus Varshamov-Gilbert korlátot.

□

A Goppa-kódokat alkalmazzák a rejtjelezésben is, a McEliece-féle titkosító rendszer a Goppa kódra épül.

14. Alternáns kódok dekódolása

Alternáns kódok dekódolására több módszer létezik, mi az egyik leghatékonyabbat ismertetjük.

Legyen C egy $A(q, m, r, \mathbf{h}, \boldsymbol{\alpha})$-paraméterű alternáns kód, ekkor a kód d távolsága legalább $r+1$, és kössük ki, hogy $\boldsymbol{\alpha}$ egyetlen komponense sem 0. Legyen $t_0 = \left\lfloor \frac{r}{2} \right\rfloor$, ekkor C t_0 hibát biztosan javít. Legyen egy üzenet továbbításánál fellépő hibavektor $\boldsymbol{\varepsilon}$, és $1 \leq w(\boldsymbol{\varepsilon}) = t \leq t_0$, ahol $w(\boldsymbol{\varepsilon})$ a hibavektor súlya, vagyis a hibahelyek száma, és legyen a hibás pozíciók indexeinek halmaza $J = \{j_i \in \mathbb{N} | t > i \in \mathbb{N} \wedge n > j_i\}$. Jelölje $t > i \in \mathbb{N}$-re X_i α_{j_i}-t, és Y_i ε_{j_i}-t. Ha ismerjük az X_i-ket és Y_i-ket, akkor ismerjük a hibás pozíciókat, és a hibás helyeken a hiba értékét, így a javítás már elvégezhető. Kérdés, hogy hogyan tudjuk ezeket az értékeket meghatározni.

Legyen $\mathbf{H}$ az az $r \times n$-méretű mátrix, amelyben $0 \leq i < r$-re és $0 \leq j < n$-re $H_{i,j} = h_j \alpha_j^i$, $\mathbf{v}$ a vett szó az $\boldsymbol{\varepsilon}$ hibával, és $\mathbf{s} = \mathbf{H}\mathbf{v} = \mathbf{H}\boldsymbol{\varepsilon}$ a szindróma, ekkor ismét $0 \leq i < r$-re

$$s_i = (\mathbf{H}\boldsymbol{\varepsilon})_i = \sum_{j=0}^{n-1} H_{i,j}\varepsilon_j = \sum_{j \in J} H_{i,j}\varepsilon_j = \sum_{l=0}^{t-1} H_{i,j_l}\varepsilon_{j_l} = \sum_{l=0}^{t-1} h_{j_l} X_l^i Y_l.$$

A korábbi feltétel szerint a hibák t száma legalább 1 és legfeljebb t_0, így $\mathbf{s} \neq \mathbf{0}$. Definiálunk három polinomot. Legyen $\sigma = \prod_{i=0}^{t-1}(e - X_i x)$, ekkor látható, hogy $\hat{\sigma}(0) = e$, $\deg(\sigma) = t \leq \frac{r}{2}$, és $\hat{\sigma}(u) = 0$ akkor és csak akkor, ha $u = X_l^{-1}$ egy $t > l \in \mathbb{N}$ indexszel. A második polinomhoz legyen $t > i \in \mathbb{N}$-re $\sigma^{(i)} = \prod_{\substack{l=0 \\ l \neq i}}^{t-1}(e - X_l x)$, és $\omega = \sum_{i=0}^{t-1} h_{j_i} Y_i \sigma^{(i)}$. Az α_j-k, tehát az X_i-k is, páronként különbözőek, és egyikük sem nulla, így $\sigma^{(i)}$ gyökeinek halmaza $\left\{X_j^{-1} \middle| t > j \in \mathbb{N} \wedge j \neq i\right\}$, és

$$\hat{\omega}\left(X_i^{-1}\right) = \sum_{l=0}^{t-1} h_{j_l} Y_l \hat{\sigma}^{(l)}\left(X_i^{-1}\right) = h_{j_i} Y_i \hat{\sigma}^{(i)}\left(X_i^{-1}\right).$$

$\hat{\sigma}^{(i)}\left(X_i^{-1}\right) \neq 0$, továbbá a kód definíciója alapján $h_{j_i} \neq 0$, ezért $Y_i = \frac{\hat{\omega}\left(X_i^{-1}\right)}{h_{j_i}\hat{\sigma}^{(i)}\left(X_i^{-1}\right)}$. $Y_i \neq 0$ is igaz, tehát $\hat{\omega}\left(X_i^{-1}\right) \neq 0$, amiből következik, hogy σ és ω relatív prímek. Mivel feltettük, hogy van hiba, és így legalább egy indexre $Y_i \neq 0$, ezért ω nem lehet a nullpolinom. ω egy olyan összeg, amelynek minden tagja egy $t-1$-edfokú polinom, így $\deg(\omega) \leq t-1$. σ a **hibahelypolinom**, míg ω a **hibaérték-polinom**. Az elnevezések érthetőek: ha ismerjük σ-t, akkor a polinom gyökeinek inverzei megadják a hibahelyeket, míg ω ismeretében meghatározhatjuk a hiba értékét.

A harmadik polinom, $S = \sum_{i=0}^{r-1} s_i x^i$, a legfeljebb $r-1$-edfokú szindrómapolinom.

Most belátjuk az egész eljárás lényegét jelentő $\omega \equiv \sigma S\ (x^r)$ kongruenciát.

$$\begin{aligned}
\omega - \sigma S &= \sum_{l=0}^{t-1} h_{j_l} Y_l \sigma^{(l)} - \sum_{i=0}^{r-1} \sigma s_i x^i = \sum_{l=0}^{t-1} h_{j_l} Y_l \sigma^{(l)} - \sum_{i=0}^{r-1} \sigma \sum_{l=0}^{t-1} h_{j_l} Y_l X_l^i x^i \\
&= \sum_{l=0}^{t-1} h_{j_l} Y_l \sigma^{(l)} - \sum_{l=0}^{t-1} \sigma h_{j_l} Y_l \sum_{i=0}^{r-1} (X_l x)^i = \sum_{l=0}^{t-1} h_{j_l} Y_l \sigma^{(l)} - \sum_{l=0}^{t-1} \sigma h_{j_l} Y_l \frac{e - (X_l x)^r}{e - X_l x} \\
&= \sum_{l=0}^{t-1} h_{j_l} Y_l \sigma^{(l)} - \sum_{l=0}^{t-1} h_{j_l} Y_l \sigma^{(l)} (e - X_l x) \frac{e - (X_l x)^r}{e - X_l x} = \left(\sum_{l=0}^{t-1} h_{j_l} Y_l \sigma^{(l)} X_l^r \right) x^r,
\end{aligned}$$

vagyis $\omega - \sigma S$ osztható x^r-rel, és ez éppen az említett kongruencia. A fenti kongruencia ekvivalens az $\omega = \vartheta x^r + \sigma S$ polinomegyenlőséggel, ahol ϑ egy alkalmas polinom. Ebben az egyenlőségben ismert x^r és S. Ha ismerjük ω-t, akkor σ az euklideszi algoritmus segítségével meghatározható, azonban ω-t nem ismerjük. Az alábbi tételből azonban kiderül, hogy S ismeretében mind σ, mind ω előállítható.

14.1. Tétel

Legyen $r_{-1} = x^r$, $r_0 = S \neq 0$, és az euklideszi algoritmus szerint $b_{-1} = 0$, $b_0 = e$, valamint $r_{i-1} = q_i r_i + r_{i+1}$ és $b_{i+1} = b_{i-1} - q_i b_i$, amíg $\deg(r_i) \geq \frac{r}{2}$. Ha r_k az első maradék, amelynek a fokszáma kisebb, mint $\frac{r}{2}$, akkor $\hat{b}_k(0) \neq 0$, és $\sigma = \left(\hat{b}_k(0)\right)^{-1} b_k$ és $\omega = \left(\hat{b}_k(0)\right)^{-1} r_k$.

Δ

Bizonyítás:

Láttuk, hogy ω felírható az x^r és S polinom-együtthatós lineáris kombinációjaként, vagyis megoldható az $\omega = x^r y + Sz$ egyenlet. A megoldhatóságból következik, hogy x^r és S legnagyobb közös osztója osztója ω-nak, és mivel ω nem nulla, ezért a legnagyobb közös osztó fokszáma nem nagyobb ω fokszámánál, vagyis kisebb, mint $\frac{r}{2}$. Ekkor van olyan $l \in \mathbb{N}$, hogy r_l foka kisebb, mint $\frac{r}{2}$. Mivel a maradékok fokszáma szigorúan monoton csökken, ezért az ilyen l indexek halmazában van egyértelműen meghatározott legkisebb k index, tehát a tételben megfogalmazott feltételnek megfelelő r_k polinom létezik és egyértelmű. Most nézzük az alábbi két egyenletet:

$$\omega = \vartheta x^r + \sigma S$$
$$r_k = a_k r^k + b_k S$$

(a_i-t az $a_{-1} = e$, $a_0 = 0$, $a_{i+1} = a_{i-1} - q_i a_i$ rekurzió határozza meg). A fenti két egyenletből

$$b_k \omega - r_k \sigma = (b_k \vartheta - a_k \sigma) x^r.$$

Ha a jobb oldalon zárójelben álló polinom nem nulla, akkor a jobb oldali polinom legalább r-edfokú. $\deg(b_k) = \deg(x^r) - \deg(r_{k-1}) \leq r - \frac{r}{2} = \frac{r}{2}$, hiszen k a legkisebb l index, amelyre r_l foka kisebb $\frac{r}{2}$-nél, $\deg(\omega) < t \leq \frac{r}{2}$, $\deg(r_k) < \frac{r}{2}$ és $\deg(\sigma) = t \leq \frac{r}{2}$. Ebből $\deg(b_k \omega) < \frac{r}{2} + \frac{r}{2} = r$ és hasonlóan $\deg(r_k \sigma) < \frac{r}{2} + \frac{r}{2} = r$, tehát ha a bal oldali polinom nem nulla, akkor a fokszáma r-nél kisebb, ami lehetetlen, hiszen az előbb láttuk, hogy a jobb oldalon legalább r-edfokú polinom áll. Ebből következik, hogy az egyenlet mindkét oldalán nulla áll, és így a bal oldali illetve a jobb oldalon a zárójelben álló különbség nulla, és így

$$b_k \omega = r_k \sigma$$
$$b_k \vartheta = a_k \sigma.$$

Figyelembe véve, hogy egyrészt a_k és b_k, másrészt σ és ω relatív prím, a fenti egyenlőségekből következik, hogy σ osztója b_k-nak és b_k osztója σ -nak, vagyis b_k és σ asszociáltak, és ha $\sigma = c b_k$, akkor c egy nem nulla konstans polinom és $\omega = c r_k$. A $\sigma = c b_k$ egyenlőségből $e = \hat{\sigma}(0) = c\hat{b}_k(0)$, tehát $\hat{b}_k(0) \neq 0$, majd innen $c = \left(\hat{b}_k(0)\right)^{-1}$, és végül $\sigma = \left(\hat{b}_k(0)\right)^{-1} b_k$ és $\omega = \left(\hat{b}_k(0)\right)^{-1} r_k$.

□

14.2. Megjegyzés

Bár az algoritmus szempontjából nem lényeges, azért megjegyezzük, hogy S nem osztója x^r-nek, és így $S \neq 0$ esetén $k > 0$. Ha $S = 0$, akkor nyilván igaz, hogy S nem osztja az x^r polinomot, ezért tegyük fel, hogy $S \neq 0$. Ekkor sem σ, sem ω nem 0, sőt, σ legalább elsőfokú. σ foka nagyobb, mint ω

foka, és így σS foka még inkább meghaladja a hibaérték-polinom fokszámát, ezért $\omega - \sigma S$ nem a null-polinom, és a foka σS fokával azonos. $\omega - \sigma S$ osztható x^r-rel, amiből következik, hogy σS foka legalább r, és akkor S foka legalább $\frac{r}{2}$, hiszen σ foka azonos a hibák számával, amiről feltettük, hogy legfeljebb $\frac{r}{2}$. Ha S osztója x^r-nek, akkor osztója $\omega - \sigma S$ -nek, tehát ω -nak is, ami lehetetlen, hiszen ekkor S foka nem haladhatná meg ω fokát, ami viszont kisebb, mint σ foka, tehát kisebb, mint $\frac{r}{2}$. Mellékeredményként azt kaptuk, hogy ha van hiba, de a hibák száma nem haladja meg $\frac{r}{2}$-t, akkor az egyébként legfeljebb $r - 1$-edfokú S polinom foka legalább $\frac{r}{2}$.

□

15. A kód idempotense

Test fölötti egyhatározatlanú polinomgyűrű euklideszi gyűrű, olyan euklideszi gyűrű, ahol a hányados és az osztási maradék egyértelműen meghatározott. Euklideszi gyűrű egyben főideálgyűrű, így minden ideálja generálható egyetlen elemmel, és ha az euklideszi gyűrűben a maradék egyértelmű, akkor egy adott, nem nulla elem által generált ideál szerinti maradékosztályok egyértelműen reprezentálhatóak a generáló elemmel való osztási maradékkal.

Legyen C egy $[n,k]$-paraméterű ciklikus kód a q-elemű test fölött. Ekkor C-t mint a kód elemeihez tartozó kódpolinomok összességét tekintve $C = \{ag | a \in \mathbb{F}_q[x] \wedge ((a \neq 0) \Rightarrow (deg(a) < k))\}$, ahol az $n-k$-fokú g főpolinom maga is eleme a kódnak. g osztója az $x^n - e$ polinomnak, C nem üres, zárt a kivonásra és az $\mathbb{F}_q$ elemeivel való szorzásra, és a C minden c elemére és minden $a \in \mathbb{F}_q$-ra $xc \bmod (x^n - e) \in C$ és $ac \bmod (x^n - e) = ac \in C$, vagyis $\bmod (x^n - e)$, ahol $\bmod f$ az f-fel való (egyértelműen meghatározott) osztási maradékot jelöli, zárt az x-szel és a-val való szorzásra. Ezen tulajdonság alapján $\bmod (x^n - e)$ bármely polinommal való szorzásra is zárt. $C. \bmod (x^n - e)$ végezve a műveleteket lényegében véve az $\mathbb{F}_q[x]/(x^n - e)$ maradékosztály-gyűrű elemeivel végezzük a műveletet, ami azt jelenti, hogy C (pontosabban szólva a C-beli elemekkel reprezentált osztályok, amelyeket azonban az egyértelműség miatt azonosíthatunk most magukkal az osztályokkal) ideálja az $\mathbb{F}_q[x]/(x^n - e)$ gyűrűnek. Ez indokolja, hogy kicsit foglalkozzunk az ideálokkal.

15.1. Definíció

Az n-változós f műveletre nézve u **idempotens**, ha $f(u, \cdots, u) = u$.

Δ

Multiplikatív félcsoportban tehát u idempotens, ha $u^2 = u$. Példa a félháló, ahol minden elem idempotens (a félháló egy halmaz egy asszociatív, kommutatív, idempotens művelettel; tipikus példa egy halmaz részhalmazai a közös résszel mint művelettel, vagy logikai algebrában az ÉS-művelet).

15.2. Tétel

Félcsoportban felcserélhető idempotens elemek szorzata idempotens.

Δ

Bizonyítás:
Ha $a^2 = a$, $b^2 = b$ és $ab = ba$, akkor $(ab)^2 = abab = aabb = a^2b^2 = ab$.

□

Ha a félcsoport két idempotens eleme nem felcserélhető, akkor már általában a szorzatuk nem idempotens. Erre példa a sík két, egymást egy pontban metsző egyenesére való vetítés kompozíciója.

15.3. Tétel

Félcsoport balról neutrális eleme és bal oldali zéruseleme idempotens.

Δ

Bizonyítás:
Ha e_b és z_b egy bal oldali egységelem illetve egy bal oldali zéruselem, akkor a félcsoport bármely u elemével $e_b u = u$ és $z_b u = z_b$, tehát $(e_b)^2 = e_b e_b = e_b$ és $(z_b)^2 = z_b z_b = z_b$.

□

Egy $\mathcal{A}$ grupoid a eleme **balról reguláris**, ha $\mathcal{A}$ bármely b eleméhez legfeljebb egy olyan u eleme van a struktúrának, amellyel $au = b$. a **reguláris**, ha mindkét oldalról reguláris. Ismert, hogy a pontosan akkor balról reguláris, ha valahányszor $au = av$ az $\mathcal{A}$-beli u és v elemekkel, mindannyiszor $u = v$.

Bal oldali neutrális elem mindig reguláris balról, hiszen ha e_b bal oldali semleges elem, és fennáll az $e_b u = e_b v$ egyenlőség, akkor $u = e_b u = e_b v = v$. Ugyanakkor bal oldali zéruselem akkor és csak akkor balról reguláris, ha nincs a grupoidnak más eleme, mert ha z_b bal oldali zéruselem, és u is a grupoid eleme, akkor $z_b u = z_b = z_b z_b$.

Félcsoportban balról reguláris elemek szorzata balról reguláris. Legyen ugyanis a és b egyaránt balról reguláris és legyen $(ab)u = (ab)v$. Ekkor $a(bu) = (ab)u = (ab)v = a(bv)$-ből $bu = bv$, és innen $u = v$. Ha a neutrális elemes félcsoport egy a elemének van bal oldali inverze, például a_b, akkor $au = av$-ből kapjuk, hogy $u = eu = (a_b a)u = a_b(au) = a_b(av) = (a_b a)v = ev = v$, vagyis ekkor a balról reguláris.

Egy grupoid (és így egy félcsoport) (balról) reguláris, ha minden eleme (balról) reguláris.

15.4. Tétel

Félcsoport eleme pontosan akkor balról reguláris idempotens elem, ha bal oldali neutrális elem.

Δ

Bizonyítás:

Bal oldali neutrális elem balról reguláris, és az előző eredmény alapján idempotens. Fordítva, legyen a félcsoportbeli u elem balról reguláris és idempotens. Ekkor a félcsoport bármely v elemével teljesül, hogy $u(uv) = (uu)v = u^2 v = uv$, és innen $uv = v$ (mert u-val balról lehet egyszerűsíteni), tehát u bal oldali egységeleme a félcsoportnak.

□

Az előbbi eredményből következik, hogy bal oldali zéruselem akkor és csak akkor balról reguláris idempotens elem, ha a félcsoportnak egyetlen eleme van. Az is adódik a fenti tételből, hogy reguláris félcsoportban legfeljebb egy idempotens elem van, a neutrális elem (ha létezik a félcsoportban).

15.5. Tétel

Legalább két elemet tartalmazó gyűrű pontosan akkor nullosztómentes, ha reguláris.

Δ

Bizonyítás:

A gyűrű bármely r elemével $r \cdot 0 = 0$, így ha $0 \neq r$ balról reguláris, és $rs = 0$ a szintén a gyűrűből vett s elemmel, akkor $s = 0$. Ha tehát mindegyik nem nulla elem reguláris, akkor egy szorzat csak úgy lehet nulla, ha legalább az egyik tényező a nullelem, a gyűrű tehát ez esetben nullosztómentes.

Fordítva, legyen a gyűrű nullosztómentes, és legyen a gyűrűbeli nem nulla r-rel $ru = rv$, ahol a jobb oldali tényezők ismét a gyűrű elemei. Ekkor $0 = r(u - v)$, ami csak úgy lehet, ha $u = v$, mert a gyűrű nullosztómentes, tehát r balról reguláris. Ugyanígy kapjuk, hogy r jobbról is reguláris, tehát reguláris, és a gyűrű reguláris.

□

15.6. Tétel

Véges félcsoport akkor és csak akkor csoport, ha reguláris.

Δ

Bizonyítás:

Reguláris $\mathcal{S}$ félcsoportban az $\mathcal{S}$ minden a elemével az $u \mapsto au$ és $u \mapsto ua$ leképezés injektíven képezi le S-t önmagába. De véges halmaz önmagába való leképezése akkor és csak akkor injektív, ha

szürjektív. Ez viszont azt jelenti, hogy S-beli bármely a-val és b-vel megoldható az $ax = b$ és $ya = b$ egyenlet, amiből következik, hogy $\mathcal{S}$ csoport.

Fordítva, ha a félcsoport nem reguláris, akkor van olyan a eleme, amely például balról nem reguláris. Ám ekkor a-nak még akkor sincs bal oldali inverze, ha van a félcsoportban bal oldali egységelem, mert már láttuk, hogy ha lenne, akkor a balról reguláris lenne.

□

15.7. Következmény

Legalább két elemet tartalmazó véges gyűrű vagy nem reguláris, vagy ferdetest.

Δ

Bizonyítás:

Véges gyűrű multiplikatív félcsoportja véges, és az előbbi tételek szerint ha reguláris, akkor a nem nulla elemek a szorzással csoportot alkotnak, így a gyűrű ferdetest.

□

15.8. Kiegészítés

Legalább két elemet tartalmazó, véges, reguláris gyűrű test.

Δ

A fenti állítás következik Wedderburn tételéből, amely szerint véges ferdetest kommutatív.

Legyen a az $\mathcal{S}$ félcsoport eleme. Ekkor az a pozitív egész kitevős hatványai vagy páronként különbözőek, vagy van olyan egyértelműen meghatározott k és a k-nál nagyobb l pozitív egész szám, hogy az a l-nél kisebb pozitív egész kitevős hatványai között nincs ismétlődés, ám $a^k = a^l$.

15.9. Definíció

Félcsoport a elemének rendje a pozitív egész l, ha a l-nél kisebb, pozitív egész kitevős hatványai páronként különbözőek, de $a^k = a^l$ egy alkalmas, az l-nél kisebb, pozitív egész kitevővel. Ha ilyen l nem létezik, akkor a rendje végtelen. Az a elem rendjét $o(a)$ vagy $|a|$ jelöli.

Δ

15.10. Tétel

Legyen a az $\mathcal{S}$ félcsoport l-edrendű eleme, $a^l = a^k$, ahol $l > k \in \mathbb{N}^+$, és legyen $m = l - k$. Ekkor minden pozitív egész t-hez van olyan egyértelműen meghatározott, az l-nél kisebb s pozitív egész szám, hogy $a^t = a^s$, és ha $t \geq k$, akkor $s = k + \big((t-k) \bmod m\big)$.

Δ

Bizonyítás:

Az egyértelműség következik abból, hogy a l-nél kisebb kitevős, pozitív egész kitevős hatványai különbözőek. Ugyanebből következik, hogy ha $t < k$, akkor $s = t$, hiszen ezesetben $t < k < l$.

$a^{k+0\cdot m} = a^{k+0} = a^k = a^l = a^{k+(l-k)} = a^{k+m} = a^{k+1\cdot m}$, és ha $a^k = a^{k+q\cdot m}$ egy $q \in \mathbb{N}$-nel, akkor $a^k = a^l = a^{k+m} = a^k a^m = a^{k+q\cdot m} a^m = a^{k+q\cdot m+m} = a^{k+(q+1)\cdot m}$, tehát minden nemnegatív egész q-val $a^k = a^{k+q\cdot m}$. Legyen t a k-nál nem kisebb egész szám, ekkor $t - k$ nemnegatív egész szám, és legyen $r = (t-k) \bmod m$. Most $t = k + q \cdot m + r$ egy nemnegatív egész q-val és r-rel. Az előző eredménnyel $a^t = a^{k+q\cdot m+r} = a^{k+q\cdot m} a^r = a^k a^r = a^{k+r} = a^s$. De $r = (t-k) \bmod m$ az m-nél kisebb nemnegatív egész szám, tehát $s = k + \big((t-k) \bmod m\big) = k + r < k + m = l$.

□

A tételből következik, hogy ha a félcsoport a elemének rendje l, és $a^l = a^k$ az l-nél kisebb pozitív egész k-val, akkor minden nemnegatív egész t-re $a^{k+t} = a^{l+t}$.

15.11. Tétel

Ha az $\mathcal{S}$ félcsoportban van véges rendű elem, akkor van idempotens elem.

Δ

Bizonyítás:

Legyen a a félcsoport l-edrendű eleme. Most $a^l = a^k$ egy, az l-nél kisebb pozitív egész k-val. Ha $m = l - k$, és $m > r \in \mathbb{N}$, akkor a^{k+r} akkor és csak akkor idempotens, ha $2(k + r) = k + r + qm$ egy alkamas nemnegatív egész m-mel. De ilyen r van, nevezetesen $r \equiv -k\ (m)$, azaz $(-k) \bmod m$.

□

Véges félcsoport minden eleme végesrendű, tehát, ha a véges félcsoport nem üres (és ezt általában beleértjük a félcsoport definíciójába), akkor a félcsoportban van idempotens elem. Gyűrű egy eleme idempotens, ha a gyűrű multiplikatív félcsoportjában idempotens. A gyűrűben mindig van ilyen elem, például a nulla. De ha a gyűrű legalább két elemet tartalmaz és véges, akkor van benne nullától különböző idempotens elem is.

Egy gyűrűben a 0-t és csak a 0-t tartalmazó halmaz ideál, a nullideál, és a gyűrűnek ideálja maga a gyűrű; ezek az ideálok a gyűrű triviális ideáljai, a többi ideál (ha van) a gyűrű nem triviális ideálja. A gyűrű mint önmaga ideálja a gyűrű egyetlen nem valódi ideálja, minden más ideál (ha van) valódi ideál. Nyilván a nullideál minden ideálnak része, és minden ideál része a teljes gyűrűnek mint a gyűrű ideáljának, így a nullgyűrű a legkisebb, maga a gyűrű a legnagyobb eleme a gyűrű ideáljainak a tartalmazással részben rendezett halmazában.

15.12. Definíció

Az $\mathcal{R}$ gyűrű $\mathcal{I}$ ideálja **minimális**, ha a gyűrű egyetlen, tőle különböző ideálját (a nullideált) tartalmazza, és **maximális**, ha egyetlen, nála szigorúan bővebb ideálja van a gyűrűnek (maga a gyűrű).

Δ

Részbenrendezett halmaz rendezett részhalmazát szokás **lánc**nak nevezni.

15.13. Tétel

Gyűrű ideáljai egy nem üres láncának uniója ideál a gyűrűben.

Δ

Bizonyítás:

Legyen $\{\mathcal{I}_\gamma | \gamma \in \Gamma \neq \emptyset\}$ az $\mathcal{R}$ gyűrű ideáljainak egy olyan rendszere, hogy a Γ bármely γ_1 és γ_2 elemével $\mathcal{I}_{\gamma_1}$ és $\mathcal{I}_{\gamma_2}$ közül legalább az egyik része a másiknak, és legyen $\mathcal{I} = \bigcup_{\gamma\in\Gamma} \mathcal{I}_\gamma$. A gyűrű nulleleme minden ideálnak eleme, így az unió minden tagja, de akkor maga az unió is tartalmazza a 0-t (mert az indexhalmaz nem üres), így az unióban is benne van ez az elem, az unió nem üres. Ha a és b az unió két eleme, akkor mindkettőt tartalmazza az unió valamely tagja, de a tagok rendezettségének köszönhetően a két tag közül az egyikben mindkét elem benne van, és akkor benne van a különbségük is, hiszen ez a tag ideál. Ugyanígy kapjuk, hogy a gyűrű tetszőleges r elemével ra és ar is benne van az a-t tartalmazó bal oldali ideálban, és így $\mathcal{I}$-ben is, $\mathcal{I}$ tehát valóban ideál.

□

15.14. Tétel

Ha a legalább két elemet tartalmazó $\mathcal{R}$ gyűrű egységelemes, akkor a gyűrű minden valódi ideálja része a gyűrű egy maximális ideáljának.

Δ

Bizonyítás:
A Zorn-lemma szerint ha egy részbenrendezett halmaz minden rendezett részhalmaza felülről korlátos az adott részbenrendezéssel, akkor a halmazban erre a részbenrendezésre nézve van maximális elem, és minden elemhez van nála nagyobb vagy vele egyenlő maximális elem. Amennyiben a gyűrű egységelemes, akkor a gyűrű egy ideálja pontosan akkor valódi, ha nem tartalmazza az egységelemet. De egységelemet nem tartalmazó ideálok uniója sem tartalmazza a gyűrű neutrális elemét, tehát egységelemes gyűrűben valódi ideálok bármely láncának uniója is a gyűrű valódi ideálja, így a valódi ideáloknak a tartalmazással részbenrendezett halmazában minden rendezett részhalmaznak van felső korlátja. Ekkor a Zorn-lemma értelmében igaz a tétel állítása.

□

Érdemes megjegyezni, hogy az üres lánc is felülről korlátos, mert egy felső korlátja a nullideál.

Véges gyűrűnek csak véges sok ideálja van. Véges részbenrendezett halmazban van minimális elem, és minden elem nagyobb vagy egyenlő legalább egy minimális elemnél, így véges testtől különböző véges gyűrűben van minimális ideál, és minden ideál tartalmaz minimális ideált. Végtelen gyűrűben ez nem feltétlenül igaz: az egész számok gyűrűje a szokásos műveletekkel főideálgyűrű, és a gyűrű bármely nem nulla elemének van valódi többszöröse, így ebben a gyűrűben a nullideáltól különböző bármely ideál tartalmazza a gyűrű egy nála határozottan szűkebb ideálját.

Ha $\mathcal{I}$ az $\mathcal{R}$ gyűrű ideálja, akkor az R-beli azon $\sim$ reláció, ahol a gyűrű a és b elemére $a \sim b$ akkor és csak akkor, ha $a - b \in R$, ekvivalencia-reláció R-en, és így osztályoz. Az osztályok a maradékosztályok, és az a által reprezentált maradékosztályt $\bar{a}$ jelöli. A maradékosztályok összeadhatóak és összeszorozhatóak, ha a műveleteket úgy értelmezzük, hogy a reprezentánsokkal végzett művelet eredményét tartalmazó osztály az osztályművelet eredménye. Ekkor gyűrűt kapunk, az adott ideál szerinti maradékosztály-gyűrűt, $\mathcal{R}/\mathcal{I}$-t.

Kommutatív gyűrű bármely ideálja szerinti maradékosztály-gyűrű kommutatív, egységelemes gyűrű bármely ideálja szerinti maradékosztály-gyűrű egységelemes (a maradékosztály-gyűrű egységeleme a gyűrű egységelemét tartalmazó osztály), de a nullosztó-mentességre ez általában nem igaz. $\mathbb{Z}$ nullosztómentes, és nullosztómentes $\mathbb{Z}/7\mathbb{Z} = \mathbb{Z}_7$, de nem nullosztómentes $\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12}$. Nem nullosztómentes $\mathbb{Z}_{12}/3\mathbb{Z}_{12} \cong \mathbb{Z}_4$, ám nullosztómentes $\mathbb{Z}_{12}/4\mathbb{Z}_{12} \cong \mathbb{Z}_3$. Nézzük, mikor lesz egy maradékosztály-gyűrű nullosztómentes (függetlenül attól, hogy maga a gyűrű ilyen tulajdonságú-e).

A maradékosztály-gyűrű nulleleme az az ideál, amely szerint a maradékosztály-gyűrűt képeztük. Ezek szerint a gyűrű valamely a és b eleme által reprezentált osztályok akkor alkotnak nullosztópárt, ha ők maguk nem, de a szorzatuk nulleleme a maradékosztály-gyűrűnek. Ez pontosan akkor igaz, ha a két elem nincs benne az ideálban, de a szorzatuk eleme az ideálnak. Ez az alábbi definícióhoz vezet.

15.15. Definíció

Az $\mathcal{R}$ gyűrű egy nem triviális $\mathcal{P}$ ideálja **prímideál**, ha valahányszor a gyűrű a és b elemének szorzata eleme az ideálnak, mindannyiszor a két elem legalább egyike is benne van az ideálban.

Δ

15.16. Tétel

Nem triviális $\mathcal{I}$ ideál szerinti maradékosztály-gyűrű pontosan akkor nullosztómentes, ha $\mathcal{I}$ prímideál. Ha $\mathcal{M}$ az $\mathcal{R}$ egységelemes kommutatív gyűrű maximális ideálja, akkor $\mathcal{M}$ prímideál, és $\mathcal{R}/\mathcal{M}$ test.

Δ

Bizonyítás:

Az első állítás bizonyítása a fenti definíció előtt megtörtént.

Legyen $\mathcal{M}$ a gyűrű egy maximális ideálja, és a és b a gyűrű olyan elemei, hogy $ab \in M$, de mondjuk a a gyűrű M-en kívüli eleme. A legszűkebb, az a-t és M minden elemét egyaránt tartalmazó ideál az $A = \{ra + m | r \in R \wedge m \in M\}$ halmaz, amely maga a teljes gyűrű, hiszen ez határozottan bővebb M-nél, és $\mathcal{M}$ maximális ideál. Ekkor $e \in A$, azaz $e = r'a + m'$. De innen kapjuk, hogy $b = r'(ab) + bm' = r'(ab) + \tilde{m} \in M$, b eleme az ideálnak, $\mathcal{M}$ tehát prímideál.

Még azt kell belátni, hogy $\mathcal{R}/\mathcal{M}$ nem nulla elemeinek van inverze. $\bar{a} = \bar{0}$ akkor és csak akkor, ha $a \in M$, legyen tehát a a gyűrű egy M-en kívüli eleme. Az előbbiek szerint ekkor $e = r'a + m'$, másként írva $\bar{e} = \overline{r'a + m'} = \bar{r'}\bar{a} + \overline{m'} = \bar{r'}\bar{a} + \bar{0} = \bar{r'}\bar{a}$, és így $\mathcal{R}/\mathcal{M}$-ben $\bar{r'}$ inverze $\bar{a}$-nak, vagyis a maradékosztály-gyűrű minden nem nulla elemének van inverze, a gyűrű test (mert kommutatív).

□

A fenti tétel szerint egységelemes kommutatív gyűrű legalább két elemet tartalmazó maximális ideálja prímideál, de ez általában fordítva nem igaz. Tekintsük $\mathbb{Z}[x]$-ben a $(2, x)$ ideált. Ebben azok és csak azok az egész együtthatós polinomok vannak, amelyeknek konstans tagja páros egész szám, tehát ez valódi ideálja a gyűrűnek, és nyilván valódi módon tartalmazza az x polinom által generált ideált, így ez utóbbi biztosan nem maximális. De prímideál, mert egy polinom akkor és csak akkor tartozik hozzá ehhez az ideálhoz, ha a konstans tagja 0, és nullosztómentes gyűrű feletti két polinom szorzatának konstans tagja akkor és csak akkor nulla, ha legalább egyikük hasonló tulajdonságú.

$\mathbb{Z}[x]$ Gauss-gyűrű, tehát már Gauss-gyűrűben sem mindig igaz, hogy prímideál maximális. Ám főideál-gyűrűben igaz a megfordítás is. Főideál-gyűrűben egy ideál akkor és csak akkor maximális, ha a generáló eleme felbonthatatlan, és pontosan akkor prímideál, ha egy prímelem generálja. De főideál-gyűrűben az előbbi két tulajdonság egybeesik, és ekkor pontosan a prímideálok a maximális ideálok.

Gyűrű bármely ideálja egyben bal oldali ideálja a gyűrűnek (ez fordítva általában nem igaz, ellenpélda lehet $1 < n \in \mathbb{N}$-nel egy gyűrű feletti n-edrendű négyzetes mátrixok gyűrűjében azon mátrixok összessége, amelyekben az oszlopok azonosak). A nullideál és a gyűrű mint önmaga ideálja a gyűrű nem triviális bal oldali ideáljai, a többi bal oldali ideál nem triviális bal oldali ideál. Bár nem lesz szükségünk rá, de a teljesség kedvéért megnézzük, melyek azok a gyűrűk, amelyekben csak triviális bal oldali ideálok (és így még inkább csak triviális ideálok) vannak. Előtte új fogalommal ismerkedünk meg.

Az $\mathcal{R}$ gyűrű egy u eleme **bal oldali annullátora** az R egy X részhalmazának, ha $uX = \{0\}$. Ha u és v bal oldali annullátora X-nek, és r a gyűrű tetszőleges eleme, akkor X bármely a elemével $(ru)a = r(ua) = r \cdot 0 = 0$ és $(u - v)a = ua - va = 0 - 0 = 0$, az X bal oldali annullátorainak B összessége, az X bal oldali annullátora bal oldali ideál (mert nem üres, hiszen a gyűrű nullelemét biztosan tartalmazza). Ha maga X is bal oldali ideál, akkor $(ur)a = u(ra) = ub = 0$, mert mos $ra = b$ is eleme X-nek, vagyis ekkor B ideál a gyűrűben.

Ha a legalább két elemet tartalmazó $\mathcal{R}$ gyűrűben van jobbról reguláris elem, és van olyan balról reguláris a elem, amellyel $ae = a$ a gyűrű egy e elemével, akkor e egységeleme a gyűrűnek. Legyen ugyanis b egy jobbról reguláris elem és c a gyűrű tetszőleges eleme. Ekkor $ac = (ae)c = a(ec)$ egyszerűsíthető a-val, tehát $c = ec$, e bal oldali egységelem, és így az is igaz, hogy $b = eb$, de ebből ugyanígy kapjuk, hogy e jobb oldalról is egységelem, tehát egységelem.

15.17. Tétel

Ferdetestnek csak triviális bal oldali ideáljai vannak. Fordítva, ha egy legalább két elemet tartalmazó gyűrű minden bal oldali ideálja triviális, akkor a gyűrű vagy egy prímszámrendű zérógyűrű vagy ferdetest.

Δ

Bizonyítás:

Legyen $\mathcal{I}$ az $\mathcal{F}$ ferdetest egy, a nullideáltól különböző bal oldali ideálja, és legyen $a \neq 0$ az I, b az $\mathcal{F}$ tetszőleges eleme. Ekkor $b = be = b(a^{-1}a) = (ba^{-1})a \in I$, I tartalmazza a ferdetest minden elemét, így $I = F$, $\mathcal{F}$-ben csak triviális bal oldali ideál van.

Legyen most $\mathcal{R}$ egy olyan, legalább kételemű gyűrű, amelyben csak a két triviális bal oldali ideál van. $\mathcal{R}$ bal oldali annullátora bal oldali ideál, tehát vagy csak a nullát tartalmazza, vagy maga a gyűrű. Az utóbbi esetben $RR = \{0\}$, azaz ekkor $\mathcal{R}$ egy zérógyűrű. Egy gyűrű minden ideálja a gyűrű additív csoportjának részcsoportja, és zérógyűrűben ez visszafelé is igaz. Ha egy csoport nem ciklikus, akkor biztosan van nem triviális részcsoportja. Legyen a egy ciklikus csoport generáló eleme. Ha a csoport végtelen, akkor az a^2 által generált részcsoport nem triviális, mint ahogy az a^u által generált részcsoport is nem triviális, ha a csoport rendje uv úgy, hogy a szorzat mindkét tényezője 1-nél nagyobb egész szám. Ha viszont a csoport prímszámrendű, akkor nincs nem triviális részcsoportja, hiszen véges csoport részcsoportjának rendje osztója a csoport rendjének.

A másik esetben R-nek egyetlen bal oldali annullátora a gyűrű nulleleme. A gyűrű jobb oldali annullátora ideál, tehát bal oldali ideál, és így ez is csak a nullát tartalmazhatja. Legyen r a gyűrű tetszőleges, nem nulla eleme. Rr bal oldali ideál, tehát $Rr = R$, mert ellenkező esetben $Rr = \{0\}$, ami nem lehet, mert ez azt jelentené, hogy R-nek van nem nulla jobb oldali annullátora. $Rr = R$ egyrészt azt jelenti, hogy $\mathcal{R}$ nullosztómentes, vagyis minden nem nulla eleme reguláris, mert ha $ab = 0$, akkor a bal oldali annullátora a $\{b\}$ halmaznak. Másrészt $Rr = R$ azt jelenti, hogy a gyűrű bármely b és tetszőleges $a \neq 0$ elemével megoldható a gyűrűben az $ya = b$ egyenlet, tehát az $ya = a$ egyenlet is, és ha ennek megoldása e, akkor e egységelem. Mivel az $ya = e$ egyenlet is megoldható, ezért minden nem nulla elemnek van bal oldal inverze, vagyis a gyűrű nem nulla elemeinek halmazában van olyan e bal oldali neutrális elem, hogy valamennyi a-hoz létezik a_b, amellyel $a_b a = e$, és ebből következik, hogy a gyűrű minden nem nulla elemének van inverze, a gyűrű tehát ferdetest.

□

15.18. Tétel

Gyűrű ideáljai tetszőleges rendszerének metszete a gyűrű ideálja.

Δ

Bizonyítás:

A metszet minden tagja, így maga a metszet is tartalmazza a nullelemet, a metszet nem üres. Ugyanígy, a metszet bármely két elemének különbsége, valamint bármelyiküknek a gyűrű tetszőleges elemével vett szorzata benne van minden tagban, és így a metszetben is, a metszet tehát valóban ideál.

□

A tétel akkor is igaz, ha a rendszer az üres halmaz, hiszen ekkor a metszet maga a gyűrű.

A tétel szerint a gyűrű ideáljainak a tartalmazással részbenrendezett halmazában minden részhalmaznak létezik az alsó határa (a halmazban lévő ideálok metszete), de ekkor bármely részhalmaznak, azaz ideálok bármely rendszerének van erre a részbenrendezésre nézve felső határa. Ez azonban nem az ideálok uniója, mert az általában nem tartalmazza a halmaz két különböző tagjából vett elem összegét. Igaz azonban a következő definíció utáni tétel.

15.19. Definíció

Legyen $n \in \mathbb{N}$, és legyen $n > k \in \mathbb{N}$-re $\mathcal{I}_k$ az $\mathcal{R}$ gyűrű ideálja. Ekkor $\mathcal{I} = \left\{\sum_{k=0}^{n-1} a_k \middle| a_k \in \mathcal{I}_k\right\}$ az $\mathcal{I}_k$ **ideálok összege**, amit $\sum_{k=0}^{n-1} \mathcal{I}_k$ jelöl.

Δ

15.20. Tétel

Legyen $\{\mathcal{I}_\gamma | \gamma \in \Gamma\}$ az $\mathcal{R}$ gyűrű ideáljainak egy rendszere és $\mathcal{I} = \bigcup_{\substack{\Delta \subseteq \Gamma \\ |\Delta| \in \mathbb{N}}} \sum_{\gamma \in \Delta} \mathcal{I}_\gamma$. Ekkor $\mathcal{I}$ az $\mathcal{R}$ legszűkebb, a rendszer minden ideálját tartalmazó ideálja.

Δ

Bizonyítás:

Ha $\mathcal{J}$ az $\mathcal{J}_\gamma$-k mindegyikét tartalmazó ideál, akkor tartalmaznia kell bármely kettőből vett tetszőleges két elem összegét, és innen indukcióval akárhogyan választott véges sok ideálhoz tartozó elemek összegét, vagyis $\bigcup_{\substack{\Delta\subseteq\Gamma \\ |\Delta|\in\mathbb{N}}} \sum_{\gamma\in\Delta}\mathcal{J}_\gamma \subseteq \mathcal{J}$-nek biztosan teljesülnie kell. De a bal oldali halmaz már ideál. Vegyük ugyanis tetszőleges két elemét, $u^{(1)} = \sum_{\gamma\in\Delta_1} a_\gamma^{(1)}$-t és $u^{(2)} = \sum_{\gamma\in\Delta_2} a_\gamma^{(2)}$-t, ahol mindkét indexhalmaz a Γ véges részhalmaza. Legyen $\Delta = \Delta_1 \cup \Delta_2$, $i \in \{1,2\}$, és legyen $\gamma \in \Delta \setminus \Delta_i$-re $a_\gamma^{(i)} = 0$. Ekkor $u^{(i)} = \sum_{\gamma\in\Delta_i} a_\gamma^{(i)} = \sum_{\gamma\in\Delta} a_\gamma^{(i)}$, tehát $u = u^{(1)} - u^{(2)} = \sum_{\gamma\in\Delta}\left(a_\gamma^{(1)} - a_\gamma^{(2)}\right) \in \sum_{\gamma\in\Delta} I_\gamma \subseteq I$, hiszen minden Δ-beli γ indexre $a_\gamma^{(1)} - a_\gamma^{(2)} \in I_\gamma$. Ennél még egyszerűbben kapjuk, hogy $ru^{(i)}$ is benne van a véges sok $\mathcal{J}_\gamma$ összegében, hiszen $ru^{(i)} = \sum_{\gamma\in\Delta_i} ra_\gamma^{(i)} \in \sum_{\gamma\in\Delta} I_\gamma$.

□

Ha $\mathcal{J}_1$ és $\mathcal{J}_2$ két ideál, $a_1^{(1)} \in \mathcal{J}_1$, $a_2^{(1)} \in \mathcal{J}_1$, $a_1^{(2)} \in \mathcal{J}_2$, $a_2^{(2)} \in \mathcal{J}_2$, és $a_1^{(1)} + a_1^{(2)} = a_2^{(1)} + a_2^{(2)}$, akkor $a_1^{(1)} - a_2^{(1)} = a_2^{(2)} - a_1^{(2)}$. A jobb oldali elem $\mathcal{J}_1$-beli, míg a másik különbség az $\mathcal{J}_2$ ideál eleme, ezért a különbség eleme a metszetnek. Ideálok metszete biztosan tartalmazza a gyűrű nullelemét, és ha más közös elem nincs, akkor $a_1^{(1)} - a_2^{(1)} = 0 = a_2^{(2)} - a_1^{(2)}$, tehát $a_1^{(1)} = a_2^{(1)}$ és $a_1^{(2)} = a_2^{(2)}$, vagyis ebben az esetben az összeg minden eleme egy és csak egyféleképpen áll elő a két ideál elemeinek összegeként. Ha viszont a metszetnek egynél több eleme van, akkor már biztosan lesz az összegnek olyan eleme, amelynek a tagokból vett összegként való felírása nem egyértelmű. Indukcióval kiadódik, hogy ez általában is igaz, vagyis pontosan akkor egyértelmű egy legalább kéttagú összeg egy elemének megadása, ha az összeg bármely tagjának a többi tag összegével egyetlen közös eleme van.

Tetszőleges gyűrűben a nullideál főideál, a nullelem által generált főideál, és egységelemes gyűrűben a teljes gyűrű mint önmaga ideálja is főideál, ezt az ideált generálja bármely egység, például az egységelem, és csak ezek az elemek. Ha a az $\mathcal{R}$ gyűrű egy eleme, akkor Ra bal oldali ideálja a gyűrűnek, de ez általában nem ideál és nem az a által generált bal oldali ideál. Amennyiben a gyűrű egységelemes, akkor már bal oldali ideál, illetve ha a gyűrű kommutatív, akkor ideál, következésképpen egységelemes, kommutatív gyűrűben $(a) = Ra$. Egy ilyen gyűrűben $(a) \subseteq (b)$ akkor és csak akkor, ha $b|a$ (következésképpen a két ideál pontosan akkor azonos, ha a két elem asszociált).

15.21. Tétel

Legyen $\{(a_\gamma)|\gamma \in \Gamma \wedge a_\gamma \in R\}$ az $\mathcal{R}$ gyűrű főideáljainak egy rendszere. Ha $\mathcal{R}$ Gauss-gyűrű, akkor az (a_γ)-k metszete az a_γ-k legkisebb közös többszöröse által generált főideál, míg főideál-gyűrűben $\sum_{\gamma\in\Gamma}(a_\gamma) = (d)$, ahol d az a_γ-k legnagyobb közös osztója.

Δ

Bizonyítás:

Gauss-gyűrű kommutatív és egységelemes, tehát egy adott elem által generált főideál az elem többszöröseinek összessége. Egy ilyen gyűrű bármely részhalmazának létezik az asszociáltságtól eltekintve egyértelműen meghatározott legkisebb közös többszöröse. Ha az a_γ-k legkisebb közös többszöröse t, akkor ez a metszet minden tagjában, de akkor magában a metszetben is benne van, és akkor a metszet eleme a t minden többszöröse, azaz a (t) minden eleme is, így (t) része a metszetnek. Ugyanakkor a metszet egy u eleme közös többszöröse az a_γ-knak, így a legkisebb közös többszörösüknek, t-nek is, amiből következik, hogy a metszet része a t által generált főideálnak, tehát meg is egyeznek egymással.

Főideálgyűrű Gauss-gyűrű, a gyűrű bármely részhalmazának van lényegében véve egyértelműen meghatározott legnagyobb közös osztója, és minden ideálja generálható egyetlen elemmel. Ekkor ez igaz az (a_γ) ideálok $\sum_{\gamma\in\Gamma}(a_\gamma) = \left\{\sum_{\gamma\in\Delta} u_\gamma \,\middle|\, \Delta \subseteq \Gamma \wedge |\Delta| \in \mathbb{N} \wedge u_\gamma \in a_\gamma\right\}$ összegére is. u_γ osztható a_γ-val, ez pedig az a_γ-k legnagyobb közös osztójával, d-vel, így d osztója $\sum_{\gamma\in\Delta} u_\gamma$-nak, tehát $\sum_{\gamma\in\Gamma}(a_\gamma)$

minden elemének, az ideálok összege része (d)-nek. Másrészről $\sum_{\gamma\in\Gamma}(a_\gamma) = (a)$ a gyűrű egy a elemével, tehát $a \in \sum_{\gamma\in\Gamma}(a_\gamma)$, vagyis $a = \sum_{\gamma\in\Delta} u_\gamma$ a Γ valamely véges Δ részhalmazával és a Δ elemeivel indexelt (a_γ) ideálokhoz tartozó u_γ elemekkel. De a $\sum_{\gamma\in\Delta} u_\gamma$ összeg minden tagja, következésképpen maga az összeg, azaz a is osztható d-vel, ezért $(a) \subseteq (d)$, és ekkor $\sum_{\gamma\in\Gamma}(a_\gamma) = (a) = (d)$.

□

Gauss-gyűrűben általában nem igaz, hogy főideálok összege a generáló elemek legnagyobb közös osztója által generált főideál, és még csak az sem feltétlenül igaz, hogy az összeg főideál. Már korábban néztük $\mathbb{Z}[x]$-ben a $(2, x)$ ideált. Ez a (2) és az (x) ideál összege. A két generáló elem legnagyobb közös osztója 1, és (1) nyilván nem azonos a $(2, x)$ ideállal, hiszen ez valódi részhalmaza $\mathbb{Z}[x]$-nek. Az viszont igaz, hogy Gauss-gyűrűben $(A) \subseteq (d)$, ha d az A (és akkor az (A)) legnagyobb közös osztója.

15.22. Következmény

Ha A és B az $\mathcal{R}$ főideálgyűrű olyan részhalmazai, hogy A legnagyobb közös osztója megegyezik B legkisebb közös többszörösével, akkor $\sum_{a\in A}(a) = \bigcap_{b\in B}(b)$.

Δ

Bizonyítás:
Ha A legnagyobb közös osztója d és B legkisebb közös többszöröse t, akkor $\sum_{a\in A}(a) = (d)$ és $\bigcap_{b\in B}(b) = (t)$. Ha tehát $d = t$, akkor $\sum_{a\in A}(a) = \bigcap_{b\in B}(b)$.

□

15.23. Tétel

Legyen $\{A_\delta | \delta \in \Delta\}$ és $\{B_\delta | \delta \in \Delta\}$ az $\mathcal{R}$ főideálgyűrű részhalmazainak olyan rendszere, hogy a Δ minden δ elemére $d_\delta = t_{\uparrow\delta}$, ahol d_δ az A_δ legnagyobb közös osztója és t_δ a B_δ legkisebb közös többszöröse, és legyen $\bigcup_{\delta\in\Delta} B_\delta = B$. Ekkor $\bigcap_{\delta\in\Delta}\sum_{a\in A_\delta}(a) = \bigcap_{b\in B}(b)$.

Δ

Bizonyítás:
$\bigcap_{\delta\in\Delta}\sum_{a\in A_\delta}(a) = \bigcap_{\delta\in\Delta}\bigcap_{b\in B_\delta}(b) = \bigcap_{b\in B}(b)$.

□

Gyűrű homomorfizmusánál a leképezés magja ideál, a kép izomorf a mag szerinti maradékosztály-gyűrűvel, és a gyűrű minden ideálja magja a gyűrű egy homomorfizmusának, például annak a leképezésnek, ahol a gyűrű minden elemét az őt tartalmazó maradékosztályra képezzük.

15.24. Tétel

Legyen $\mathcal{I}$ és $\mathcal{J}$ az $\mathcal{R}$ gyűrű ideálja, és legyen φ az $\mathcal{R}$-nek $\mathcal{R}/\mathcal{I}$-re való kanonikus szürjekciója, vagyis a $\varphi: r \mapsto \bar{r}$ leképezés, ahol most $\bar{r}$ az r-et tartalmazó $\mathcal{I}$ szerinti maradékosztály. Ekkor $\varphi(\mathcal{J})$ ideál a maradékosztály-gyűrűben, főideál képe főideál, és az $\mathcal{R}/\mathcal{I}$ minden ideáljának teljes inverze az $\mathcal{R}$ egy, az $\mathcal{I}$-t tartalmazó ideálja. $\varphi(\mathcal{J})$ teljes inverze $\mathcal{I} + \mathcal{J}$, és ha $I \subseteq J$, akkor $(\varphi^{-1}\varphi)(\mathcal{J}) = \mathcal{J}$.

Δ

Bizonyítás:
φ homomorf, tehát ha a és b eleme J-nek és r az R-nek, akkor $\bar{a} - \bar{b} = \overline{a - b} \in \varphi(J)$, valamint $\bar{r}\bar{a} = \overline{ra} \in \varphi(J)$, és ideál nem üres, tehát az ideál képe sem üres. Homomorfizmusnál generátorrendszer képe generátorrendszere a képnek, amiből következik, hogy főideál képe főideál.

A képtér ideáljának teljes inverze tartalmazza a képtér nullelemének teljes inverzét, tehát tartalmazza I-t (és így biztosan nem üres). Ha az ideál teljes inverzéből veszünk két elemet, ezek képei, de

akkor a különbségük is eleme az ideálnak, és így a két elem különbsége, mint a képek különbségének inverze is benne van az ideál teljes inverzében. Ugyanígy láthatjuk, hogy az ideál inverzének a gyűrű bármely elemével vett szorzata is benne van az ideál teljes inverzében, tehát ideál teljes inverze ideál.

Ha c eleme $\varphi(\mathcal{J})$ teljes inverzének, akkor egy $\mathcal{J}$-beli a elem képének egy őse. Legyen $b = c - a$. Ekkor $\varphi(a) + \bar{0} = \varphi(a) = \varphi(c) = \varphi(a+b) = \varphi(a) + \varphi(b)$, tehát $\varphi(b) = \bar{0}$, amiből következik, hogy $b \in \mathcal{I}$, így $c \in \mathcal{I} + \mathcal{J}$, és $\varphi^{-1}\big(\varphi(\mathcal{J})\big) \subseteq \mathcal{I} + \mathcal{J}$. Ugyanakkor halmaz képének teljes inverze tartalmazza az eredeti halmazt, így $\varphi(\mathcal{J})$ teljes inverze egy, a J-t, továbbá az előbbiek szerint $\mathcal{I}$-t is tartalmazó ideál. A legszűkebb, mind az $\mathcal{I}$, mind a $\mathcal{J}$ ideált tartalmazó ideál $\mathcal{I} + \mathcal{J}$, így ez része $\varphi^{-1}\big(\varphi(\mathcal{J})\big)$-nek, és az előbbi, fordított irányú tartalmazással következik, hogy a $\varphi(\mathcal{J})$ teljes inverze $\mathcal{I} + \mathcal{J}$.

Ha $I \subseteq J$, akkor $(\varphi^{-1}\varphi)(\mathcal{J}) = \varphi^{-1}\big(\varphi(\mathcal{J})\big) = \mathcal{I} + \mathcal{J} = \mathcal{J}$, mert az adott tartalmazás miatt minden olyan összeg, amelynek egyik tagja I-beli, a másik J eleme, J-hez tartozik.

□

$\mathcal{J}$ és $\mathcal{I} + \mathcal{J}$ képe azonos az $\mathcal{R}/\mathcal{I}$ gyűrűben, és a tétel alapján a $\mathcal{J}_1$ és $\mathcal{J}_2$ ideál $\mathcal{R}/\mathcal{I}$-beli képe akkor és csak akkor azonos, ha $\mathcal{I} + \mathcal{J}_1 = \mathcal{I} + \mathcal{J}_2$. Speciálisan, ha $\mathcal{R}$ főideálgyűrű, $\mathcal{I} = (a)$ és $\mathcal{J} = (b)$, akkor $\mathcal{J}$ képe az $\mathcal{R}/\mathcal{I}$ gyűrűben azonos (d) képével, ahol d az a és b legnagyobb közös osztója, hiszen most $\mathcal{I} + \mathcal{J} = (d)$. Ebből következően $\mathcal{R}/\mathcal{I}$ ideáljai az a osztói által generált $\mathcal{R}$-beli ideálok $\mathcal{R}/\mathcal{I}$-beli képei.

15.25. Tétel

Ha $\mathcal{I}$ és minden $\gamma \in \Gamma$-ra $\mathcal{J}_\gamma$ az $\mathcal{R}$ gyűrű ideálja, és φ az $\mathcal{R}$ gyűrű $\mathcal{R}/\mathcal{I}$-be való homomorfizmusa, akkor $\varphi\big(\sum_{\gamma\in\Gamma}\mathcal{J}_\gamma\big) = \sum_{\gamma\in\Gamma}\varphi\big(\mathcal{J}_\gamma\big)$, és ha minden γ-ra $I \subseteq J_\gamma$, akkor $\varphi\big(\bigcap_{\gamma\in\Gamma}\mathcal{J}_\gamma\big) = \bigcap_{\gamma\in\Gamma}\varphi\big(\mathcal{J}_\gamma\big)$.

Δ

Bizonyítás:

$\sum_{\gamma\in\Gamma}\mathcal{J}_\gamma = \big\{\sum_{\gamma\in\Delta} j_\gamma \,\big|\Delta \subseteq \Gamma \wedge |\Delta| \in \mathbb{N}\big\}$. φ műveletartó, ezért $\varphi\big(\sum_{\gamma\in\Delta} j_\gamma\big) = \sum_{\gamma\in\Delta}\varphi\big(j_\gamma\big)$, így

$$\varphi\left(\sum_{\gamma\in\Gamma}\mathcal{J}_\gamma\right) = \varphi\big(\big\{\sum_{\gamma\in\Delta} j_\gamma \,\big|\Delta \subseteq \Gamma \wedge |\Delta| \in \mathbb{N}\big\}\big) = \big\{\varphi\big(\sum_{\gamma\in\Delta} j_\gamma\big)\big|\Delta \subseteq \Gamma \wedge |\Delta| \in \mathbb{N}\big\}$$
$$= \big\{\sum_{\gamma\in\Delta}\varphi\big(j_\gamma\big) \,\big|\Delta \subseteq \Gamma \wedge |\Delta| \in \mathbb{N}\big\} = \sum_{\gamma\in\Gamma}\varphi\big(\mathcal{J}_\gamma\big),$$

mert $\varphi\big(\mathcal{J}_\gamma\big)$ ideál, és $\varphi\big(J_\gamma\big) = \big\{\varphi(j)\big|j \in J_\gamma\big\}$.

Ha f az A halmazt a B halmazba képező függvény, és az A_γ halmazok az A, a B_δ halmazok a B részhalmazai a Γ-beli γ és Δ-beli δ indexekkel, akkor $f\big(\bigcap_{\gamma\in\Gamma} A_\gamma\big) \subseteq \bigcap_{\gamma\in\Gamma} f\big(A_\gamma\big)$, $f^{-1}\big(\bigcap_{\delta\in\Delta} B_\delta\big) = \bigcap_{\delta\in\Delta} f^{-1}(B_\delta)$, és $(ff^{-1})(B_\delta) = f\big(f^{-1}(B_\delta)\big) = B_\delta \cap Im(f)$. Legyen most $\mathcal{I}$ és minden $\gamma \in \Gamma$-ra $\mathcal{J}_\gamma$ az $\mathcal{R}$ gyűrű ideálja úgy, hogy valamennyi γ-ra $I \subseteq J_\gamma$, legyen $\mathcal{J} = \bigcap_{\gamma\in\Gamma}\mathcal{J}_\gamma$ továbbá φ az $\mathcal{R}$ gyűrű $\mathcal{R}/\mathcal{I}$-be való homomorfizmusa. Ekkor $I \subseteq J$, és

$$\mathcal{J} = (\varphi^{-1}\varphi)(\mathcal{J}) = \varphi^{-1}\big(\varphi(\mathcal{J})\big) = \varphi^{-1}\left(\varphi\left(\bigcap_{\gamma\in\Gamma}\mathcal{J}_\gamma\right)\right) \subseteq \varphi^{-1}\left(\bigcap_{\gamma\in\Gamma}\varphi\big(\mathcal{J}_\gamma\big)\right)$$
$$= \bigcap_{\gamma\in\Gamma}\varphi^{-1}\left(\varphi\big(\mathcal{J}_\gamma\big)\right) = \bigcap_{\gamma\in\Gamma}(\varphi^{-1}\varphi)\big(\mathcal{J}_\gamma\big) = \bigcap_{\gamma\in\Gamma}\mathcal{J}_\gamma = \mathcal{J},$$

tehát $\varphi^{-1}\left(\varphi\big(\bigcap_{\gamma\in\Gamma}\mathcal{J}_\gamma\big)\right) = \varphi^{-1}\big(\bigcap_{\gamma\in\Gamma}\varphi\big(\mathcal{J}_\gamma\big)\big)$. De szürjektív leképezésnél $f\big(f^{-1}(V)\big) = V$, így ilyen esetben különböző halmazok teljes inverze különböző, amiből $\varphi\big(\bigcap_{\gamma\in\Gamma}\mathcal{J}_\gamma\big) = \bigcap_{\gamma\in\Gamma}\varphi\big(\mathcal{J}_\gamma\big)$.

□

15.26. Tétel

Főideálgyűrű nem triviális ideálja pontosan akkor maximális, ha generáló eleme irreducibilis, és pontosan akkor prímideál, ha a gyűrű egy prímeleme generálja.

Δ

Bizonyítás:

Legyen $\mathcal{J}_1 = (u_1)$ és $\mathcal{J}_2 = (u_2)$ az $\mathcal{R}$ főideálgyűrű két ideálja. Ekkor $I_1 \subseteq I_2$ akkor és csak akkor, ha u_2 osztója u_1-nek, $I_2 = R$ akkor és csak akkor, ha $u_2 = e$ (pontosabban szólva, ha u_2 egység), és $\mathcal{J}_1$ pontosan akkor maximális, ha $I_1 \neq R$, de minden olyan $\mathcal{J} \neq \mathcal{R}$ ideálra, amellyel $I_1 \subseteq I$, $I = I_1$. Most legyen I_1 legalább kételemű, ekkor $u_1 \neq 0$. Az előbbiek szerint I_1 akkor és csak akkor maximális, ha nincs más osztója, mint az egységek valamint a saját asszociáltjai, vagyis akkor és csak akkor, ha u_1 irreducibilis.

(a) akkor és csak akkor prímideál, ha $uv \in (a)$-ból, azaz abból, hogy a osztója a szorzatnak, következik, hogy legalább egyik tényező is eleme az ideálnak, vagyis osztója legalább az egyik tényezőnek,. De ez éppen azt jelenti, hogy a egy prímeleme a gyűrűnek.

□

Főideálgyűrűben a prímek és a felbonthatatlan elemek összessége megegyezik, amiből következik, hogy főideálgyűrű egy nem triviális ideálja szerinti maradékosztály-gyűrű vagy test, vagy nem nullosztómentes. Egy összetett elem által generált ideálja szerinti maradékosztály-gyűrű kommutatív, egységelemes és minden ideálja főideál, de nem főideálgyűrű, mert nem nullosztómentes. Most ilyen gyűrűket és ezek ideáljait vizsgáljuk.

Adott prímeket tartalmazó összetett elemek között a legegyszerűbbek azok, amelyek minden prímet csak egyszeres faktorként tartalmaznak, és ezek az adott prímekből álló szorzatok mindegyikének osztói, tehát az általuk generált ideál tartalmazza az összes olyan ideált, amelyeket az adott prímekből álló szorzatok generálnak. Érdemes ezért az ilyen ideálokkal és maradékosztály-gyűrűkkel foglalkozni.

15.27. Definíció

Gauss-gyűrű a eleme négyzetmentes, ha nem nulla, nem az egységelem, és minden felbonthatatlan faktora egyszeres.

Δ

A nullideál egyetlen eleme 0, és ez idempotens. Más ideálnak is lehet olyan eleme, amelynek a négyzete önmaga, de korábban láttuk, hogy legfeljebb egy lehet reguláris. Az alábbiakban egy $\mathcal{R}$ főideálgyűrű a eleme által generált ideálja szerinti maradékosztály-gyűrűt, azaz $\mathcal{R}/(a)$-t $\mathcal{R}_{(a)}$-val, a megfelelő halmazt $R_{(a)}$-val fogjuk jelölni.

15.28. Tétel

Ha az $\mathcal{R}$ főideálgyűrű a eleme négyzetmentes, akkor az $\mathcal{R}_{(a)}$ gyűrű minden nem nulla ideáljában van egy és csak egy, az ideált generáló idempotens elem, és ez egységelem az ideálban.

Δ

Bizonyítás:

$\mathcal{R}_{(a)}$ minden nem nulla ideálja az a egy osztója által generált ideál. Legyen az R egy b eleme a osztója, és legyen $c = \frac{a}{b}$, ekkor b és c relatív prímek, mivel a négyzetmentes. Ebből következően $\mathcal{R}$-ben $e = bu + cv$ az R valamilyen u és v elemével (e a szokásos módon az $\mathcal{R}$ egységeleme). $\overline{bu} = \bar{b}\bar{u}$, tehát $bu = \varepsilon$ $\mathcal{R}_{(a)}$-beli képe eleme a maradékosztály-gyűrű $\bar{b}$ által generált ideáljának. Átrendezve $\varepsilon = bu = e - cv$, majd ezzel $\varepsilon^2 = bu(e - cv) = bu - (bc)(uv) = \varepsilon - aw$, tehát $\bar{\varepsilon}^2 = \bar{\varepsilon}$, $\bar{\varepsilon}$ idempotens $\mathcal{R}_{(a)}$-ban. Legyen most $\bar{s}$ a $(\bar{b})$ ideál tetszőleges eleme, és így $s \in (b)$ is teljesül. Ekkor s a b többszöröse,

tehát $s = bt$, és $\varepsilon s = es - cvs = s - (bc)(tv) = s - ar$, vagyis $\bar{\varepsilon}\bar{s} = \bar{s}$, $\bar{\varepsilon}$ neutrális elem a $(\bar{b})$ ideál mint gyűrű multiplikatív félcsoportjában, tehát van reguláris idempotens elem, és ez egyértelmű, hiszen egységelem egyértelműen meghatározott.

Egységelem által generált ideál a teljes gyűrű, vagyis most maga az ideál. Legyen $\bar{u}$ az ideál egy olyan idempotens eleme, amely szintén generálja az ideált. Ekkor az ideál bármely $\bar{w}$ elemére $\bar{w} = \bar{u}\bar{v}$ a maradékosztály-gyűrű egy $\bar{v}$ elemével. Innen, alkalmazva, hogy $\bar{u}$ idempotens, $\bar{u}\bar{w} = \bar{u}^2\bar{v} = \bar{u}\bar{v} = \bar{w}$, $\bar{u}$ tehát neutrális eleme az ideálbeli szorzásnak. De $\bar{\varepsilon}$ is egységeleme ennek a műveletnek, így $\bar{u} = \bar{\varepsilon}$.

□

15.29. Definíció

Főideálgyűrű egy négyzetmentes eleme által generált ideálja szerinti maradékosztály-gyűrű egy nem nulla ideáljának reguláris idempotens eleme az ideál **generáló idempotens**e, röviden **idempotens**e.

Δ

$\mathcal{R}_{(a)}$ mint önmaga ideálja a gyűrű egységeleme, az e által generált ideál képe. Ekkor $c = a$, és $e = ee + c \cdot 0$, azaz $\mathcal{R}_{(a)}$ idempotense az e $\mathcal{R}_{(a)}$-beli képe.

15.30. Tétel

Legyen a az $\mathcal{R}$ főideálgyűrű négyzetmentes eleme, $b \in R$ osztója a-nak és $u \in R$. Ekkor $\varepsilon = bu$ pontosan akkor idempotense a (b) $\mathcal{R}_{(a)}$-beli képének, ha $p|e - \varepsilon$ a $c = \frac{a}{b}$ minden p prímosztójára.

Δ

Bizonyítás:

Ha ε idempotense a (b) $\mathcal{R}_{(a)}$-beli képének, akkor $e = bu + cv$, és így $p|cv = e - bu = e - \varepsilon$. Fordítva, legyen a c minden prímosztója osztója $e - \varepsilon$-nak. Négyzetmentes a minden prímosztója egyszeres, és így legfeljebb egyszeres osztója c-nek. Ebből következik, hogy c páronként különböző prímosztók szorzata, és ha minden prímosztója osztja $e - \varepsilon$-t, akkor maga c is osztója ennek a különbségnek, vagyis $e - \varepsilon = cv$, ahonnan $e = \varepsilon + cv = bu + cv$, tehát ε idempotense (b) $\mathcal{R}_{(a)}$-beli képének.

□

15.31. Megjegyzés

Az előbbi tétel másként fogalmazva azt jelenti, hogy az R egy ε eleme akkor és csak akkor idempotense az $\mathcal{R}$ főideálgyűrű a négyzetmentes eleme egy b osztója által generált ideál $\mathcal{R}_{(a)}$-beli képének, ha a b prímosztói ε-nak, az a többi prímosztója $e - \varepsilon$-nak osztója. A mostani feltétel ugyanis ekvivalens azzal, hogy ε $\mathcal{R}$-beli többszöröse b-nek és az $e - \varepsilon$ különbség $c = \frac{a}{b}$-nek.

Δ

15.32. Tétel

Ha a az $\mathcal{R}$ főideálgyűrű eleme, ε az $\mathcal{R}$-beli $\mathcal{I}$ ideál $\mathcal{R}_{(a)}$-beli képének idempotense, akkor $\mathcal{I} = (b)$, ahol $b = (\varepsilon, a)$.

Δ

Bizonyítás:

Gyűrű egysége, tehát például egységeleme által generált ideál maga a gyűrű, így az $\bar{\varepsilon}$ $\mathcal{R}_{(a)}$-beli többszöröseiből álló ideál az a egy b osztójának $\bar{b}$ képe által generált ideál. Ekkor $\mathcal{R}$-ben az (ε) és a (b) $\mathcal{R}_{(a)}$-beli képének teljes inverze azonos, és ez a közös ideál az (ε, a) és (b, a) által generált ideál, ahol most (u, v) az u és v legnagyobb közös osztója. De $b|a$, így $(b, a) = b$, tehát $b = (\varepsilon, a)$.

□

Főideálok metszete a generáló elemek legkisebb közös többszöröse által generált ideál, míg az összegüket a legnagyobb közös osztó generálja. Nézzük a metszetet és összeget az idempotensekkel.

15.33. Tétel

Ha a az $\mathcal{R}$ főideálgyűrű négyzetmentes eleme, és ε_1 és ε_2 az $\mathcal{R}_{(a)}$ két ideáljának idempotense, akkor a metszet idempotense $\varepsilon_1\varepsilon_2$, míg az összegé $\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2$.

Δ

Bizonyítás:

$\overline{\varepsilon_1\varepsilon_2} = \overline{\varepsilon_1}\,\overline{\varepsilon_2}$ mindkét ideálnak eleme, hiszen ideál zárt a gyűrű bármely elemével való szorzásra, így a metszetüknek is eleme. Ha $\bar{u}$ a metszet tetszőleges eleme, akkor $(\overline{\varepsilon_1}\,\overline{\varepsilon_2})\bar{u} = \overline{\varepsilon_1}(\overline{\varepsilon_2}\bar{u}) = \overline{\varepsilon_1}\bar{u} = \bar{u}$, tehát $\overline{\varepsilon_1\varepsilon_2}$ neutrális elem az ideálban, következésképpen reguláris és idempotens.

$\overline{\varepsilon_1}\,\overline{\varepsilon_2}$ eleme a metszetnek, és így például $\overline{\varepsilon_1 - \varepsilon_1\varepsilon_2}$ az egyik ideálnak, ezért $\overline{\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2}$ benne van a két ideál összegében. Még azt kell megmutatni, hogy ez az elem reguláris és idempotens, amihez ismét elég megmutatni, hogy semleges eleme az összegnek.

Legyen $\bar{u}$ az összeg egy eleme. Ekkor $\bar{u} = \bar{u}_1 + \bar{u}_2$ a két ideálból vett egy-egy elemmel, és

$$\begin{aligned}\overline{\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2}\bar{u} &= \overline{\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2}(\bar{u}_1 + \bar{u}_2) = (\overline{\varepsilon_1} + \overline{\varepsilon_2} - \overline{\varepsilon_1}\,\overline{\varepsilon_2})(\bar{u}_1 + \bar{u}_2)\\ &= \overline{\varepsilon_1}\bar{u}_1 + \overline{\varepsilon_1}\bar{u}_2 + \overline{\varepsilon_2}\bar{u}_1 + \overline{\varepsilon_2}\bar{u}_2 - \overline{\varepsilon_1}\,\overline{\varepsilon_2}\bar{u}_1 - \overline{\varepsilon_1}\,\overline{\varepsilon_2}\bar{u}_2\\ &= \bar{u}_1 + \overline{\varepsilon_1}\bar{u}_2 + \overline{\varepsilon_2}\bar{u}_1 + \bar{u}_2 - \overline{\varepsilon_2}\bar{u}_1 - \overline{\varepsilon_1}\bar{u}_2 = \bar{u}_1 + \bar{u}_2 = \bar{u},\end{aligned}$$

ami azt jelenti, hogy $\overline{\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2}$ egységeleme az ideál mint gyűrű multiplikatív félcsoportjának.

□

Az előbbi tételből indukcióval könnyen kapjuk, hogy a maradékosztály-gyűrű ideáljainak metszetében az idempotensek szorzata, míg az összegükben $\sum_{\emptyset\neq K\subseteq L}(-1)^{|K|-1}\prod_{i\in K}\varepsilon_i$ a generáló idempotens, ahol L az adott ideálok indexeiből álló halmaz.

Ha a az $\mathcal{R}$ főideálgyűrű összetett, négyzetmentes eleme, és $a = \prod_{i=0}^{m-1} a_i$ az a irrdeducibilis elemekre való felbontása, akkor az a_i-k páronként különbözőek, és az $\mathcal{R}_{(a)}$ gyűrű egy ideálja akkor és csak akkor maximális, ha valamely i-re az (a_i) képe, míg pontosan akkor minimális, ha $\left(\frac{a}{a_i}\right)$-nek a maradékosztály-gyűrűbeli képe.

15.34. Tétel

Ha a az $\mathcal{R}$ főideálgyűrű összetett, négyzetmentes eleme, $a = \prod_{i=0}^{m-1} a_i$, ahol a szorzat tényezői a gyűrű felbonthatatlan elemei, $K \subseteq \{i \in \mathbb{N} | i < m\} = \mathbb{N}_m$, $L = \mathbb{N}_m \backslash K$, $b = \prod_{i\in L} a_i$ és az $\mathbb{N}_m$ részhalmazainak egy $\{U_\delta | \delta \in \Delta\}$ rendszerének metszete az üres halmaz, akkor

1. $\sum_{i\in K}\left(\overline{\frac{a}{a_i}}\right) = \cap_{i\in L}(\bar{a}_i) = (\prod_{i\in L}\bar{a}_i) = (\bar{b})$;
2. $\cap_{\delta\in\Delta}\sum_{i\in U_\delta}\left(\overline{\frac{a}{a_i}}\right) = (\bar{0})$;
3. $\bar{u} \in (\bar{b})$ egy- és csak egyféleképpen írható $\left(\overline{\frac{a}{a_i}}\right)$-beli elemek összegeként.

Δ

Bizonyítás:

Láttuk, hogy homomorfizmusnál ideálok összegének képe a képek összege, és ez a metszetre is igaz, ha a metszet minden tagja tartalmazza a homomorfizmus magját.

a négyzetmentes, tehát $\frac{a}{a_i}$ nem osztható a_i-vel, de osztható minden $i \neq j$-re a_j-vel. Ebből következik, hogy ha $W \subseteq \mathbb{N}_m$, akkor az $\left\{\frac{a}{a_i}\middle| i \in W\right\}$ halmaz minden eleme osztható minden olyan a_j-vel, ahol $j \notin W$, és pontosan egy eleme a halmaznak nem osztható a_i-vel, ha i eleme W-nek. Ekkor viszont $\left\{\frac{a}{a_i}\middle| i \in W\right\}$ legnagyobb közös osztója $d_w = \prod_{i\in\mathbb{N}_m\setminus W} a_i$.

1. Ha d_K az $\left\{\frac{a}{a_i}\middle| i \in K\right\}$ halmaz legnagyobb közös osztója, akkor $d_K = \prod_{i\in\mathbb{N}_m\setminus K} a_i = \prod_{i\in L} a_i$, és a jobb oldalon álló szorzat az $\{a_i | i \in L\}$ halmaz legkisebb közös többszöröse. Ekkor $\sum_{i\in K}\left(\frac{\bar{a}}{a_\iota}\right) = \left(\bar{d}_K\right) = \left(\overline{\prod_{\iota\in L} a_\iota}\right) = \left(\prod_{i\in L} \bar{a}_i\right) = \bigcap_{i\in L}(\bar{a}_i)$;
2. $\bigcap_{\delta\in\Delta}\sum_{i\in U_\delta}\left(\frac{\bar{a}}{a_\iota}\right) = \bigcap_{\delta\in\Delta}\bigcap_{i\in\mathbb{N}_m\setminus U_\delta}(\bar{a}_i) = \left(\overline{\prod_{\delta\in\Delta}\prod_{\iota\in\mathbb{N}_m\setminus U_\delta} a_\iota}\right) = \left(\overline{\prod_{\iota\in\bigcup_{\delta\in\Delta}\mathbb{N}_m\setminus U_\delta} a_\iota}\right) = \left(\overline{\prod_{\iota\in\overline{\bigcap_{\delta\in\Delta} U_\delta}} a_\iota}\right) = \left(\overline{\prod_{\iota\in\bar{\emptyset}} a_\iota}\right) = \left(\overline{\prod_{\iota\in\mathbb{N}_m} a_\iota}\right) = (\bar{a}) = (\bar{0})$;
3. az előző pont alapján minden $i \in \mathbb{N}_m$-re $\left(\frac{\bar{a}}{a_\iota}\right) \cap \sum_{j\in K\setminus i}\left(\frac{\bar{a}}{a_\iota}\right) = (\bar{0})$.

□

A 2. pont alapján különböző minimális ideálok metszete a nullideál, és ha $\bar{u}$ a maradékosztály-gyűrű eleme, akkor ez az elem egyértelműen írható a minimális ideálokból vett elemek összegeként.

15.35. Definíció

Az $\mathcal{R}$ főideálgyűrű egy összetett, négyzetmentes a eleme által generált ideálja szerinti maradékosztály-gyűrű egy minimális ideáljának generáló idempotense az $\mathcal{R}_{(a)}$ **primitív idempotens**e.

Δ

15.36. Tétel

Ha $a = \prod_{i=0}^{m-1} a_i$ az $\mathcal{R}$ főideálgyűrű összetett, négyzetmentes eleme, és $\varepsilon^{(i)}$ az $\mathcal{R}_{(a)}$-ban az $\left(\frac{a}{a_i}\right)$-hez tartozó minimális ideál idempotense, akkor

1. különböző index esetén $\overline{\varepsilon^{(\iota)}} \cdot \overline{\varepsilon^{(\jmath)}}$ az $\mathcal{R}_{(a)}$ nulleleme;
2. $\sum_{i=0}^{m-1} \overline{\varepsilon^{(\iota)}} = \bar{e}$;
3. minimális ideálban a generáló idempotensen kívül csak a nullelem idempotens;

Δ

Bizonyítás:

1. $\overline{\varepsilon^{(\iota)}} \cdot \overline{\varepsilon^{(\jmath)}}$ a két ideál metszetének eleme. Ha $i \neq j$, akkor a két ideál metszete az ideálok valódi része, és ez csak a nullideál lehet, hiszen a két ideál minimális.
2. Az $\left(\frac{a}{a_i}\right)$-k legnagyobb közös osztója az $\mathcal{R}$ egységeleme, így $\mathcal{R}_{(a)}$ a minimális ideálok összege, és az idempotense $\bar{e}$. Ekkor $\bar{e}$ az ideálok idempotenseinek, valamint idempotensek szorzatainak bizonyos előjelekkel vett összege. De az előző pont szerint a legalább kéttényezős szorzatok mindegyike 0, következésképpen $\sum_{i=0}^{m-1} \overline{\varepsilon^{(\iota)}} = \bar{e}$.
3. Legyen ε idempotens az $\overline{\varepsilon^{(\iota)}}$-t tartalmazó ideálban. ε $\mathcal{R}_{(a)}$-beli többszörösei ideált alkotnak $\mathcal{R}_{(a)}$-ban, amely ideál része a minimális ideálnak, tehát meg is egyezik vele. Ám ideált generáló idempotens csak egy van, amiből következik, hogy minimális ideálban csak triviális idempotensek vannak.

□

A minimális ideálok további fontos tulajdonságát írja le az alábbi tétel.

15.37. Tétel

Ha $\mathcal{R}$ főideálgyűrű, $a \in R$ összetett és négyzetmentes, akkor $\mathcal{R}_{(a)}$-ban minimális ideál test.

Δ

Bizonyítás:

Egy legalább két elemet tartalmazó kommutatív gyűrű akkor és csak akkor test, ha minden nem nulla elemének van inverze. Mivel a összetett, ezért az (a) szerinti maradékosztály-gyűrűben van nem triviális ideál, következésképpen a minimális ideálnak is van legalább két eleme. Legyen $\bar{u} \neq \bar{0}$ az $\mathcal{M}$ minimális ideál egy eleme, és legyen $\mathcal{M}$ idempotense ε. Mivel $\bar{u}$ nem nulla, és az őt tartalmazó ideál minimális, ezért $(\bar{u}) = M$, tehát $\bar{\varepsilon}$ is $\bar{u}$ egy többszöröse, $\bar{\varepsilon} = \bar{u}\bar{v}$, ahol $\bar{v}$ az $\mathcal{R}/(a)$ eleme. Most $\bar{w} = \bar{v}\bar{\varepsilon}$ mint az $\mathcal{M}$ ideál egy elemének többszöröse maga is eleme M-nek, és $\bar{\varepsilon} = \bar{\varepsilon}^2 = \bar{u}\bar{v}\bar{\varepsilon} = \bar{u}\bar{w}$, ami éppen azt jelenti, hogy $\bar{u}$-nak van inverze $\mathcal{M}$-ben.

□

A fentebbiekben főleg főideálgyűrű bizonyos tulajdonságairól írtunk. Gyűrűk másik fontos típusa az euklideszi gyűrű. A tárgyalt tulajdonságok az ilyen gyűrűkben is teljesülnek az alábbi tétel alapján.

15.38. Tétel

Euklideszi gyűrű főideálgyűrű.

Δ

Bizonyítás:

Legyen $\mathcal{R}$ euklideszi gyűrű, és $\mathcal{J}$ az $\mathcal{R}$ legalább két elemet tartalmazó ideálja (a csak a nullelemet tartalmazó ideál nyilván főideál). Mivel az ideál tartalmaz nem nulla elemet, az ideálbeli elemek euklideszi normáinak halmaza a nemnegatív egész számok halmazának nem üres részhalmaza, így van benne egyértelműen meghatározott legkisebb elem, mondjuk s, és az ideálnak van s-normájú eleme, például u. Ha most v az ideál egy tetszőleges eleme, akkor v-t maradékosan osztva u-val, $v = qu + r$, ahol vagy r a gyűrű nulleleme, vagy r normája kisebb, mint u normája. De ez utóbbi nem lehetséges, ugyanis u és v eleme az ideálnak, ekkor qu és $r = v - qu$ is benne van az ideálban, és $\mathcal{J}$-ben minden nem nulla elem normája legalább akkora, mint u normája, hiszen u egy minimális normájú eleme az ideálnak. Ebből következően $r = 0$, tehát $v = qu$, vagyis az ideál minden eleme az u többszöröse, és kommutatív egységelemes gyűrűben – márpedig euklideszi gyűrű ilyen – egy elem többszörösei főideált alkotnak.

□

Test fölötti polinomgyűrű euklideszi, tehát főideálgyűrű. és ekkor nem triviális ideál szerinti maradékosztály-gyűrű (egymást kizáró módon) test vagy nem nullosztómentes. $x^n - e$ akkor és csak akkor felbonthatatlan, ha $n = 1$, így, ha $\mathcal{K}$ test és $1 < n \in \mathbb{N}$, akkor $\mathcal{K}[x]/(x^n - e)$ nem nullosztómentes.

Visszatérünk a ciklikus kódokhoz. Legyen q egy pozitív egész kitevős prímhatvány, és $1 < n$ a q-hoz relatív prím egész. A fejezet elején megmutattuk, hogy ekkor az $\mathbb{F}_q$ fölötti, n-szóhosszúságú ciklikus kódok az $x^n - e \in \mathbb{F}_q[x]$ által generált ideál szerinti maradékosztály-gyűrű ideáljai, ahol ezek az ideálok az $x^n - e$ $\mathbb{F}_q[x]$-beli g főpolinom-osztóihoz tartozó ideálok képei. $\mathbb{F}_q[x]$ főideálgyűrű. Mivel n nagyobb, mint 1 és relatív prím n-hez, ezért $x^n - e$ a polinomgyűrű felbontható, négyzetmentes eleme, alkalmazhatjuk a fentebb kifejtetteket. A rövidség kedvéért $\mathcal{R}[x]/(x^n - e)$ helyett $\mathcal{R}^{(n)}$-et írunk.

Legyen $x^n - e = \prod_{i=0}^{m-1} g_i$ az irreducibilis főpolinomokra való felbontás, $g^{(i)} = \frac{x^n - e}{g_i} = h_i$ és $G \subseteq \{g \in \mathbb{F}_q[x] | g | x^n - e \text{ főpolinom}\}$. Az alábbiakban C egy $[n,k]_q$-paraméterű ciklikus kódot, míg C_g a $g | x^n - e$ főpolinom által generált kódot jelöli.

1. $\bigcap_{g \in G} C_g$ és $\sum_{g \in G} C_g$ $[n,k]_q$-paraméterű kód, ahol az előbbi generátoreleme a g-k legkisebb közös többszöröse, az utóbbié a legnagyobb közös osztó (ciklikus kódoknál láttuk két halmaz esetére);
2. $\bigcap_{g \in G} C_g$ idempotense $\prod_{g \in G} \varepsilon_g$ és $\sum_{g \in G} C_g$ idempotense $\sum_{\emptyset \neq H \subseteq G} (-1)^{|H|-1} \prod_{g \in H} \varepsilon_g$;

3. ha $K \subseteq \{0,\cdots,m-1\} = T$ és $g = \prod_{i\in K} g_i$, akkor $\bigcap_{i\in K} C_{g_i} = C_g = \sum_{i\in T\setminus K} C_{g^{(i)}}$, és C_g idempotense $\prod_{i\in K} \varepsilon_{g_i} = \varepsilon_g = \sum_{\emptyset\neq L\subseteq K}(-1)^{|L|-1}\prod_{i\in L}\varepsilon_{g^{(i)}}$;
4. az $f \in \mathbb{F}_q[x]$ által generált ciklikus kód pontosan akkor azonos C_g-vel, ha $(f, x^n - e) = g$ (a nullától különböző legnagyobb közös osztónál mindig a főpolinomot tekintjük);
5. C_g-hez van egy és csak egy reguláris idempotens elem: ha $e = ug + v\frac{(x^n-e)}{g}$, akkor $\varepsilon_g = ug$, és a megfelelő kódszó $\varepsilon_g \bmod (x^n - e)$, amely a kód neutrális eleme;
6. az előző két pont alapján $g = (\varepsilon_g, x^n - e)$;
7. a primitív idempotensek az $\varepsilon_{g^{(i)}}$-k;
8. ha $i \neq j$, akkor $g^{(i)}g^{(j)} = u\cdot(x^n - e)$ egy nem nulla u polinommal;
9. $C_{g^{(i)}}$-ben 0 és $\varepsilon_{g^{(i)}}$ idempotens, és más idempotens nincs;
10. $C_{g^{(i)}}$ test.

C_{g_i} maximális, $C_{g^{(i)}}$ minimális kód, és azt a ciklikus kódoknál láttuk, hogy minimális kód test.

Kód idempotensével kapcsolatban külön kiemeljük az n-edik egységgyökökkel való kapcsolatát.

15.39. Tétel

Legyen $(n, q) = 1$, ε a q-elemű test fölötti, a g polinom által generált n-szóhosszúságú ciklikus kód idempotense és α primitív n-edik egységgyök $\mathbb{F}_q$ fölött. Ekkor $\hat{\varepsilon}(\alpha^i) = 0$, ha α^i gyöke g-nek, különben $\hat{\varepsilon}(\alpha^i) = e$.

Δ

Bizonyítás:
$x^n - e$ prímtényezői az $x - \alpha^i$ polinomok, és test fölötti polinomok esetén $x - u$ akkor és csak akkor osztója az f polinomnak, ha $\hat{f}(u) = 0$. Ezek után az állítás már egyenes következménye az 15.30. Tételnek és 15.31. Megjegyzésnek.

□

15.40. Tétel

Ha $\varepsilon = \sum_{i=0}^{n-1}\varepsilon_i x^i$ a g polinom által generált $[n,k]_q$-paraméterű C ciklikus kód idempotense, akkor a $\mathbf{G} = \begin{pmatrix} \vec{\boldsymbol{\varepsilon}}_0 \\ \vdots \\ \vec{\boldsymbol{\varepsilon}}_i \\ \vdots \\ \vec{\boldsymbol{\varepsilon}}_{k-1} \end{pmatrix}$ mátrix sorai a kód egy generátorrendszere, ahol $\boldsymbol{\varepsilon}$ az ε polinomhoz tartozó kódszó, és $k > i \in \mathbb{N}$-re $\vec{\boldsymbol{\varepsilon}}_i$ az $\boldsymbol{\varepsilon}$ i pozícióval való ciklikus jobbra léptetésével kapott szó.

Δ

Bizonyítás:
$\boldsymbol{\varepsilon}$ kódszó, és mivel a kód ciklikus, ezért minden ciklikus eltoltja, tehát $k > i \in \mathbb{N}$-re $\vec{\boldsymbol{\varepsilon}}_i$ is kódszó (ahol $\vec{\boldsymbol{\varepsilon}}_0 = \boldsymbol{\varepsilon}$), így elegendő belátni, hogy ezek a kódszavak lineárisan függetlenek, vagyis, ha a egy legfeljebb $k-1$-edfokú polinom, akkor $a\varepsilon \bmod (x^n - e) = 0$ akkor és csak akkor, ha $a = 0$. Legyen g a kód generátorpolinomja. ε egységelem a kódban, vagyis bármely c kódszóra $c\varepsilon \bmod (x^n - e) = c$, ezért $a\varepsilon \bmod (x^n - e)$ akkor és csak akkor lesz a nullpolinom, ha $0 = 0g = (a\varepsilon \bmod (x^n - e))g = a(\varepsilon g) \bmod (x^n - e) = ag$, és ez pontosan akkor teljesül, ha $a = 0$.

□

15.41. Kiegészítés

Ha $\varepsilon = \sum_{i=0}^{n-1} \varepsilon_i x^i$ a g polinom által generált $[n,k]_q$-paraméterű C ciklikus kód idempotense, akkor a $\mathbf{G}' = \begin{pmatrix} \boldsymbol{\varepsilon}_{\overrightarrow{0}} \\ \vdots \\ \boldsymbol{\varepsilon}_{\overrightarrow{i}} \\ \vdots \\ \boldsymbol{\varepsilon}_{\overrightarrow{n-1}} \end{pmatrix}$ mátrix is kód egy generátormátrixa.

Δ

Bizonyítás:
A mátrix sorai most is elemei a kódnak, így bármely lineáris kombinációjuk az adott kód egy kódszava. Az előbbi tétel szerint a mátrix első k sora bázisa a kódnak, és bázis bármely bővítése generátorrendszere az adott lineáris térnek.

□

15.42. Megjegyzés

Vannak olyan kódok, és majd mi is foglalkozunk ilyen kóddal, ahol a kód generátormátrixaként $\mathbf{G}'$-t adják meg.

Δ

Legyen S egy legalább két elemet tartalmazó szimbólumhalmaz, $n \in \mathbb{N}^+$ és $C \subseteq S^n$ egy (n, M, d) paraméterű, S fölötti kód. Ekkor az S^n-beli $\mathbf{u} = u_0 \cdots u_i \cdots u_{n-1}$ elemekre alkalmazott $\mathbf{u} \mapsto \boldsymbol{\pi}\mathbf{u}$ szabály, ahol $\boldsymbol{\pi}\mathbf{u} = u_{\pi(o)} \cdots u_{\pi(i)} \cdots u_{\pi(n-1)}$ az $\mathbb{N}_n = \{i \in \mathbb{N} | n > i\}$ halmaz egy π permutációjával, az S^n egy önmagába való távolságtartó leképezése (és így egy önmagára való bijekciója). Ez azt is jelenti, hogy a $\boldsymbol{\pi}C = \{\boldsymbol{\pi}\mathbf{c} | \mathbf{c} \in C\}$ halmaz a C-vel ekvivalens kód. Az n-hez relatív prím r egésszel a $\pi^{(r)}: i \mapsto ri \bmod n$ megfeleltetés az $\mathbb{N}_n$ permutációja. Ha r, r_1 és r_2 relatív prím n-hez, és s az r modulo n inverze, akkor $r_1 r_2$ és s, valamint 1 is relatív prím n-hez. $\pi^{(r_2)}\pi^{(r_1)} = \pi^{(r_2 r_1)} = \pi^{(r_2 r_1 \bmod n)} = \pi^{(r_1 r_2 \bmod n)} = \pi^{(r_1 r_2)} = \pi^{(r_1)}\pi^{(r_2)}$, $\pi^{(1)} = \varepsilon$ és $\pi^{(s)}\pi^{(r)} = \varepsilon = \pi^{(r)}\pi^{(s)}$ (ε az identikus leképezés), tehát az n-hez relatív prím, n-nél kisebb, nemnegatív egész r-rekkel a $\pi^{(r)}$ permutációk az n-edfokú szimmetrikus csoport egy részcsoportját képezik. A továbbiakban $\boldsymbol{\pi}^{(r)}\mathbf{u}$-t $\mathbf{u}^{(r)}$ és $\boldsymbol{\pi}^{(r)}C$-t $C^{(r)}$ jelöli. Az előbbi eredménnyel $\left(\mathbf{u}^{(s)}\right)^{(r)} = \mathbf{u}^{(rs)} = \mathbf{u} = \mathbf{u}^{(sr)} = \left(\mathbf{u}^{(r)}\right)^{(s)}$, és hasonlóan, $\left(C^{(s)}\right)^{(r)} = C = \left(C^{(r)}\right)^{(s)}$.

Mivel $\mathbf{u}$ és $\mathbf{u}^{(r)}$ komponensei – a többszörösségükkel együtt – azonosak, ezért a két szó súlya is azonos. Ha S egy additív Abel-csoport alaphalmaza, akkor még az is igaz, hogy az egymásnak megfelelő szavak komponenseinek összege is azonos.

$\big((ri \bmod n) + 1\big) \bmod n = \big((ri \bmod n) + (rs \bmod n)\big) \bmod n = r\big((i+s) \bmod n\big) \bmod n$, és ebből következik, hogy ha a C-beli $\mathbf{c}$-vel $\mathbf{c}_{\rightarrow} = c_{n-1}c_0 \cdots c_{n-2}$ is eleme a kódnak, akkor $\left(\boldsymbol{\pi}^{(r)}\mathbf{c}\right)_{\rightarrow} = \boldsymbol{\pi}^{(r)}\mathbf{c}_{\overrightarrow{s}} \in \boldsymbol{\pi}^{(r)}C$. Ennek alapján, ha $S = \mathbb{F}_q$, és C ciklikus kód, akkor a vele ekvivalens $C^{(r)}$ kód is ciklikus (mert a komponensek permutációja lineáris kódot lineáris kódba képez), jóllehet, ciklikus kóddal ekvivalens kód nem mindig ciklikus (példaként tekintsük a Hamming-kódokat).

Most tekintsük a ciklikus kódokhoz tartozó polinomokat. Ha $\sum_{i=0}^{n-1} c_i x^i = c \in \mathbb{F}_q[x]$, és r az n-hez relatív prím egész szám, akkor

$$c^{(r)} = \sum_{i=0}^{n-1} c_{ri \bmod n} x^i = \sum_{i=0}^{n-1} c_{r(si \bmod n) \bmod n} x^{si \bmod n}$$
$$= \sum_{i=0}^{n-1} c_{(rs)i \bmod n} x^{si \bmod n} = \sum_{i=0}^{n-1} c_i x^{si \bmod n},$$

ahol s ismét az r modulo n inverze. Láthatóan $c^{(r)}$ is az $\mathbb{F}_q$ fölötti, legfeljebb $n-1$-edfokú polinom. Ha γ egy $\mathbb{F}_q$ feletti n-edik egységgyök, akkor $\widehat{c^{(r)}}(\gamma) = \sum_{i=0}^{n-1} c_i \gamma^{si \bmod n} = \sum_{i=0}^{n-1} c_i (\gamma^s)^i = \hat{c}(\gamma^s)$, így γ pontosan akkor gyöke $c^{(r)}$-nek, amikor γ^s a c gyöke. Ha például α egy primitív n-edik egységgyök a q-elemű test fölött, és $\gamma = (\alpha^r)^k$ egy k egész számmal, akkor $\gamma^s = \alpha^k$, vagyis α^k akkor és csak akkor gyöke a c polinomnak, amikor $(\alpha^r)^k$ gyöke $c^{(r)}$-nek. Ám α^r is primitív n-edik egységgyök a q-elemű test fölött, és a $\beta = \alpha^r$ jelöléssel $\widehat{c^{(r)}}(\beta^k) = \hat{c}(\alpha^k)$, $c^{(r)}$-nek a β azon és csak azon kitevős hatványai gyökei, amely kitevőhöz tartozó α-hatványok annullálják a c polinomot.

Ha g az $\mathbb{F}_q$ fölötti n-szóhosszúságú C ciklikus kód generátor-polinomja, akkor g minden gyöke $\mathbb{F}_q$ fölötti n-edik egységgyök. Legyen egy adott, $\mathbb{F}_q$ fölötti α primitív n-edik egységgyökkel a g gyökei kitevőinek halmaza K. g a C minden c elemének osztója, tehát $\{\alpha^k | k \in K\}$ minden eleme gyöke mindegyik kódpolinomnak. De ebből következik, hogy ha $c^{(r)} \in C^{(r)}$, akkor $c^{(r)}$-nek a K minden k elemével gyöke α^{rk}. Ez fordítva is igaz. Legyen $f \in \mathbb{F}_q[x]$ egy legfeljebb $n-1$-edfokú polinom, amelynek minden előbbi α^{rk} gyöke. Ekkor $f^{(s)}$ egy olyan, $\mathbb{F}_q$ fölötti, legfeljebb $n-1$-edfokú polinom, amelynek a g minden gyöke gyöke, tehát $f^{(s)} \in C$. Most $f = \left(f^{(s)}\right)^{(r)}$, és így $f \in C^{(r)}$. Összefoglalva, $C^{(r)}$ pontosan azon polinomok összessége, amelyeknek g valamennyi gyökének r-edik hatványa gyöke.

Legyen $g_{(r)} = \sum_{k \in K}(x - \alpha^{rk})$. A fenti eredmény alapján $g_{(r)}$ eleme $C^{(r)}$-nek, és osztója a $C^{(r)}$-hez tartozó valamennyi polinomnak, következésképpen $g_{(r)}$ a $C^{(r)}$ ciklikus kód generátorpolinomja.

$g_{(r)}$ gyökei a g gyökei r-edik hatványai, azaz $g^{(r)}$ azon gyökei, amelyek $\mathbb{F}_q$ fölötti n-edik egységgyökök. De ekkor $g_{(r)}$ éppen a $g^{(r)}$ és $x^n - e$ legnagyobb közös osztója.

A $c^{(r)}$ polinomot más alakban is meg tudjuk adni. Legyen u nemnegatív és v pozitív egész szám és $u = lv + t$, ahol l és t nemnegatív egész szám úgy, hogy $v > t$. Ekkor $x^u = x^{lv+t} = x^{lv+t} - x^t + x^t = x^t\left((x^v)^l - e^l\right) + x^t$. $(x^v)^l - e^l$ osztható $x^v - e$-vel, így $x^u \bmod (x^v - e) = x^t = x^{u \bmod v}$. Ezt alkalmazva

$$c^{(r)} = \sum_{i=0}^{n-1} c_i x^{si \bmod n} = \sum_{i=0}^{n-1} c_i x^{si} \bmod (x^n - e)$$
$$= \sum_{i=0}^{n-1} c_i (x^s)^i \bmod (x^n - e) = (c \circ x^s) \bmod (x^n - e).$$

A fentiekben bizonyítottuk a következő tételt.

15.43. Tétel

Legyen g generátor-polinomja egy $[n, k]_q$-paraméterű C ciklikus kódnak, és legyen r az n-hez relatív prím pozitív egész szám. Ekkor a $g_{(r)} = (g \circ x^s, x^n - e)$ polinom által generált $C^{(r)}$ ciklikus kód az előbbivel ekvivalens kód, ahol a C-beli $c = \sum_{i=0}^{n-1} c_i x^i$ kódszónak megfelelő $C^{(r)}$-beli kódszót a $c^{(r)} = \sum_{i=0}^{n-1} c_{ri \bmod n} x^i = (c \circ x^s) \bmod (x^n - e)$ polinom adja. Itt s az r modulo n inverze.

Δ

A következő részben a fenti eredmények egy jó részét konkrét kódosztályokra fogjuk alkalmazni.

16. Maradékkód

Az alább definiálandó kódhoz szükségünk lesz a következő eredményre.

16.1. Tétel

Legyen n és m pozitív egész szám, és $m > i \in \mathbb{N}$-re $C^{(i)}$ az $\mathbb{F}_q$ test fölötti, n-szóhosszúságú ciklikus kód. Ha $c^{(i)}$ a $C^{(i)}$ egy $\mathbf{c}^{(i)}$ eleméhez tartozó polinom, akkor a $c = \left(\prod_{i=0}^{m-1} c^{(i)}\right) \bmod (x^n - e)$-hez tartozó $\mathbf{c}$ szó $w(\mathbf{c})$ súlya legfeljebb $\prod_{i=0}^{m-1} w\left(\mathbf{c}^{(i)}\right)$.

Δ

Bizonyítás:
$\prod_{i=0}^{m-1} c^{(i)} \bmod (x^n - e) = \left(\prod_{i=0}^{m-2} c^{(i)} \bmod (x^n - e)\right) c^{(m-1)} \bmod (x^n - e)$, ezért elegendő $m = 2$ esetére bizonyítani az állítást, innen indukcióval kapjuk minden más, pozitív egész m-re az eredményt (az $m = 1$ eset nyilvánvaló). $c^{(1)}c^{(2)} \bmod (x^n - e)$ a $c_i^{(2)}\left(x^i c^{(1)} \bmod (x^n - e)\right)$ kódszavak összege, azaz $\sum_{c_i^{(2)} \neq 0} c_i^{(2)}\left(x^i c^{(1)} \bmod (x^n - e)\right)$. Ez az összeg $w\left(\mathbf{c}^{(2)}\right)$ darab nemnulla szó összege, ahol mindegyik tag súlya $w\left(\mathbf{c}^{(1)}\right)$. De a súlyokra teljesül a háromszög-egyenlőtlenség, így az összeg súlya nem nagyobb a tagok súlyai összegénél, a jelen esetben tehát $w\left(\mathbf{c}^{(1)}\right)w\left(\mathbf{c}^{(2)}\right)$-nél.

□

Felidézzük, hogy a pozitív egész n-hez relatív prím u egész szám m-edik maradék modulo n, ahol m is pozitív egész, ha van olyan v egész, amellyel $v^m \equiv u\ (n)$, míg ellenkező esetben u m-edik nemmaradék modulo n. Ha $p > 2$ prímszám, akkor u akkor és csak akkor m-edik maradék modulo p, ha $u^{\frac{p-1}{t}} \equiv 1\ (p)$, ahol t az m és $p - 1$ legnagyobb közös osztója. Ebből következik, hogy u pontosan akkor m-edik maradék modulo p, ha ugyanezen modulus szerint t-edik maradék. A modulo p m-edik maradékok száma $\frac{p-1}{t}$.

16.2. Definíció

Legyen $n > 2$ prímszám, $1 < t | n - 1$ egész szám, $R^{(0)}$ a modulo n t-edik maradékok halmaza, és q olyan pozitív egész kitevős prímhatvány, hogy $q \in R^{(0)}$. Ekkor a $g = g^{(0)} = \prod_{i \in R^{(0)}}\left(x - \alpha^i\right)$ és az $(x - e)g$ polinomok által generált $C^{(0)} = C$ és $\overline{C^{(0)}} = \bar{C}$ kód, ahol α egy $\mathbb{F}_q$ fölötti primitív n-edik gyök, a **t-edik maradékkód**. $t = 2$ esetén a kód a **kvadratikus maradékkód**, röviden **QR-kód**.

Δ

$q \in R^{(0)}$ akkor és csak akkor, ha $q^{\frac{n-1}{t}} \equiv 1\ (n)$, és ez a kongruencia pontosan akkor teljesül, ha a q modulo n rendje, $o_n(q)$, osztója $\frac{n-1}{t}$-nek. Általánosabban, legyen q a p prím m-edik hatványa egy pozitív egész m-mel. m egyértelműen írható $m = kt + l$ alakban egy nemnegatív egész k-val és t-nél kisebb nemnegatív egész l-lel. Ekkor $q^{\frac{n-1}{t}} = (p^m)^{\frac{n-1}{t}} = p^{k(n-1)}p^{l\frac{n-1}{t}} \equiv p^{l\frac{n-1}{t}}\ (n)$, hiszen n prím és nem többszöröse p-nek. E szerint q pontosan akkor t-edik maradék modulo n, ha p^l rendelkezik ezzel a tulajdonsággal (és biztosan ez a helyzet, ha $l = 0$, azaz ha $t | m$). Ez azt is jelenti, hogy amennyiben p egy modulo n t-edik maradék, akkor bármely pozitív egész m-re $q = p^m$ t-edik maradék modulo n.

$0 \notin R^{(0)}$, és $n > 2$-ből $R^{(0)} \neq \emptyset$, továbbá $g | (x - e)g$, így a $\bar{C}$ kód egy valódi, nem üres részkódja a g-hez tartozó C kódnak, nevezetesen $\bar{C}$ a C azon és csak azon szavait tartalmazza, amelyekben a komponensek összege 0 (tehát $\mathbf{0} \notin C \backslash \bar{C}$). Ez a törlésnek felel meg, míg a másik irány a növelés, ezért C-re mint a **növelt kód**ra (**a**ugmented code), és $\bar{C}$-ra mint a **törléses kód**ra (**e**xpurgated code) is hivatkozunk.

Tekintsünk az $\mathcal{A} = (A; +)$ véges additív Ábel-csoport mint szimbólumhalmaz fölött valamilyen pozitív egész n-nel egy $C \subseteq A^n$ kódot. Legyen $\hat{C}$ a kiterjesztett kód, ahol az $\mathbf{a}^T = a_0 \cdots a_{n-1}$, $\mathbf{a} \in C$ kódszót az $a_n = -\sum_{i=0}^{n-1} a_i$ komponenssel egészítjük ki. Ezt a jegyet neveztük paritásjegynek. Amennyiben $|A| = 2$, akkor a kód bináris, és ez esetben az is teljesül, hogy a C egy kódszavának súlya akkor és csak akkor páros, ha az összeg 0, de más esetben ez általában nem igaz. Legyen $b \in A$-ra C_b a C azon és csak azon $\mathbf{a}$ elemeinek összessége, amelyekre $\sum_{i=0}^{n-1} a_i = b$. Nyilvánvaló, hogy ezek a halmazok páronként idegenek, és az uniójuk a teljes kódhalmaz. A nem üres halmazok a kód részkódjai. Legyen most még C csoportkód, azaz olyan kód, ahol valahányszor $\mathbf{u}$ és $\mathbf{v}$ eleme a kódnak, mindannyiszor a különbségük, $\mathbf{u} - \mathbf{v}$ is hozzá tartozik C-hez, ahol $(\mathbf{u} - \mathbf{v})_i = u_i - v_i$ (és C-nek van legalább egy eleme). $\sum_{i=0}^{n-1}(\mathbf{u} - \mathbf{v})_i = \sum_{i=0}^{n-1}(u_i - v_i) = \sum_{i=0}^{n-1} u_i - \sum_{i=0}^{n-1} v_i$ akkor és csak akkor 0, ha $\mathbf{u}$ és $\mathbf{v}$ ugyanazon b-hez tartozó C_b eleme. Ebből egyrészt következik, hogy a C_0 részkód maga is csoportkód, másrészt, hogy a C_b részkódok a C_0 szerinti mellékosztályok, vagy másként mondva, a C_0 eltoltjai, azaz, ha $\mathbf{a}_b$ a C_b egy tetszőleges, rögzített eleme, akkor $C_b = \mathbf{a}_b + C_0$. Lineáris kód csoportkód, de ekkor még az is igaz, hogy ha e a multiplikatív neutrális elem, akkor $\mathbf{a}_b = b\mathbf{a}_e$ egy lehetséges reprezentáns-rendszer.

A továbbiakban, feltéve, hogy a szimbólumhalmaz véges additív Abel-csoport és $C_0 \neq \emptyset$, a C_0 elemeit a kód **párosszerű elem**einek, **párosszerű kódszó**nak nevezzük, C_0 a kód **párosszerű részkód**ja, és ezen részkód súlya a kód **párosszerű részsúly**a. Magát ezt a részkódot általában C_e-vel, a súlyát w_e-vel jelölik (az *even-like* után) A $C_o = C \setminus C_e$ részkód a **páratlanszerű részkód**, minden eleme egy **páratlanszerű kódszó**, és a súlya, w_o a kód **páratlanszerű részsúly**a (most az o index az *odd-like* utáni). Nyilván a kód w súlya a két részsúly minimuma. Ha $C = C_e$, akkor a kód **párosszerű**.

A fentebb definiált maradékkódra alkalmazhatjuk az új fogalmakat, és ennek alapján $\bar{C}$ a C kód párosszerű részkódja, míg $C \backslash \bar{C} = C_o$. Ha C n-szóhosszúságú kód, r az n-hez relatív prím egész, és $\mathbf{c}$ egy C-beli kódszó, akkor $w(\mathbf{c}) = w\left(\mathbf{c}^{(r)}\right)$ és $\sum_{i=0}^{n-1} c_i = \sum_{i=0}^{n-1} c_i^{(r)}$, így a 145. oldalon kapott eredmény szerint $\left(C^{(r)}\right)_e = (C_e)^{(r)}$ és $\left(C^{(r)}\right)_o = (C_o)^{(r)}$.

16.3. Tétel

A 16.2. Definícióban leírt kód $\mathbb{F}_q$ fölötti kód.

Δ

Bizonyítás:

modulo n t-edik maradék relatív prím n-hez (különben nem lehetne egy pozitív egész kitevős hatványa 1-gyel kongruens modulo n), és t-edik maradékok szorzata t-edik maradék, ezért ha u, v, v_1 és v_2 $R^{(0)}$ elemei, akkor uv_1 és uv_2 is eleme ennek a halmaznak, és $uv_1 \equiv uv_2\ (n)$ akkor és csak akkor, ha $v_1 = v_2$, tehát a $v \mapsto uv$ megfeleltetés $R^{(0)}$ önmagába való injekciója, azaz bijekciója. Ekkor $\{qv | v \in R^{(0)}\} = R^{(0)}$, hiszen $q \in R^{(0)}$. Most $g^q = \prod_{i \in R^{(0)}}\left(x^q - \alpha^{qi}\right) = \prod_{i \in R^{(0)}}\left(x^q - \alpha^i\right) = g \circ x^q$, tehát $g \in \mathbb{F}_q[x]$. De $x - e$ nyilván eleme $\mathbb{F}_q[x]$-nek, így $(x - e)g$ is $\mathbb{F}_q$ fölötti polinom.

□

Ha n prímszám, akkor létezik modulo n primitív gyök, azaz olyan a egész szám, hogy a $\varphi(n)$-nél kisebb nemnegatív egész kitevős hatványai egy redukált maradékrendszert adnak modulo n. Ebből következően $\{a^i \bmod n \,|n - 1 > i \in \mathbb{N}\}$ az n-nél kisebb pozitív egészek halmaza.

16.4. Tétel

Legyen n prímszám, $t|n - 1$ pozitív egész szám, a egy modulo n primitív gyök, és a t-nél kisebb nemnegatív egész i-vel legyen $R^{(i)} = \left\{a^{jt+i} \middle| \frac{n-1}{t} > j \in \mathbb{N}\right\}$. Ha $t > 1$, a q prímhatvány t-edik maradék modulo n és α primitív n-edik gyök $\mathbb{F}_q$ fölött, akkor a $g^{(i)} = \sum_{l \in R^{(i)}}\left(x - \alpha^l\right)$ polinomok által generált $C^{(i)}$ kódok ekvivalensek, és $x^n - e = (x - e)\prod_{i=0}^{t-1} g^{(i)}$, így $\prod_{i=0}^{t-1} g^{(i)} = \sum_{i=0}^{n-1} x^i$.

Δ

Bizonyítás:

a^l, ahol $n-1 > l = jt + i \in \mathbb{N}$, $j \in \mathbb{N}$ és $t > i \in \mathbb{N}$, pontosan akkor t-edik maradék modulo n, ha $1 \equiv \left(a^l\right)^{\frac{n-1}{t}} = \left(a^{jt+i}\right)^{\frac{n-1}{t}} = (a^{n-1})^j a^{i\frac{n-1}{t}} \equiv a^{i\frac{n-1}{t}}\ (n)$. Ez akkor és csak akkor teljesül, ha t osztója i-nek, vagyis ha $i = 0$, tehát $R^{(0)}$ elemei, és csak ezek t-edik maradékok modulo n. $a^{jt+i} = a^{jt}a^i$-ből kiolvasható, hogy $R^{(i)} = a^i R^{(0)}$. $s = a^l \in R^{(i)}$-re $\alpha^s = \alpha^{a^{jt+i}} = \alpha^{a^i s'}$, ahol $s' = a^{jt} \in R^{(0)}$. n prímszám és $n > a^i \bmod n \in \mathbb{N}^+$, tehát $\left(a^i, n\right) = 1$, amiből már következik, hogy a $C^{(i)}$ kódok ekvivalensek (lásd az 15.43. Tételt illetve az előtte lévő eredményeket).

□

A tételből következik, hogy az $(x-e)g^{(i)}$ polinomok által generált $\overline{C^{(i)}}$ kódok is ekvivalensek.

Mind a tétel, mind az előbbi kiegészítés eléggé nyilvánvaló: primitív n-edik egységgyök n-hez relatív prím kitevős hatványa is primitív n-edik egységgyök, így másik ilyen gyököt választva α-nak, egy másik i-hez tartozó $g^{(i)}$ polinom lesz $g^{(0)}$ és vele együtt $C^{(0)} = C$.

Ha az $\mathcal{R}$ kommutatív gyűrűben $a \equiv b\ (u)$ és $v|u$, akkor $a \equiv b\ (v)$, és például vagy mindkettő oszható v-vel, vagy egyikük sem. Amennyiben $\mathcal{R}$ euklideszi gyűrű, amelyben az osztási maradék egyértelmű, $b \neq 0$, és $a = tb + r$, ahol $r = a \bmod b$, akkor $a \equiv r\ (b)$, tehát a b egy osztója vagy mind a-nak és r-nek osztója, vagy egyiküket sem osztja, továbbá ha a p felbonthatatlan elem k-szoros osztója b-nek, akkor egy, a k-nál nem nagyobb pozitív egész l-lel akkor és csak akkor osztja p^l a-t, ha osztja a maradékot is. Speciálisan, ha $\mathcal{R}$ egy test fölötti egyhatározatlanú polinom, akkor a b egy u gyöke vagy mind a-nak, mind r-nek gyöke, vagy egyiküknek sem, és ha u k-szoros gyöke b-nek, akkor $k \geq l \in \mathbb{N}^+$-szal vagy a-nak és r-nek is l-szeres gyöke, vagy egyiküknek sem lesz ilyen többszörösséggel gyöke.

16.5. Tétel

Ha C egy n-szóhosszúságú t-edik maradékkód, ahol $2 < n \in \mathbb{N}$ prímszám és $1 < t \in \mathbb{N}$, továbbá $\mathbf{c} \in C \backslash \bar{C}$ súlya $w(\mathbf{c}) = d$, akkor $d^t > n$.

Δ

Bizonyítás:

Legyen a $\mathbf{c} \in C \backslash \bar{C}$ kódszó súlya d, és c a megfelelő kódpolinom. $\mathbf{c} \in C \backslash \bar{C}$-ből következik, hogy $c \neq 0$ (és így $d > 0$). A $c^{(i)} = \left(c \circ x^{a^i}\right) \bmod (x^n - e)$ polinom a $C \backslash \bar{C}$-tal ekvivalens kódnak a c-vel azonos súlyú kódszava. $g^{(i)} \left| c^{(i)} \right.$ és $\sum_{i=0}^{n-1} x^i \left| x^n - e \right.$ következtében $\sum_{i=0}^{n-1} x^i = \prod_{i=0}^{t-1} g^{(i)}$ osztója az $u = \prod_{i=0}^{t-1} c^{(i)} \bmod (x^n - e)$ polinomnak. Ám $x - e$ nem osztója a maradéknak, mert nem osztója a szorzat egyik tényezőjének, tehát magának a szorzatnak sem, így a maradék nem a nullpolinom. u legfeljebb $n-1$-edfokú, mivel egy n-edfokú polinommal való osztás maradéka, másrészt legalább $n-1$edfokú, ugyanis nem nulla és osztható az $n-1$-edfokú $\sum_{i=0}^{n-1} x^i$ polinommal. Ekkor u pontosan $n-1$-edfokú, és többszöröse az ugyanilyen fokszámú $\sum_{i=0}^{n-1} x^i$ polinomnak, ami csak úgy lehet, ha az utóbbi polinomnak egy nem nulla konstansszorosa. Ebből adódik, hogy $w(u) = n$. Másrészt a t-tényezős $\prod_{i=0}^{t-1} c^{(i)}$ szorzat minden tényezője d-súlyú, tehát $n = w(u) = w\left(\prod_{i=0}^{t-1} c^{(i)} \bmod (x^n - e)\right) \leq \prod_{i=0}^{t-1} d = d^t$. n prímszám, így nagyobb, mint 1, ebből következően d is 1-nél nagyobb egész szám, t pedig a tétel kikötése szerint legalább 2. Egyenlőség esetén ebből azt kapnánk, hogy d nem tiriviális osztója n-nek, ami nem lehet, így az egyenlőtlenség szigorú, $d^t > n$.

□

A tétel semmit nem mond C távolságáról, mert részkód súlya lehet nagyobb a kód súlyánál.

Mivel a modulo n t-edik maradékok száma $\frac{n-1}{t}$, ezért a C t-edik (növelt) maradékkód egy $[n, k]$-paraméterű kód, ahol $k = n - \frac{n-1}{t} = \frac{(t-1)n+1}{t}$.

A továbbiakban a kvadratikus maradékkódokat nézzük. Ezeket, mint már korábban jeleztük, általában QR-kódnak nevezik az angol *quadratic residue code* rövidítéseként. Most $t = 2$, és t osztója $n - 1$-nek, ezért QR-kód esetén a szóhossz páratlan prímszám.

A 147. oldalon kapott eredmény alapján a $q = p^m$-elemű test fölött, ahol p prímszám és m pozitív egész szám, pontosan akkor van páratlan n prímszámmal n-szóhosszúságú kvadratikus maradékkód, ha vagy p kvadratikus maradék $\mathrm{modulo}\, n$, vagy m páros. Két fontos speciális esetet külön megnézünk.

$p = 2$ esetén teljesülnie kell a $2^{\frac{n-1}{2}} \equiv 1\ (n)$ kongruenciának, ami akkor és csak akkor igaz, ha $n = 8k \pm 1$, azaz ha $n \equiv \pm 1\ (8)$. Ennek igazolására nézzük a $\prod_{i=1}^{\frac{n-1}{2}} (2i)$ szorzatot:

$$2^{\frac{n-1}{2}} \prod_{i=1}^{\frac{n-1}{2}} i = \prod_{i=1}^{\frac{n-1}{2}} (2i) = \prod_{i=1}^{\left\lfloor \frac{n-1}{4} \right\rfloor} (2i) \prod_{i=\left\lfloor \frac{n-1}{4} \right\rfloor + 1}^{\frac{n-1}{2}} (2i) = (-1)^{\frac{n-1}{2} - \left\lfloor \frac{n-1}{4} \right\rfloor} \prod_{i=1}^{\left\lfloor \frac{n-1}{4} \right\rfloor} (2i) \prod_{i=\left\lfloor \frac{n-1}{4} \right\rfloor + 1}^{\frac{n-1}{2}} (-2i)$$

$$\equiv (-1)^{\frac{n-1}{2} - \left\lfloor \frac{n-1}{4} \right\rfloor} \prod_{i=1}^{\left\lfloor \frac{n-1}{4} \right\rfloor} (2i) \prod_{i=\left\lfloor \frac{n-1}{4} \right\rfloor + 1}^{\frac{n-1}{2}} (n - 2i)$$

$$= (-1)^{\frac{n-1}{2} - \left\lfloor \frac{n-1}{4} \right\rfloor} \prod_{i=1}^{\left\lfloor \frac{n-1}{4} \right\rfloor} (2i) \prod_{i=1}^{\frac{n-1}{2} - \left\lfloor \frac{n-1}{4} \right\rfloor} (2i - 1) = (-1)^{\frac{n-1}{2} - \left\lfloor \frac{n-1}{4} \right\rfloor} \prod_{i=1}^{\frac{n-1}{2}} i\ (n).$$

n prímszám, így minden, nála kisebb pozitív egész, és akkor a szorzatuk is relatív prím n-hez, következésképpen $\prod_{i=1}^{\frac{n-1}{2}} i$-vel lehet a kongruenciát egyszerűsíteni. Marad tehát a $2^{\frac{n-1}{2}} \equiv (-1)^{\frac{n-1}{2} - \left\lfloor \frac{n-1}{4} \right\rfloor}\ (n)$ kongruencia. A jobb oldal akkor és csak akkor 1, és ennek megfelelően a 2 pontosan akkor kvadratikus maradék $\mathrm{modulo}\, n$, ha $\frac{n-1}{2} - \left\lfloor \frac{n-1}{4} \right\rfloor = \left\lceil \frac{n-1}{4} \right\rceil$ páros. n-et írhatjuk $8k \pm (2\varepsilon + 1)$ alakban, ahol $\varepsilon = 0$ vagy $\varepsilon = 1$. Ekkor $\left\lceil \frac{n-1}{4} \right\rceil = \left\lceil 2k - \frac{1 \mp (2\varepsilon+1)}{4} \right\rceil = 2k - \left\lfloor \frac{1 \mp (2\varepsilon+1)}{4} \right\rfloor$. Ez akkor és csak akkor páros, ha páros a második tag, $\left\lfloor \frac{1 \mp (2\varepsilon+1)}{4} \right\rfloor$. ε lehetséges értékeit kipróbálva azt kapjuk, hogy $\left\lfloor \frac{1 \mp (2\varepsilon+1)}{4} \right\rfloor = 0$, ha $\varepsilon = 0$, azaz ha $2\varepsilon + 1 = 1$, és $\left\lfloor \frac{1 \mp (2\varepsilon+1)}{4} \right\rfloor = \mp 1$, amennyiben $\varepsilon = 1$, amikoris $2\varepsilon + 1 = 3$. Az eredmény valóban az, hogy páratlan n prímszám esetén a 2 pontosan akkor kvadratikus maradék, ha $n = 8k \pm 1$ alakú, és kvadratikus nemmaradék, ha $n = 8k \pm 3$.

Általánosan, ha $2 < n$ prímszám, r pozitív egész szám és $q = 2^r$, úgy a q-elemű test fölött pontosan akkor van n-hosszú kódszavakból QR-kód, ha r páros, vagy n 8-cal való osztási maradéka ± 1.

Másik fontos speciális eset, amikor a test karakterisztikája 3. Most ismét az a kérdés, hogy milyen n páratlan prím esetén kvadratikus maradék a 3. Mivel n és 3 egyaránt prímszám, ezért tekinthetjük a Legendre-szímbólumot, és alkalmazhatjuk a reciprocitási törvényt. A p páratlan prímre adott $\left(\frac{a}{p}\right)$ Legendre-szimbólum lényegében véve a $\mathrm{modulo}\, p$ kvadratikus karakter, azaz $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék $\mathrm{modulo}\, p$, és -1 az értéke nemmaradék esetén. Ezt még ki lehet egészíteni azzal, hogy amennyiben $(a, p) \neq 1$, akkor $\left(\frac{a}{p}\right) = 0$. Mivel két egész szám szorzata akkor és csak akkor maradék, ha vagy mindkét tényező maradék, vagy egyikük sem az, és pontosan akkor relatív prím a szorzat p-hez, ha mindkét szám ilyen tulajdonságú, ezért láthatóan a Legendre-szimbólum multiplikatív. Az is nyilvánvaló, hogy p szerint kongruens egészekre a Legendre-szimbólum azonos értéket ad, valamint az is, hogy $\left(\frac{1}{p}\right) = 1$. Az előző szakaszban azt is megmutattuk, hogy $\left(\frac{2}{p}\right) = 1$ akkor és csak akkor, ha a prím $8k \pm 1$ alakú (páratlan prímeket tekintve). A mostani kérdés tehát az, hogy mikor teljesül a $\left(\frac{3}{p}\right) = 1$ feltétel.

Ehhez használjuk a kvadratikus reciprocitás törvényét, amely szerint $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$, ahol q is egy páratlan prím. Ezt alkalmazva, az $\varepsilon = n \bmod 3$ jelöléssel

$$\left(\frac{3}{n}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{3-1}{2}}\left(\frac{n}{3}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{n \bmod 3}{3}\right)$$
$$= (-1)^{\frac{n-1}{2}}\left(\frac{\varepsilon}{3}\right) = (-1)^{\frac{n-1}{2}}\varepsilon^{\frac{3-1}{2}} = \varepsilon(-1)^{\frac{n-1}{2}}.$$

A fentiek szerint 3 akkor és csak akkor kvadratikus maradék n szerint, ha $3k+1 = n = 4l+1$ vagy $3k-1 = n = 4l-1$, vagyis akkor és csak akkor, ha n-et 3-mal és 4-gyel osztva egyaránt vagy 1-et vagy -1-et kapunk maradékul, azaz pontosan akkor, ha a 12-vel való osztási maradéka ± 1, másként írva, ha $n = 12k \pm 1$ alakú prím.

$x^n - e = (x-e)g^{(0)}g^{(1)}$, ahol $g^{(0)} = \prod_{r\in Q}(x-\alpha^r)$, $g^{(1)} = \prod_{s\in NQ}(x-\alpha^s)$, α a q-elemű test fölötti primitív n-edik gyök, Q a modulo n kvadratikus maradékok és NQ a nemmaradékok összessége. Nyilván az előbb megadott két halmaz idegen, mindkettőnek $\frac{n-1}{2}$ eleme van, egyiküknek sem eleme 0, végül $\{0\} \cup Q \cup NQ = \mathbb{N}_n$. A $g^{(0)}$ által generált $C^{(0)}$ és a $g^{(1)}$ által generált $C^{(1)}$ kód ekvivalens, és ekvivalens az $(x-e)g^{(0)}$-hoz és $(x-e)g^{(1)}$-hez tartozó $\overline{C^{(0)}}$ és $\overline{C^{(1)}}$ kód (esetenként a rövidség kedvéért $C^{(0)}$ helyett C-t írunk).

Ekvivalens kódok között nincs lényeges különbség, ezért mind a $g^{(0)}$, mind a $g^{(1)}$ által generált $C = C^{(0)}$ és $C^{(1)}$ kódot (növelt) kvadratikus maradékkódnak, míg a megfelelő törléses kódokat, tehát $\bar{C} = \overline{C^{(0)}}$-át és $\overline{C^{(1)}}$-et törléses kvadratikus maradékkódnak nevezzük.

Az előzőekben kapott $k = n - \frac{n-1}{t} = \frac{(t-1)n+1}{t}$-ből kvadratikus maradékkódnál $k = \frac{n+1}{2}$, és az $x-e$-vel nem osztható kódszavak d súlyáról láttuk, hogy $d^2 > n$, azaz $d > \sqrt{n}$. $n = 4k-1$ esetén ennél többet is tudunk mondani.

16.6. Tétel

Ha az $\mathbb{F}_q$ fölötti kvadratikus maradékkód szóhosszúsága $n = 4k-1$, akkor az $x-e$-vel nem osztható kódszavak d súlyára $d^2 - d + 1 \geq n$, továbbá $q = 2$ és $n = 8k-1$ esetén $d \equiv 3\ (4)$.

Δ

Bizonyítás:

Az első állítás bizonyítása közben egy másik igazolását is látjuk majd, hogy egy t-edik maradékkód $x-e$-vel nem osztható kódszavainak súlya nagyobb, mint $\sqrt[t]{n}$.

Legyen $i = 1, 2$-re $f^{(i)} = \sum_{j=0}^{n^{(i)}} a_j^{(i)} x^j$, $I^{(i)} = \left\{n^{(i)} \geq j \in \mathbb{N} \middle| a_j^{(i)} \neq 0\right\}$, K az $I^{(1)}$ és $I^{(2)}$ komplexus-összege, és $L = \left\{k \in K \middle| \sum_{j\in I^{(1)}} a_j^{(1)} a_{k-j}^{(2)} \neq 0\right\}$. Ekkor $L \subseteq K$, és $d = |L| \leq |K| \leq \left|I^{(1)} \times I^{(2)}\right| = \left|I^{(1)}\right|\left|I^{(2)}\right| = d^{(1)}d^{(2)}$, ahol tehát $d^{(i)}$ az $f^{(i)}$ polinom nullától különböző együtthatóinak száma, azaz a szorzatban szereplő nem nulla együtthatók száma legfeljebb a két polinom nullától különböző együtthatói számának szorzata. Innen indukcióval kapjuk, hogy ha $m \in \mathbb{N}^+$, és $m > i \in \mathbb{N}$-re az $f^{(i)}$ polinom súlya $d^{(i)}$, akkor a szorzat súlya legfeljebb a súlyok szorzata.

Most tekintsünk egy olyan kódot, ahol a szóhosszúság $n = 4k-1$. Ez esetben a -1 nemmaradék, és ha a d-súlyú c kódszó $x-e$-vel nem osztható, akkor $c^{(-1)} = c \circ x^{-1}$-gyel a $cc^{(-1)}$ szorzatban minden olyan i indexre, amelyre $c_i \neq 0$, szerepel $c_i c_i x^{i-i} = c_i c_i$. Ilyen szorzat éppen d van, tehát a szorzatban legalábbis d tag ugyanazon kitevőhöz tartozik, amiből következik, hogy a szorzat súlya biztosan legalább $d-1$-gyel kisebb, mint a súlyok szorzata, d^2. Ebből kapjuk, hogy $n \leq d^2 - d + 1$.

Ha n $8k-1$-alakú, akkor egyben $4k-1$-alakú is, alkalmazható a d-re kapott előző eredmény. Vegyük még figyelembe, hogy ha egy i_1, j_1 és egy, az előzőtől különböző i_2, j_2 párra $0 \neq i_1 - j_1 =$

$i_2 - j_2$, akkor a szorzatban szerepel a $c_{i_1}c_{j_1}x^{i_1-j_1} + c_{i_2}c_{j_2}x^{i_2-j_2} + c_{j_1}c_{i_1}x^{j_1-i_1} + c_{j_2}c_{i_2}x^{j_2-i_2}$ összeg, és ez $q = 2$ esetén $x^{i_1-j_1} + x^{i_2-j_2} + x^{j_1-i_1} + x^{j_2-i_2}$. De az indexpárok egyenlősége következtében most $x^{i_1-j_1} + x^{i_2-j_2} + x^{j_1-i_1} + x^{j_2-i_2} = x^{i_1-j_1} + x^{i_1-j_1} + \quad ^{j_1-i_1} + x^{j_1-i_1} = 0$, vagyis mindig egyszerre négy tag esik ki. A szorzat végül, a kitevők modulo n redukálása után, $\sum_{i=0}^{n-1} x^i$, ami azt jelenti, hogy valamilyen nemnegatív egész t-vel $n = d^2 - d + 1 + 4t$. Mivel most $n = 4k - 1$, ezért 4 osztója $d^2 - d + 2$-nek, és d páratlan. Páratlan szám négyzete mindig $8k + 1$-alakú, de akkor 4-gyel osztva is 1-et ad maradékul. Ekkor $d^2 + 2$ maradéka 3 és így $d^2 - d + 2$ pontosan akkor osztható 4-gyel, ha d 4-gyel való osztási maradéka 3, azaz ha $d \equiv 3\ (4)$.

□

Meghatározzuk a kvadratikus maradékkód duálisát.

16.7. Tétel

A q-elemű test fölötti, páratlan n szóhosszúságú kvadratikus maradékkód duálisa $4k - 1$-alakú n esetén $\bar{C}$, míg az ellenkező esetben $C^{\perp} = \overline{C^{(1)}}$.

Δ

Bizonyítás:

$(x - e)g^{(0)}g^{(1)} = x^n - e$-ből $(x - e)g^{(1)} = \frac{x^n - e}{g^{(0)}}$, azaz a $g^{(0)}$ által generált ciklikus kód ellenőrző polinomja $h^{(0)} = (x - e)g^{(1)}$. Tetszőleges C ciklikus kód esetén, feltéve, hogy q és n relatív prím, a kód g generátor- és h ellenőrző polinomja relatív prím. Ebből következik, hogy az általuk generált két kód metszete $\{0\}$, azaz csak a nullpolinomot tartalmazza, míg a két kód összege valamennyi legfeljebb $n - 1$-edfokú polinomot tartalmazza, ahol n a szóhosszúság, és minden polinom egy és csak egyféleképpen írható fel $g^{(0)}$ és $h^{(0)}$ olyan lineáris kombinációjaként, ahol $g^{(0)}$ együtthatója legfeljebb $k - 1$-edfokú, míg a $h^{(0)}$ együtthatója legfeljebb $(n - k) - 1$-fokú polinom, a két kód által alkotott tér egymás kiegészítő altere. Tudjuk azonban, hogy a $g^{(0)}$ által generált C kód duálisa nem a $h^{(0)}$ által generált kód, hanem az a kód, amelynek generátor-polinomja a $h^{(0)^*}$-hoz tartozó főpolinom. Ha egy polinom konstans tagja nem nulla, akkor a duálisa, konstans szorzótól eltekintve, az a polinom, amelynek gyökei az eredeti polinom gyökeinek inverzei az eredetivel megegyező többszörösséggel. Ebből arra jutunk, hogy az $\mathbb{F}_q$ fölötti primitív n-edik egységgyökkel, α-val generált $g^{(0)} = \prod_{r \in Q}(x - \alpha^r)$-hez tartozó kód duálisát az $(x - e^{-1})\prod_{s \in NQ}(x - \alpha^{-s})$ polinom generálja. Két egész szám szorzata akkor és csak akkor kvadratikus maradék modulo n, ha vagy mindkettő maradék, vagy mindkettő nemmaradék. $-s = (-1) \cdot s$, és $s \in NQ$, így $-s$ maradék, ha a -1 is nemmaradék modulo n, ellenkező esetben $-s \in NQ$. n páratlan prímszám, ekkor a -1 pontosan akkor maradék, ha $n = 4k + 1$. Ez azt jelenti, hogy $4k - 1$-alakú n esetén $(x - e)\prod_{r \in Q}(x - \alpha^r)$ a $g^{(0)}$-generálta kód duálisának generátor-polinomja, és ez a kód $\bar{C}$, míg a másik esetben a generátorpolinom $(x - e)\prod_{s \in NQ}(x - \alpha^s)$, vagyis ebben az esetben $C^{\perp} = \overline{C^{(1)}}$.

□

Most a kód idempotensével foglalkozunk. Elsőként a 2-karakterisztikájú testek feletti QR-kód idempotensét határozzuk meg.

16.8. Tétel

Legyen $m \in \mathbb{N}^+$, $q = 2^m$, $p \equiv -1\ (8)$ prímszám, $g = \sum_{r \in Q}(x - \alpha^r)$ és $g^{(1)} = \sum_{s \in NQ}(x - \alpha^s)$, ahol α egy $\mathbb{F}_q$ fölötti primitív p-edik egységgyök, Q a modulo p kvadratikus maradékok és NQ a nemmaradékok halmaza. Ha C a g- és $C^{(1)}$ a $g^{(1)}$ által generált QR-kód, és rendre $\bar{C}$ és $\overline{C^{(1)}}$ a megfelelő törléses maradékkód, akkor az α primitív p-edik gyök alkalmas választásával a megfelelő idempotensek $E = \sum_{r \in Q} x^r$, $E^{(1)} = \sum_{s \in NQ} x^s$, $\bar{E} = e + \sum_{s \in NQ} x^s$ és $\overline{E^{(1)}} = e + \sum_{r \in Q} x^r$, ahol e a test egységeleme.

Δ

Bizonyítás:

E pontosan akkor idempotense a kódnak, ha $r \in Q$ esetén α^r gyöke a polinomnak, $\hat{E}(e) = e$, és $\hat{E}(\alpha^s) = e$, amennyiben $s \in NQ$.

Már láttuk, hogy $x^u \bmod (x^v - e) = x^{u \bmod v}$, így $\sum_{i=0}^{l} a_i x^i \bmod (x^p - e) = \sum_{i=0}^{l} a_i x^{i \bmod p}$. Ha r' kvadratikus maradék és s' nemmaradék modulo p, akkor modulo p $r'Q = Q = s'NQ$ valamint $r'NQ = NQ = s'Q$. Ekkor $\left(E \circ x^{r'}\right) \bmod (x^p - e) = \sum_{r \in Q} x^{r' r \bmod p} = \sum_{r \in Q} x^r = E$, és hasonlóan kapjuk, hogy $\left(E \circ x^{s'}\right) \bmod (x^p - e) = \sum_{r \in Q} x^{s' r \bmod p} = \sum_{s \in NQ} x^s = E^{(1)}$. A test karakterisztikája 2, így $E^2 = \left(\sum_{r \in Q} x^r\right)^2 = \sum_{r \in Q} x^{2r} = E \circ x^2$, és mivel $2 \in Q$, ezért $E^2 \bmod (x^p - e) = E$, E idempotens az $x^p - e$ szerinti maradékosztály-gyűrűben.

Ha f és $g \neq 0$ test fölötti polinomok, akkor $f^{(1)} = f \bmod g = f - gh$-ból $\widehat{f^{(1)}}(u) = \hat{f}(u) - \hat{g}(u)\hat{h}(u)$, és ha u gyöke g-nek, akkor $\widehat{f^{(1)}}(u) = \hat{f}(u)$. E-re alkalmazva $\left(\hat{E}(u)\right)^2 = \widehat{E^2}(u) = \hat{E}(u)$ az $x^p - e$ bármely u gyökére, következésképpen $\hat{E}(u)$ értéke vagy 0 vagy e. $\{0\}$, Q és NQ páronként diszjunkt, egyikük sem üres, és az uniójuk a p-nél kisebb nemnegatív egész számok halmaza, amiből következik, hogy $e + E + E^{(1)} = x^0 + \sum_{r \in Q} x^r + \sum_{s \in NQ} x^s = \sum_{i=0}^{p-1} x^i$. Ekkor a $\sum_{i=0}^{p-1} x^i$ tetszőleges v gyökére $e + \hat{E}(v) + \widehat{E^{(1)}}(v) = 0$. $x^p - e = (x - e)\sum_{i=0}^{p-1} x^i$, tehát v egyben $x^p - e$-nek is gyöke, így mind $\hat{E}(v)$, mind $\widehat{E^{(1)}}(v)$ vagy 0 vagy e. A két polinom helyettesítési értéke nem lehet azonos, mert akkor $e + \hat{E}(v) + \widehat{E^{(1)}}(v) = e$, így egyikük 0, a másik e, v az egyik és csak az egyik polinomnak gyöke. Mivel x^0-t egyikük sem tartalmazza, mindkettő legfeljebb $p - 1$-edfokú, nem nulla főpolinom, és $\sum_{i=0}^{p-1} x^i$ pontosan $p - 1$-edfokú főpolinom, ezért $\sum_{i=0}^{p-1} x^i$ nem osztója egyik polinomnak sem. Ez egyben azt is jelenti, hogy egyiküknek sem gyöke $\sum_{i=0}^{p-1} x^i$ valamennyi gyöke, és ekkor mindkettőnek gyöke az előbbi gyökök legalább egyike.

$\hat{E}\left(v^{r'}\right) = \left(E \circ \left(x^{r'} \circ v\right) = \left(E \circ x^{r'}\right) \bmod (x^p - e)\right) \circ v = \hat{E}(v)$, ahol v ismét a $\sum_{i=0}^{p-1} x^i$ gyöke és $r' \in Q$, míg $\hat{E}\left(v^{s'}\right) = \left(E \circ \left(x^{s'} \circ v\right) = \left(E \circ x^{s'}\right) \bmod (x^p - e)\right) \circ v = \widehat{E^{(1)}}(v)$, ha s' nemmaradék. $\sum_{i=0}^{p-1} x^i$ gyökei az e-től különböző p-edik egységgyökök, vagyis az α p-nél kisebb pozitív egész kitevős hatványai. α választható úgy, hogy gyöke legyen E-nek. Ellenkező esetben $v = \alpha$-val és az előző s'-vel $0 = \widehat{E^{(1)}}(\alpha) = \hat{E}\left(\alpha^{s'}\right)$. p prímszám, ezért s' relatív prím p-hez, és így $\alpha^{s'}$ is primitív p-edik egységgyök a test fölött, ezért α helyett $\alpha^{s'}$-t választva már olyan α-nk van, amely gyöke E-nek. Ilyen α-val és $p > t \in \mathbb{N}^+$ kitevővel α^t pontosan akkor gyöke E-nek, ha t kvadratikus maradék. Végül $\hat{E}(e) = e$, mert a test karakterisztikája 2 és a polinom tagjainak száma $\frac{(4k-1)-1}{2} = 2k - 1$, azaz páratlan. Ezen eredmények alapján most E a C kód idempotense.

A fentiekből az is rögtön kiadódik, hogy az előbbi α-val $E^{(1)}$ a $C^{(1)}$, $e + E^{(1)}$ a $\bar{C}$ és végül $e + E$ a $\overline{C^{(1)}}$ kód idempotense, csak azt kell még figyelembe venni, hogy például $(e + E)^2 = e + E^2$.

□

16.9. Tétel

Ha az előző tételben $p \equiv 1\ (8)$, akkor a C, $C^{(1)}$, $\bar{C}$ és $\overline{C^{(1)}}$ kódok idempotense az α primitív p-edik gyök alkalmas megválasztásával rendre $E = e + \sum_{r \in Q} x^r$, $E^{(1)} = e + \sum_{s \in NQ} x^s$, $\bar{E} = \sum_{s \in NQ} x^s$ valamint $\overline{E^{(1)}} = \sum_{r \in Q} x^r$, ahol e a test egységeleme.

Δ

Bizonyítás:

Az előző esethez képest csak annyi az eltérés, hogy most $\sum_{r \in Q} x^r$ és $\sum_{s \in NQ} x^s$ páros számú tagot tartalmaz, így ezeknek a polinomoknak gyöke e, ezért csak a törléses kód idempotensei lehetnek.

□

A páratlan q prímhatvány esete bonyolultabb. Először szükségünk lesz egy speciális elemre.

16.10. Tétel

Legyen $\theta = \sum_{i=0}^{p-1} \chi(i)\alpha^i$, ahol $p > 2$ olyan prímszám, hogy q kvadratikus maradék a p modulusra, α a q-elemű test fölötti primitív p-edik egységgyök, és χ egy modulo p kvadratikus karakter. Ekkor $\theta \in \mathbb{F}_q$, és ha $p = 4k + \varepsilon$ úgy, hogy $\varepsilon \in \{+1, -1\}$, akkor $\theta^2 = \varepsilon pe$.

Δ

Bizonyítás:

q relatív prím p-hez, így $\{qi | p > i \in \mathbb{N}\}$ teljes maradékrendszer modulo p, tetszőleges $k \in \mathbb{Z}$-re $\alpha^k = \alpha^{k \bmod p}$, így $\{\alpha^{qi} | p > i \in \mathbb{N}\} = \{\alpha^i | p > i \in \mathbb{N}\}$. $\chi(i)$ 0-val illetve ± 1-gyel egyenlő, és ezek bármelyikének páratlan egész kitevős hatványa önmaga, $(\chi(i))^q = \chi(i)$. Mivel q kvadratikus maradék modulo p, ezért qi és i egyszerre maradék, nemmaradék vagy p-vel osztható, ennélfogva $\chi(qi) = \chi(i)$ tetszőleges i egész szám esetén. Mindezek alapján

$$\theta^q = \left(\sum_{i=0}^{p-1} \chi(i)\alpha^i\right)^q = \sum_{i=0}^{p-1} \left(\chi(i)\alpha^i\right)^q$$
$$= \sum_{i=0}^{p-1} (\chi(i))^q (\alpha^i)^q = \sum_{i=0}^{p-1} \chi(qi)\alpha^{qi} = \sum_{i=0}^{p-1} \chi(i)\alpha^i = \theta,$$

ami azt jelenti, hogy $\theta \in \mathbb{F}_q$. Határozzuk most meg θ négyzetét.

$$\theta^2 = \left(\sum_{i=0}^{p-1} \chi(i)\alpha^i\right)^2 = \left(\sum_{i=0}^{p-1} \chi(i)\alpha^i\right)\left(\sum_{i=0}^{p-1} \chi(i)\alpha^i\right) = \left(\sum_{i=0}^{p-1} \chi(i)\alpha^i\right)\left(\sum_{j=0}^{p-1} \chi(j)\alpha^j\right)$$
$$= \left(\sum_{i=0}^{p-1} \chi(i)\alpha^i\right)\left(\sum_{j=-i}^{p-1-i} \chi(j)\alpha^j\right) = \left(\sum_{i=0}^{p-1} \chi(i)\alpha^i\right)\left(\sum_{j=0}^{p-1} \chi(j-i)\alpha^{j-i}\right)$$
$$= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \chi(i)\chi(j-i)\alpha^i\alpha^{j-i} = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \chi(i)\chi(j-i)\alpha^j = \sum_{j=0}^{p-1}\left(\sum_{i=0}^{p-1} \chi(i)\chi(j-i)\right)\alpha^j.$$

$i = 0$ esetén $\chi(i) = 0$, így j-től függetlenül $\chi(i)\chi(j-i) = 0$, $\sum_{i=0}^{p-1} \chi(i)\chi(j-i) = \sum_{i=1}^{p-1} \chi(i)\chi(j-i)$. $p > i \in \mathbb{N}^+$ esetén i-nek létezik modulo p inverze, i'. A karakter multiplikatív, és bármely, a p-hez relatív prím i egész esetén $\chi(i^2) = 1$, így az előbbi i-re $\chi(i)\chi(j-i) = \chi(i^2)\chi(i'j-1) = \chi(i'j-1)$. Ha $j = 0$, akkor $\chi(i'j-1) = \chi(-1) = \varepsilon$, ahol $\varepsilon = \pm 1$ úgy, hogy $p = 4k + \varepsilon$. θ^2 fentebbi kifejezésében az összeg $j = 0$ indexhez tartozó tagja $\sum_{i=0}^{p-1} \chi(i)\chi(0-i)\alpha^0 = \sum_{i=1}^{p-1} \varepsilon e = \varepsilon(p-1)e$. Nézzük a többi esetet, vagyis amikor $p > j \in \mathbb{N}^+$. Különböző $p > i \in \mathbb{N}^+$-hoz különböző, szintén p-nél kisebb pozitív egész i' tartozik, amely relatív prím p-hez, ennélfogva $\{i'j | p > i \in \mathbb{N}^+\}$ egy modulo p redukált maradékrendszer, vagyis a teljes maradékrendszerből csak a 0-nak megfelelő elem hiányzik. Ezt tudva kapjuk, hogy $\{(i'j-1) \bmod p | p > i \in \mathbb{N}^+\} \cup \{-1\}$ egy teljes maradékrendszer p-re mint modulusra nézve, és ezért $p > j \in \mathbb{N}^+$ esetén

$$\sum_{i=1}^{p-1} \chi(i)\chi(j-i) = \sum_{i=1}^{p-1} \chi(i'j-1) = \sum_{i=0}^{p-1} \chi(i) - \chi(-1) = -\chi(-1) = -\varepsilon.$$

A geometriai sor összegképletével $\sum_{j=1}^{p-1} \alpha^j = \alpha\frac{e-\alpha^{p-1}}{e-\alpha} = \frac{\alpha-\alpha^p}{e-\alpha} = \frac{\alpha-e}{e-\alpha} = -e$. Ezt, valamint az előző eredményt alkalmazva

$$\theta^2 = \sum_{j=0}^{p-1}\left(\sum_{i=0}^{p-1}\chi(i)\chi(j-i)\right)\alpha^j = \left(\sum_{i=0}^{p-1}\chi(i)\chi(0-i)\right)\alpha^0 + \sum_{j=1}^{p-1}\left(\sum_{i=0}^{p-1}\chi(i)\chi(j-i)\right)\alpha^j$$
$$= \varepsilon(p-1)e + \sum_{j=1}^{p-1}(-\varepsilon)\alpha^j = \varepsilon\left((p-1)e - \sum_{j=1}^{p-1}\alpha^j\right) = \varepsilon\big((p-1)e + e\big) = \varepsilon pe.$$

□

$\theta \in \mathbb{F}_q$ és $\theta^2 = \varepsilon pe$ azt jelenti, hogy εpe kvadratikus eleme a q-elemű testnek.

Ha $\theta \in \mathbb{F}_q$, akkor ez $-\theta$-ra is igaz, és az is, hogy $(-\theta)^2 = \theta^2 = \varepsilon pe$, vagyis akár θ, akár $-\theta$ tekinthető εpe négyzetgyökének. A két elemre együtt $\epsilon\theta$-ként is fogunk hivatkozni, ahol $\epsilon \in \{\pm 1\}$.

Rátérhetünk az idempotens meghatározására.

p (páratlan) prímszám, így minden, p-vel nem osztható egész szám, tehát például a p-nél kisebb pozitív egész számok, relatív prím p-hez, és ezek fele kvadratikus maradék, a másik fele nemmaradék modulo p. Amennyiben t a p-hez relatív prím, akkor van modulo p inverze, azaz létezik olyan t' egész szám, amellyel $t't \equiv 1\ (p)$. Legyen α egy $\mathbb{F}_q$ fölötti primitív p-edik egységgyök és χ egy modulo p kvadratikus karakter. Ahogy már fentebb is láttuk, ha $u \equiv v\ (p)$, akkor $\alpha^u = \alpha^v$ és $\chi(u) = \chi(v)$, továbbá tetszőleges i és t egész számmal $\chi(ti) = \chi(t)\chi(i)$, és $\chi(ti)$ egymást kizáró módon 0, ha t osztható p-vel, $\chi(i)$, ha t egy modulo p kvadratikus maradék, végül $-\chi(i)$, amennyiben t egy modulo p kvadratikus nemmaradék. $p \nmid t$ esetén $\chi(i) = \chi(1\cdot i) = \chi\big((t't)i\big) = \chi\big(t'(ti)\big) = \chi(t')\chi(ti)$. Legyen $p > t \in \mathbb{N}^+$. Ekkor α^t is $\mathbb{F}_q$ fölötti primitív p-edik egységgyök, és $\alpha^t \neq e$, azaz $e - \alpha^t \neq 0$, $e - \alpha^t$-vel lehet osztani. Ezen eredmények felhasználásával

$$\sum_{i=1}^{p-1}(\alpha^t)^i = \sum_{i=0}^{p-1}(\alpha^t)^i - (\alpha^t)^0 = \frac{e-(\alpha^t)^p}{e-\alpha^t} - e = -e,$$
$$\sum_{i=1}^{p-1}\chi(i)(\alpha^t)^i = \sum_{i=1}^{p-1}\chi(t')\chi(ti)(\alpha^t)^i = \chi(t')\sum_{i=1}^{p-1}\chi(ti)(\alpha^t)^i = \chi(t)\sum_{i=1}^{p-1}\chi(ti)\alpha^{ti}$$
$$= \chi(t)\sum_{i=0}^{p-1}\chi(ti)\alpha^{ti} = \chi(t)\sum_{i=0}^{p-1}\chi(i)\alpha^i = \chi(t)\theta,$$

ahol felhasználtuk, hogy t és t' egyszerre kvadratikus maradék vagy nemmaradék, valamint azt, hogy a ti-k összessége is egy teljes maradékrendszer modulo p.

Keressük f-et $a + b\sum_{r\in Q}x^r + c\sum_{s\in NQ}x^s = a + \frac{b+c}{2e}\sum_{i=1}^{p-1}x^i + \frac{b-c}{2e}\sum_{i=1}^{p-1}\chi(i)x^i$ alakban $\mathbb{F}_q$-beli a, b és c együtthatókkal. f pontosan akkor idempotense egy $\mathbb{F}_q$ fölötti, n-szóhosszúságú kvadratikus maradékkódnak, ha vagy minden $r \in Q$-ra α^r gyöke a kódnak, és NQ-beli s-re α^s nem gyöke ennek a kódnak, vagy fordítva, és e is vagy gyök, vagy nem gyök. Ennek megfelelően egy $u \in \{0,1\}$ és egy $v \in \{0,1\}$ egésszel

$$ue = a + \frac{b+c}{2e}\sum_{i=1}^{p-1}(\alpha^r)^i + \frac{b-c}{2e}\sum_{i=1}^{p-1}\chi(i)(\alpha^r)^i = a - \frac{b+c}{2e} + \frac{b-c}{2e}\,\theta,$$
$$(1-u)e = a + \frac{b+c}{2e}\sum_{i=1}^{p-1}(\alpha^s)^i + \frac{b-c}{2e}\sum_{i=1}^{p-1}\chi(i)(\alpha^s)^i = a - \frac{b+c}{2e} - \frac{b-c}{2e}\,\theta,$$
$$ve = a + \frac{b+c}{2e}\sum_{i=1}^{p-1}e^i + \frac{b-c}{2e}\sum_{i=1}^{p-1}\chi(i)e^i = a + (p-1)\frac{b+c}{2e}.$$

Ez egy három egyenletből álló, három ismeretlent tartalmazó lineáris egyenletrendszer. Az első egyenletből kivonva a másodikat $(b-c)\,\theta = (2u-1)e$, vagyis $b-c = \frac{(2u-1)e}{\theta}$. Ugyanezt a két egyenletet összeadva $2a-(b+c) = e$. A harmadik egyenlettel összehasonlítva innen

$$e+(b+c) = 2ve-(p-1)(b+c),$$

és ebből $b+c = \frac{(2v-1)e}{pe}$, majd ezzel és a $2a-(b+c) = e$ egyenlőséggel

$$a = \frac{e}{2e} + \frac{(2v-1)e}{2pe}.$$

Végül $b-c$-ből és $b+c$-ből

$$b = \frac{(2u-1)e}{2\,\theta} + \frac{(2v-1)e}{2\,pe},$$
$$c = -\frac{(2u-1)e}{2\,\theta} + \frac{(2v-1)e}{2\,pe}.$$

Az u és v értékétől függően négy különböző f polinomot kapunk, pontosan annyit, ahány különböző kvadratikus maradékkód van adott test fölött egy adott szóhosszúsággal. A négy polinom

$$v=0,u=0\colon f_0 = \left(\frac{e}{2e}-\frac{e}{2pe}\right)-\left(\frac{e}{2pe}+\frac{e}{2\theta}\right)\sum_{r\in Q}x^r-\left(\frac{e}{2pe}-\frac{e}{2\theta}\right)\sum_{s\in NQ}x^s$$
$$v=0,u=1\colon f_1 = \left(\frac{e}{2e}-\frac{e}{2pe}\right)-\left(\frac{e}{2pe}-\frac{e}{2\theta}\right)\sum_{r\in Q}x^r-\left(\frac{e}{2pe}+\frac{e}{2\theta}\right)\sum_{s\in NQ}x^s$$
$$v=1,u=0\colon f_2 = \left(\frac{e}{2e}+\frac{e}{2pe}\right)+\left(\frac{e}{2pe}-\frac{e}{2\theta}\right)\sum_{r\in Q}x^r+\left(\frac{e}{2pe}+\frac{e}{2\theta}\right)\sum_{s\in NQ}x^s$$
$$v=1,u=1\colon f_3 = \left(\frac{e}{2e}+\frac{e}{2pe}\right)+\left(\frac{e}{2pe}+\frac{e}{2\theta}\right)\sum_{r\in Q}x^r+\left(\frac{e}{2pe}-\frac{e}{2\theta}\right)\sum_{s\in NQ}x^s.$$

Éppen négy idempotensre van szükségünk, nevezetesen a C, a $\bar{C}$, a $C^{(1)}$ és a $\overline{C^{(1)}}$ kód E, $\bar{E}$, $E^{(1)}$ és $\overline{E^{(1)}}$ idempotensére. Az első két egyenletnek gyöke e (ez a két egyenlet tartozik $v=0$-hoz), a másik kettőnek nem, így az első két egyenlet lehet a törléses kódok, a második kettő pedig a növelt kódok idempotense. A polinomok az előbbi sorrendben

$$f_0 = \left(\frac{e}{2e}-\frac{e}{2pe}\right)-\frac{e}{2pe}\sum_{i=1}^{p-1}x^i-\frac{e}{2\theta}\sum_{i=1}^{p-1}\chi(i)x^i$$
$$f_1 = \left(\frac{e}{2e}-\frac{e}{2pe}\right)-\frac{e}{2pe}\sum_{i=1}^{p-1}x^i+\frac{e}{2\theta}\sum_{i=1}^{p-1}\chi(i)x^i$$
$$f_2 = \left(\frac{e}{2e}+\frac{e}{2pe}\right)+\frac{e}{2pe}\sum_{i=1}^{p-1}x^i-\frac{e}{2\theta}\sum_{i=1}^{p-1}\chi(i)x^i$$
$$f_3 = \left(\frac{e}{2e}+\frac{e}{2pe}\right)+\frac{e}{2pe}\sum_{i=1}^{p-1}x^i+\frac{e}{2\theta}\sum_{i=1}^{p-1}\chi(i)x^i$$

alakban is írhatóak (látható, hogy ϵ másik választásával csak annyi történne, hogy felcserélődik egyrészt f_0 és f_1, másrészt f_2 és f_3). Az α adott választásával $u=0$. Ekkor $f_2 = E$, $f_0 = \bar{E}$, $f_3 = E^{(1)}$ és végül

$f_1 = \overline{E^{(1)}}$, megkaptuk a négy kód idempotensét. α helyett α^s-t választva egy kvadratikus nemmaradék s-sel, felcserélődik egyrészt f_0 és f_1, másrészt f_2 és f_3. Az eredményt az alábbi tételben megismételjük és kiegészítjük.

16.11. Tétel

Legyen q páratlan prímhatvány, és legyen $g = \sum_{r\in Q}(x-\alpha^r)$ valamint $g^{(1)} = \sum_{s\in NQ}(x-\alpha^s)$, ahol α egy $\mathbb{F}_q$ fölötti primitív p-edik egységgyök, Q a modulo p kvadratikus maradékok és NQ a nemmaradékok halmaza. Ha C a g- és $C^{(1)}$ a $g^{(1)}$ által generált QR-kód, és rendre $\bar{C}$ és $\overline{C^{(1)}}$ a megfelelő törléses maradékkód, akkor az α primitív p-edik gyök alkalmas választásával a megfelelő idempotensek a C, $\bar{C}$, $C^{(1)}$ és $\overline{C^{(1)}}$ sorrendben

$$\begin{aligned}
E &= \left(\frac{e}{2e}+\frac{e}{2pe}\right)+\left(\frac{e}{2pe}-\frac{e}{2\theta}\right)\sum_{r\in Q}x^r+\left(\frac{e}{2pe}+\frac{e}{2\theta}\right)\sum_{s\in NQ}x^s\\
&= \frac{(p+1)e}{2pe}x^0+\frac{e}{2pe}\sum_{i=1}^{p-1}(e-\varepsilon\chi(i)\theta)x^i\\
\bar{E} &= \left(\frac{e}{2e}-\frac{e}{2pe}\right)-\left(\frac{e}{2pe}+\frac{e}{2\theta}\right)\sum_{r\in Q}x^r-\left(\frac{e}{2pe}-\frac{e}{2\theta}\right)\sum_{s\in NQ}x^s\\
&= \frac{(p-1)e}{2pe}x^0-\frac{e}{2pe}\sum_{i=1}^{p-1}(e+\varepsilon\chi(i)\theta)x^i\\
E^{(1)} &= \left(\frac{e}{2e}+\frac{e}{2pe}\right)+\left(\frac{e}{2pe}+\frac{e}{2\theta}\right)\sum_{r\in Q}x^r+\left(\frac{e}{2pe}-\frac{e}{2\theta}\right)\sum_{s\in NQ}x^s\\
&= \frac{(p+1)e}{2pe}x^0+\frac{e}{2pe}\sum_{i=1}^{p-1}(e+\varepsilon\chi(i)\theta)x^i\\
\overline{E^{(1)}} &= \left(\frac{e}{2e}-\frac{e}{2pe}\right)-\left(\frac{e}{2pe}-\frac{e}{2\theta}\right)\sum_{r\in Q}x^r-\left(\frac{e}{2pe}+\frac{e}{2\theta}\right)\sum_{s\in NQ}x^s\\
&= \frac{(p-1)e}{2pe}x^0-\frac{e}{2pe}\sum_{i=1}^{p-1}(e-\varepsilon\chi(i)\theta)x^i.
\end{aligned}$$

Δ

Legyen C a q-elemű test fölötti, p-hosszúságú kódszavakat tartalmazó kvadratikus maradékkód. $(x-e)\sum_{i=0}^{p-1}x^i = x^p - e = (x-e)gg^{(1)}$-ből, valamint abból, hogy x^p-e gyökei egyszeresek következik, hogy g osztója $\sum_{i=0}^{p-1}x^i$-nek, $(x-e)g$ viszont nem. Ekkor a minden pozíción e-t tartalmazó szó eleme C-nek, de nem eleme $\bar{C}$-nak. Korábban láttuk, hogy egy kód idempotensének eltoltjai generálják a kódot. Legyen $\overline{\mathbf{G}}$ az $\bar{E}$ eltoltjait tartalmazó mátrix. Ez a mátrix a $\frac{p-1}{2}$-dimenziós $\bar{C}$-t generálja. Mivel ennek a kódnak gyöke e, ezért minden szó komponenseinek összege 0 (a q-elemű testben). Kibővítve $\overline{\mathbf{G}}$-t a csupa e-t tartalmazó $\mathbf{e}^T$ sorral, a kapott $\mathbf{G}$ mátrix C-t generálja, hiszen ez utóbbi kódnak része $\bar{C}$ és tartalmazza $\mathbf{e}$-t, tehát ezek bármely lineáris kombinációját, ám így $\frac{p+1}{2}$-dimenziós kódot kapunk, éppen akkorát, amekkora C (egyébként az is könnyen kiszámolható, hogy $E = \bar{E} + \frac{e}{pe}\sum_{i=0}^{p-1}x^i$, vagyis C idempotense lineáris kombinációja $\bar{C}$ idempotensének és $\sum_{i=0}^{p-1}x^i$-nek, azaz a csupa e-t tartalmazó szónak). Ugyanezt az eredményt kapjuk $\overline{C^{(1)}}$-nál is.

Terjesszük ki ezeket a kódokat. A kiterjesztett kódokat $\hat{C}$ és $\widehat{C^{(1)}}$, a hozzájuk tartozó generátormátrixot $\hat{\mathbf{G}}$ és $\widehat{\mathbf{G}^{(1)}}$ fogja jelölni. A kód elemeit egy ∞-indexű elemmel egészítjük ki úgy, hogy az $\mathbf{u}$ kódszóra $u_\infty = -y\sum_{i=0}^{p-1}u_i$ legyen az $\mathbb{F}_q$ egy y elemével. $\bar{C}$ és $\overline{C^{(1)}}$ mátrixának minden sorában az y

értékétől függetlenül $u_\infty = 0$. Az előbbiekből következik, hogy y-t a csupa e-t tartalmazó sor valamilyen tulajdonságával definiálhatjuk. Válasszuk y-t úgy, hogy $4k-1$-alakú szóhossz esetén legyen $\hat{C}$ és $\widehat{C^{(1)}}$ önortogonális, míg a másik esetben legyen a két kód egymás duálisa.

Ha $p = 4k-1$, akkor $C^\perp = \bar{C}$-ból $\bar{C} \subseteq C = \bar{C}^\perp$, vagyis $\overline{\mathbf{G}}$ bármely két sorának skalárszorzata 0. Mivel egy sor komponenseinek összege 0, ezért, mint láttuk, kiterjesztésnél az új elem is 0 lesz. Ha pedig vesszük a skalárszorzatát $\mathbf{e}^T e_\infty$-nek és $\mathbf{a}^T a_\infty = \mathbf{a}^T 0$-nak, ahol $\mathbf{a}$ a $\overline{\mathbf{G}}$ egy sora, akkor ez $\mathbf{a}^T a_\infty$ komponenseinek öszege, ami ismét 0. Az eddigiek szerint elegendő, ha a csupa e-t tartalmazó sorokat úgy egészítjük ki, hogy legyen önmagára merőleges. Ekkor a C kiterjesztésének, $\hat{C}$-nak $\widehat{\mathbf{G}}$ mátrixában bármely két sor ortogonális, következésképpen $\hat{C}$ önortogonális. De a kiterjesztett kód szóhosszúsága $p+1$, míg a dimenziója $\frac{p+1}{2}$ (mert azonos az eredeti kód, azaz C dimenziójával), és ebből következik, hogy ez a kód önduális, $\hat{C} = \hat{C}^\perp$. Az analógia alapján ismét kapjuk az adott tulajdonságokat a $g^{(1)}$-hez tartozó kódnál.

$4k+1$-alakú szóhosszúság esetén $C^\perp = \overline{C^{(1)}}$, és ekkor $\bar{C} \subseteq C = \overline{C^{(1)}}^\perp$ valamint $C^{(1)^\perp} = \bar{C}$, és innen $\overline{C^{(1)}} \subseteq C^{(1)} = \bar{C}^\perp$. Az előző esethez képest csupán annyi az eltérés, hogy most két olyan sor szorzata kell, hogy nulla legyen, ahol az utolsó komponensek kivételével mindkét sorban mindenütt e áll, és így, ha a két utolsó elem $e_\infty^{(0)}$ és $e_\infty^{(1)}$, akkor $pe + e_\infty^{(0)} e_\infty^{(1)} = 0$-t kell biztosítanunk. Ha ez teljesül, akkor most $\hat{C}^\perp = \widehat{C^{(1)}}$, ami azt is jelenti, hogy $\widehat{C^{(1)}}^\perp = \hat{C}$.

2-karakterisztikájú test esetén minden esetben mindkét mátrixban a kiegészítő elem e. Nézzük a többi esetet. Írjunk y helyett y_0-át és y_1-et úgy, hogy a $4k-1$-hez tartozó esetben legyen $y_0 = y_1$, míg a másik esetben egyikük tartozzon az egyik, a másik érték pedig a másik kódhoz. A két kódnál az utolsó sor (a kiegészítő jegy nélkül) azonos, és minden elem e, ezért a sor önmagával vett, illetve a két mátrix utolsó sorának szorzata a kiegészítéssel azonos eredményt ad, nevezetesen (az y_0 és y_1 előbbi választásával) az eredmény $pe + (-py_0)(-py_1) = p\big(e + p(y_0 y_1)\big)$. Az önortogonalitáshoz illetve a dualitáshoz ez az érték 0-t kell, hogy adjon, ami akkor és csak akkor teljesül, ha $0 = e + p(y_0 y_1) = e + (y_0 y_1)(\varepsilon\theta^2)$, azaz ha $y_0 y_1 = -\varepsilon\frac{e}{\theta^2} = \frac{\varepsilon e}{\epsilon\theta}\cdot\frac{-e}{\epsilon\theta}$. Az eredményből kiolvasható, hogy a két kódhoz tartozó y választható úgy, hogy az egyik kódnál az értéke $\frac{\varepsilon e}{\epsilon\theta} = \frac{\epsilon\theta}{pe}$, a másiknál $\frac{-e}{\epsilon\theta} = -\varepsilon\frac{\epsilon\theta}{pe}$ legyen. De ebből az is látszik, hogy ilyen választással $\varepsilon = -1$ esetén $y_0 = y_1$, ahogy azt eleve szerettük volna, míg a másik esetben $y_1 = -y_0$. ϵ-ként a két lehetséges érték bármelyikét választhatjuk, de a későbbiekben majd figyelembe kell vennünk a választást. Most már meg tudjuk adni a ∞-indexű sor ∞-indexű $-py$ elemét, ugyanis ez az előbbi eredményeknek megfelelően $-\epsilon\theta$, illetve $\varepsilon\epsilon\theta$.

Könnyen meghatározható y értéke 3-karakterisztikájú test esetében. Ekkor $p = 12k + \varepsilon$, majd ezzel $\theta^2 = \varepsilon pe = e$, $\theta = \epsilon e$, és most $y_0 = \varepsilon e$, $y_1 = -e$, és ennek megfelelően $-py$ értéke $-e$ és εe.

16.12. Tétel

Legyen C egy bináris vagy ternáris, $p = 4k-1$ szóhosszúságú kvadratikus maradékkód. Ekkor

- $q = 2$ esetén $\hat{C}$ minden szavának súlya osztható 4-gyel, míg a C-beli kódszavak súlya 0-val vagy 3-mal kongruens modulo 4;
- ha $q = 3$, akkor a kiterjesztett kód minden kódszavának súlya osztható 3-mal, míg az eredeti kód szavainak súlya 0-val vagy 2-vel kongruens modulo 3.

Δ

Bizonyítás:

Ha $q = 2$ és $p = 4k-1$, akkor $p = 8k-1$, így a kiterjesztett kód szóhosszúsága a 8 többszöröse. Most az $\bar{E}$ idempotensben a 0-, valamint a modulo p kvadratikus nemmaradékokhoz tartozó indexeknél a komponens e, a többi helyen 0. A kvadratikus nemmaradékok száma $\frac{p-1}{2} = 4k-1$, így a kiterjesztett kódban a 0-indexű sorban a nullától különböző elemek száma, tehát a kódszó súlya $4k$, és nyilván ugyanez a helyzet a többi véges indexű sorban, hiszen ezek az előbbi sor ciklikus eltoltjai. Az

utolsó sorban minden elem, tehát $p+1=8k$ elem e, ennek a sornak a súlya is osztható 4-gyel. A generátorrendszer önortogonális, és ez a tulajdonság azzal, hogy a generátorrendszer minden elemének súlya 4 többszöröse, azt eredményezi, hogy a kiterjesztett kódban minden kódszó súlya osztható 4-gyel. A kiterjesztett kódból elhagyva a kiegészítő komponenst, visszakapjuk az eredeti kódot. Ez az elhagyás a kód átszúrása, és átszúrásnál minden szó súlya vagy változatlan, vagy pontosan 1-gyel csökken, amiből következik, hogy most egy kódszó súlya vagy 4-gyel osztható (ha az átszúrás helyén 0 állt), vagy eggyel csökkent, és ekkor a 4-gyel való osztási maradék 3.

A kiterjesztett kód minden sorában $\sum_{i=0}^{p-1} a_i^2 + a_\infty^2 = 0$ a testbeli művelekkel, mert a kód önortogonális, tehát bármely sor önmagával vett skalárszorzata 0. A háromelemű testben minden nem nulla elem négyzete e, így az összeg azt jelenti, hogy a sorban található nem nulla elemek száma a 3 többszöröse, a sor súlya osztható 3-mal. Most hasonló a helyzet a bináris esethez, vagyis visszatérve az eredeti kódra, egy-egy kódszó súlya vagy változatlan, vagy eggyel csökken, tehát vagy osztható 3-mal, vagy a 3-mal való osztási maradék 2.

□

A ciklikus kódoknál foglalkoztunk a hibacsapda-dekódolással. Kvadratikus maradékkódok esetén ez a módszer az egyik legjobban alkalmazható eljárás az esetleges javítható hibaminták feltárására és korrigálására. A lényeg az volt, hogy ciklikus kód esetén a kódszavakban a szimbólumok ciklikus eltolásával ismét kódszót kapunk, és így a beérkezett szó ciklikus eltoltjainak szindrómáiból tudtunk következtetni az eredeti vett szó hibahelyeire és hibaértékeire, feltéve, hogy valamely eltolt megfelelt a dekódolási feltételnek. Ez a gondolat általánosítható, a ciklikus eltolásnál esetleg általánosabb transzformáció is alkalmazható. Korábban megfogalmaztuk a kódok ekvivalenciáját, és láttuk, hogy emlékezet nélküli, diszkrét, szimmetrikus csatornát feltételezve, minimális távolságú dekódolással a távolságtartó leképezés ekvivalens kódot eredményez. Azt is láttuk, hogy a leképezés akkor és csak akkor távolságtartó, ha kimerül a kódszavak komponenseinek olyan transzformációjában, amely a kódszón belüli sorrendjüket permutálja, valamint koordinátánként egymástól független permutáció a kód szimbólumkészletén. Két kód **permutáció-ekvivalens**, ha csupán a komponensek sorrendjének változtatásával ekvivalensek. Lineáris kód esetén távolságtartó leképezést kapunk, ha a komponensek sorrendjének permutálása mellett, az egyes koordinátahelyeken egymástól független, nem nulla elemmel szorozzuk a szó adott helyen lévő elemét. Az így végzett átalakítással kapott kódokat neveztük skalár-ekvivalensnek. Skalár-ekvivalencia helyett azt is mondjuk, hogy a két kód **monomiálisan ekvivalens**. Lineáris kód esetén minden szó minden komponensére a test azonos automorfizmusát alkalmazva lineáris kódot kapunk, és ez a leképezés is távolságtartó. Lineáris kódokat legáltalánosabban ez utóbbival együtt mondunk ekvivalensnek.

Egy adott S szimbólumhalmaz fölötti n-hosszúságú szavak halmazán az ekvivalens leképezéseket a $T=(\pi,\boldsymbol{\sigma})$ párok adják, ahol π az indexhalmaz permutációja, míg $\boldsymbol{\sigma}$ egy olyan rendezett n-es, amelynek minden komponense az S egy permutációja, és ezzel $(\mathbf{u}T)_{i\pi}=u_i\sigma_i$. A kódok ekvivalenciájának definíciója alapján ez a tulajdonság reflexív, szimmetrikus és tranzitív, tehát ekvivalencia-reláció az S^n részhalmazainak halmazán. A reflexivitást az $(\varepsilon,(\iota,\cdots,\iota,\cdots,\iota))$ pár biztosítja. A tranzitivitás azt jelenti, hogy a $T=(\pi,\boldsymbol{\sigma})$ és $T'=(\pi',\boldsymbol{\sigma}')$ ekvivalencia-leképezések kompozíciója is ilyen alakú. Valóban,

$$\big(\mathbf{u}(TT')\big)_{i(\pi\pi')}=\big((\mathbf{u}T)T'\big)_{(i\pi)\pi'}=(\mathbf{u}T)_{i\pi}\sigma'_{i\pi}=(u_i\sigma_i)\sigma'_{i\pi}=u_i(\sigma_i\sigma'_{i\pi})$$

és $\sigma_i\sigma'_{i\pi}$ is S egy permutációja, mert egy halmaz permutációinak szorzata is permutációja ugyanezen halmaznak. Végül a reláció szimmetrikussága azt jelenti, hogy T-nek van inverze. Ez könnyen megkapható az előző eredményből. Ha π' a π inverze, továbbá $\boldsymbol{\sigma}'$-ben $\sigma'_{i\pi}=\sigma_i^{-1}$, akkor $\sigma_{i\pi'}=(\sigma'_i)^{-1}$, és közvetlenül látható, hogy $\big(\mathbf{u}(TT')\big)_i=u_i=\big(\mathbf{u}(T'T)\big)_i$, így TT' és $T'T$ az identikus leképezés, a két leképezés egymás inverze.

Az előbbiekben beláttuk, hogy adott szimbólumhalmaz és adott szóhosszúság esetén az ekvivalens leképezések a

$$\big(\pi,(\sigma_0,\cdots,\sigma_i,\cdots,\sigma_{n-1})\big)\big(\pi',(\sigma'_0,\cdots,\sigma'_i,\cdots,\sigma'_{n-1})\big)=\Big(\pi\pi',\big(\sigma_0\sigma'_{0\pi},\cdots,\sigma_i\sigma'_{i\pi},\cdots,\sigma_{n-1}\sigma'_{(n-1)\pi}\big)\Big)$$

művelettel csoportot alkotnak.

Amennyiben egy C kódra alkalmazott valamely ekvivalens átalakítással az eredeti kódot kapjuk, úgy az adott transzformáció **a kód automorfizmusa**. A kód automorfizmusai az előbb adott szabállyal egy csoport, a **kód automorfizmus-csoportja**, $AUT(C)$. Azon automorfizmusok, amelyek csak a komponensek sorrendjét változtatják, részcsoportot alkotnak, ez a kód $PAUT(C)$ **permutáció-automorfizmus csoportja**. Lineáris kód esetén a monomiális leképezések is csoportot alkotnak, hiszen a test nem nulla elemeinek szorzata is a test egy nullától különböző eleme. A C lineáris kód monomiális automorfizmusainak $MAUT(C)$-vel jelölt összessége a kód **monomiális-automorfizmus csoportja**. Végül a test automorfizmusai is csoportot képeznek, így például a test bármely τ automorfizmusával $\tau^* = (\sigma'_{i\pi})^{-1}\tau\sigma'_{i\pi}$ is a test egy automorfizmusa, és így $(\sigma_i\tau)(\sigma'_{i\pi}\tau') = (\sigma_i\sigma'_{i\pi})(\tau^*\tau')$, és ez a lineáris kód automorfizmus-csoportja, $\Gamma AUT(C)$. Rögtön látható, hogy monomiálisan ekvivalens kódok ekvivalensek és permutáció-ekvivalens kódok monomiálisan ekvivalensek, $PAUT(C) \leq MAUT(C) \leq \Gamma AUT(C)$, de a fordított irány általában nem teljesül. Bináris kód esetén a három csoport egybeesik, míg prímszámelemű test esetén a két utóbbi csoport azonos. Adott kód esetén a kód összes automorfizmusának $AUT(C)$ csoportja $\Gamma AUT(C)$-nél bővebb is lehet.

Lineáris kód esetén a generátorrendszer elemein végrehajtott fenti átalakítások a teljes kód megfelelő átalakítását eredményezik. n-szóhosszúságú kódnál a koordináták permutációját egy n-edrendű permutációs mátrixszal jobbról való szorzással kapjuk, azaz olyan mátrixszal, amelynek minden sorában és minden oszlopában pontosan egy nem nulla elem áll, amely e. A mátrix inverze a mátrix transzponáltja. Monomiális transzformáció monomiális mátrixszal jobbról való szorzással kapható. Az n-edrendű mátrix monomiális, ha minden sorában és minden oszlopában egy és csak egy nem nulla elem van. Minden ilyen mátrix felírható egy diagonálmátrix és egy permutációs mátrix szorzataként, mégpedig bármely sorrendű szorzataként (de a két esetben a diagonálmátrix különböző lehet). A szokásos esetben a diagonálmátrixot a permutációs mátrix bal oldalára írjuk. Nullától különböző elemek diagonálmátrixának inverze diagonálmátrix, ahol az átlóban az eredeti elem inverze található. Ezzel már a monomiális mátrix inverzét is megkapjuk, ám most a diagonális rész a permutációs rész jobb oldalán van. Ezt könnyen átvihetjük a másik oldalra, mert csak azt kell megnézni, hogy a szorzatmátrix egyes soraiban milyen egyetlen nem nulla elem áll.

Ha C n szóhosszúságú ciklikus kód, akkor $PAUT(C)$, és így $\Gamma AUT(C)$ biztosan tartalmazza az $i \mapsto (i+1) \bmod n$ leképezést, hiszen ez nem más, mint a ciklikusság definíciója. Most a kvadratikus maradékkódokhoz meghatározunk egy bővebb monomiális automorfizmus-csoportot.

Tekintsük a $\mathcal{K}$ test elemein az $u \mapsto \frac{au+b}{cu+d}$ hozzárendelést a K-beli a, b, c és d elemekkel. Az rögtön látható, hogy ha egy u-ra értelmezett a leképezés, akkor a képelem is K eleme, továbbá ha egy u képe v, akkor $u = \frac{dv+(-b)}{(-c)v+a}$, az inverz leképezés hasonló alakú, mint az eredeti megfeleltetés.

Ha c és d egyaránt a test nulleleme, akkor a nevező a test minden u eleme esetén 0, és ekkor vagy minden u-ra a leképezés nem értelmezett ($a = 0 = b$ esetén), vagy legfeljebb egyetlen u kivételével $\frac{au+b}{cu+d} = \frac{z}{0}$, ahol $z \neq 0$, míg az esetleges egyetlen kivételes pontban ($a \neq 0$-nál a $-\frac{b}{a}$ pontban) ismét $\frac{0}{0}$-alakú a leképezés, vagyis ez esetben sincs sehol értelmezve a megfeleltetés. Ennek megfelelően ki kell kötnünk, hogy c és d legalább egyike nem nulla.

Elsőként legyen $c = 0$. Ekkor, az előzőeknek megfelelően, $d \neq 0$, és $\frac{au+b}{cu+d} = \frac{a}{d}u + \frac{b}{d}$. Ez a test minden elemén értelmezett, és könnyen ellenőrizhetően injektív és szürjektív, tehát bijektív leképezése a testnek önmagára, ha $a \neq 0$, míg $a = 0$ esetén minden u képe $\frac{b}{d}$, a leképezés ez esetben nem injektív és nem szürjektív. Most $a = 0$ akkor és csak akkor, ha $ad - bc = 0$.

Nézzük a $c \neq 0$ esetet. Nyilván most a függvény a $-\frac{d}{c}$ pontban és csak ebben a pontban nincs értelmezve, függetlenül a többi paraméter értékétől. Átalakítjuk a kifejezést (a test egységelemét a szokásnak megfelelően e-vel jelölve):

$$\frac{au+b}{cu+d} = \frac{e}{c}\frac{c(au+b)}{cu+d} = \frac{e}{c}\frac{a(cu+d)+(bc-ad)}{cu+d} = \frac{a}{c} + \frac{e}{c^2}\frac{bc-ad}{u+\frac{d}{c}} = r + s^2\frac{-\Delta}{u+t},$$

ahol $r = \frac{a}{c}$, $s = \frac{e}{c}$, $t = \frac{d}{c}$ és $\Delta = ad - bc$. Kételemű test esetén az értelmezési tartomány egyetlen pontja $e + d$, és ebben a pontban a függvény értéke $a + \Delta$, ami a, ha $\Delta = 0$, különben $a +$ e. Nézzük a többi esetet.

$\Delta = 0$ esetén az értelmezési tartomány minden elemének képe azonos, így a leképezés nem injektív, ezért nem invertálható. Az érdekesebb és fontosabb $\Delta \neq 0$ esetben a leképezés injektív, továbbá a képhalmaz a test egyetlen pontját nem tartalmazza, $r = \frac{a}{c}$-t, így a függvény $v \mapsto \frac{dv+(-b)}{(-c)v+a}$ inverze ezen egyetlen ponttól eltekintve mindenütt létezik. A hasonlóság alapján az inverz azonos tulajdonságokkal rendelkezik, mint az eredeti leképezés, ugyanis $ad - bc$-nek most $ad - (-b)(-c)$ felel meg, és ez a két kifejezés azonos.

A $c = 0$ és $c \neq 0$ esetet együtt tekintve látjuk, hogy mindkét esetben $ad - bc$ a vízválasztó (leszámítva a kételemű testet). A lényeges $ad - bc \neq 0$ esetén a leképezés mindig tartalmaz $u \mapsto u + p$ alakú eltolást (amely speciális esetben lehet a helybenhagyás is) és $u \mapsto zu$ alakú leképezést (amely ismét lehet helybenhagyás), és ha $c \neq 0$, akkor még $u \mapsto u^{-1}$ alakú megfeleltetést. Ezen utolsó leképezés egy pontban nincs értelmezve. Bővítsük K-t egy új, ∞-nel jelölt szimbólummal, és részlegesen a műveleteket is értelmezzük ezen elemre: $\frac{e}{0} = \infty$, $\frac{e}{\infty} = 0$, $a + \infty = \infty = \infty + a$ tetszőleges $a \in K$-val, és $a \neq 0$ esetén $a \cdot \infty = \infty = \infty \cdot a$. Az előbbiekből természetesen adódik az is, hogy bármely $a \neq 0$-val $\frac{a}{0} = \infty$ és $\frac{a}{\infty} = 0$, és $\frac{au+b}{cu+d} = r + s^2 \frac{-\Delta}{u+t}$-ből pedig (ha $\Delta \neq 0$), hogy $\frac{a\cdot\infty+b}{c\cdot\infty+d} = \frac{a}{c}$. Ezzel a kiterjesztéssel már, feltéve, hogy $ad - bc \neq 0$, a leképezés értelmezési tartománya a teljes kibővített test, a leképezés bijekció magára a kibővített testre, és ennek megfelelően az inverz leképezés is létezik ugyanilyen tulajdonságokkal (sőt, maga az inverz lényegében véve azonos az eredeti leképezésekkel, csupán más paraméterekkel). A 0 képe $\frac{b}{d}$, míg ∞ az $\frac{a}{c}$-re képződik; $-\frac{b}{a}$ képe a 0, végül $-\frac{d}{c}$ megy át a ∞-be.

Ha a $K \cup \{\infty\}$-t $\overline{K}$ jelöli, akkor az előbbiek szerint az $u \mapsto \frac{au+b}{cu+d}$ szabály az $ad - bc \neq 0$ feltétellel a $\overline{K}$ egy permutációja, és két ilyen permutáció kompozíciója is megadható ilyen alakban (a, b, c és d továbbra is K elemei). Valóban,

$$\frac{au+b}{cu+d} \circ \frac{a'u+b'}{c'u+d'} = \frac{a\frac{a'u+b'}{c'u+d'} + b}{c\frac{a'u+b'}{c'u+d'} + d} = \frac{(aa'+bc')u + (ab'+bd')}{(ca'+dc')u + (cb'+dd')} = \frac{\tilde{a}u+\tilde{b}}{\tilde{c}u+\tilde{d}},$$

és itt a', b', c' és d' valamint $\tilde{a}$, $\tilde{b}$, $\tilde{c}$ és $\tilde{d}$ szintén K eleme.

Egy A halmaz összes permutációja a kompozícióval csoportot alkot. Ennek egy részcsoportja egy pozitív egész k-val k-**szorosan tranzitív**, ha A bármely $(a_1, \cdots, a_i, \cdots a_k)$ és $(b_1, \cdots, b_i, \cdots b_k)$ rendezett k-asához van a csoportban olyan π permutáció, hogy $\pi(a_i) = b_i$ minden $1 \leq i \leq k$-ra. σ háromszorosan tranzitív. Ehhez elegendő belátni, hogy a $\overline{K}$ bármely, páronként különböző u, v és w eleméhez van olyan a, b, c és d elem K-ban, amellyel $ad - bc \neq 0$, és a $z \mapsto \frac{az+b}{cz+d}$ szabály az adott három elemhez a 0, e, ∞ elemeket rendeli az előbb megadott sorrendben. Ehhez az

$$\begin{aligned} ua + b &= 0 \\ va + b &= vc + d \\ wc + d &= 0 \end{aligned}$$

egyenleteknek kell teljesülniük. Külön kell nézni azt az esetet, amikor az u, v, w valamelyike (és a feltételhez illeszkedően legfeljebb csak az egyike) a ∞. $\infty \cdot a + b = 0$ csak úgy lehet, ha $a = 0$, és ekkor $ad - bc \neq 0$-ból $b \neq 0 \neq c$. Most tetszőleges $0 \neq c$-vel már egyértelműen kapjuk b és d értékét. Ehhez hasonló a helyzet, ha $w = \infty$, csupán felcserélődik a és c szerepe. Végül, ha a ∞ képe e, akkor a második egyenletből $a = c \neq 0$, és tetszőleges, nullától különböző a-t választva megkapjuk b és d értékét.

Ha u, v és w mindegyike K-beli, akkor a fenti egyenletrendszernek az $ad - bc \neq 0$ feltételt kielégítő megoldása pontosan akkor van, ha az

$$\begin{aligned} ua + eb &= 0 \\ va + eb + (-v)c + (-e)d &= 0 \\ wc + \quad ed &= 0 \end{aligned}$$

homogén lineáris egyenletrendszer van nemtriviális megoldása. Az egyenletek száma kisebb, mint az ismeretleneké, így van nemtriviális megoldás. Egy nemtriviális megoldásban $ad - bc \neq 0$. Ellenkező esetben ugyanis $(ac)u = -bc = -ad = (ac)w$, és innen a és c legalább egyike 0. Ha $a = 0$, akkor $ua + b = 0$ miatt $b = 0$, és ha a és b egyaránt 0, akkor $vc + d$ is 0. De így $vc = wc$, tehát c, és vele együtt d is nulla, ám ez a triviális megoldás lenne. $c = 0$-val hasonló eredményre jutnánk.

Az 1., 2. és 4. oszlop együtthatóiból álló determináns értéke $u - v$, míg a 2., 3. és 4. oszlop együtthatóiból állóé $w - v$, és ezek egyike sem nulla, ezért egyetlen szabad érték van. Ekkor a c illetve az a értéke (de csak az egyiké) szabadon választható, továbbá, ha egy adott a, b, c és d az előbbi egyenletrendszer egy megoldása, akkor az összes megoldás $\lambda a, \lambda b, \lambda c$ és λd a test egy tetszőleges λ elemével. Az eredmények azt mutatják, hogy ez a transzformáció legalább háromszorosan tranzitív. De négyszeresen már nem (ez nyilvánvaló, ha $\overline{K}$-nak három eleme van, azaz K a kételemű test), ugyanis tetszőleges $\lambda \neq 0$-val és $z \in K$-val $\frac{(\lambda a)z+(\lambda b)}{(\lambda c)z+(\lambda d)} = \frac{az+b}{cz+d}$, így egy negyedik, az első három mindegyikétől különböző pontot már nem tudjuk a kibővített test tetszőleges pontjára leképezni.

Láttuk, hogy $ad - bc \neq 0$ az alapmegoldásnál. $(\lambda a)(\lambda d) - (\lambda b)(\lambda c) = \lambda^2(ad - bc) = \lambda^2\Delta$, ahol $\Delta = ad - bc$. Ha Δ a test valamely t elemének négyzete, akkor ezen t elem inverzével mint λ-val $(\lambda a)(\lambda d) - (\lambda b)(\lambda c) = \lambda^2\Delta = e$, megválasztható tehát a négy paraméter, hogy $ad - bc = e$ legyen. Ha a $\mathcal{K}$ testben minden elemnek van négyzetgyöke, akkor ez mindig lehetséges, vagyis ekkor a $\overline{K}$ bármely, adott sorrendben megadott három különböző pontja átvihető szintén tetszőleges három, páronként különböző pontjába olyan leképezéssel, amelynél teljesül még az $ad - bc = e$ feltétel. Ilyen test például $\mathbb{C}$, vagy bármely 2-karakterisztikájú test, tehát bármely páros számú, azaz 2-hatvány számú elemet tartalmazó test, más véges test esetén azonban nem ez a helyzet. Az $a = e = d$, $b = 0 = c$ választással $z \mapsto \frac{az+b}{cz+d}$ az identikus leképezés, és ezekkel a paraméterekkel $\Delta = e$. Az is könnyen ellenőrizhető, hogy a $\Delta = e$ feltételt kielégítő $z \mapsto \frac{az+b}{cz+d}$ leképezések kompozíciója, valamint egy ilyen leképezés inverze is ilyen tulajdonságú, így bármely test esetén az ilyen leképezések a kompozícióval csoportot alkotnak.

A fenti egyenletrendszer egy lehetséges megoldása, ha például a-t választjuk paraméternek:

$$\begin{aligned} b &= -ua \\ c &= -\frac{u - v}{v - w}a \\ d &= w\frac{u - v}{v - w}a, \end{aligned}$$

és ezzel

$$\Delta = ad - bc = \frac{(u - v)(w - u)}{v - w}a^2.$$

Látható, hogy ha a három adott pont közül bármely kettőt felcseréljük, akkor Δ egy négyzetelem ellentettjével szorzódik. Ha a testben $-e$-nek van négyzetgyöke, akkor az adott három pont minden permutációja esetén egységesen vagy van az aktuális Δ-nak (az adott testben) négyzetgyöke, vagy egyik esetben sincs, míg ha $-e$ nem kvadratikus az adott testben, akkor ha egy adott sorrend mellett van Δ-nak négyzetgyöke, akkor a pontok páros permutációjánál lesz négyzetgyök, míg páratlan permutáció esetén (vagyis két pont felcserélésénél) nem lesz. Azt közvetlen behelyettesítéssel és kis átalakítással láthatjuk, hogy kompozíciónál a Δ-k szorzódnak, a kvadratikusság szorzattartó, így az inverz transzformációhoz tartozó Δ is a négyzetgyök szempontjából hasonló tulajdonságú, mint az eredeti, hiszen az identikus leképezéshez tartozó Δ biztosan négyzetelem. A valós test esetén könnyű látni, hogy akkor és csak akkor lehet $+1$-re normálni Δ-t, ha ciklikusan tekintve a pontokat, a három pont ugyanolyan sorrendben követi egymást, mint a megfelelő képpontok. Ekkor ugyanis $u < v < w$-vel és $u' < v' < w'$-vel $u \mapsto 0$, $v \mapsto$

$e, w \mapsto \infty$-nél $\Delta > 0$, és hasonlóan, az $u' \mapsto 0$, $v' \mapsto e$, $w' \mapsto \infty$ transzformációnál $\Delta' > 0$. De ekkor az elsőként megadott transzformáció és a második inverze u-t u'-be, v-t v'-be és w-t w'-be viszi.

Ha a $\mathcal{K}$ testben nem mindegyik elem négyzete a test egy elemének, akkor a $\Delta = e$ feltételt kielégítő $u \mapsto \frac{au+b}{cu+d}$ leképezések csoportja, mint láttuk, nem lesz háromszorosan tranzitív, de kétszeresen igen. Ehhez ugyanis csak az kell, hogy két különböző u és w elemhez legyen olyan a, b, c és d, amellyel $ua + b = 0$, $wc + d = 0$ és $ad - bc = e$. Ha most a és c a test tetszőleges nem nulla elemei, akkor $d = -wc$, $b = -ua$, $ad - bc = (-ac)w - (-ac)u = -(ac)(w - u)$, és például $a = -(w - u)^{-1}$-et és $c = e$-t választva már olyan paramétereket kapunk, amelyekre teljesül a normálási feltételünk.

$\Delta = e$ esetén $c = 0$-nál a transzformáció $u \mapsto \frac{a}{d}u + \frac{b}{d} = \frac{e}{d^2}u + \frac{b}{d} = s^2u + b'$, vagyis a szorzás most is a test egy elemének négyzetével történik. Ha tehát $\Delta = e$, akkor minden esetben a transzformációt megkapjuk eltolásból, a test egy kvadratikus elemével való szorzásból, valamint esetleg még egy $u \mapsto -\frac{e}{u}$ alakú leképezésből.

16.13. Definíció

Legyen $\mathcal{K}$ test, ∞ a K-hoz nem tartozó szimbólum, $\overline{K} = K \cup \{\infty\}$, K-beli u-val $u + \infty = \infty = \infty + u$, $\frac{u}{\infty} = 0$, $\frac{\infty}{u} = \infty$, és $u \neq 0$ esetén $u \cdot \infty = \infty = \infty \cdot u$. Ekkor a K-beli a, b, c, d és $\overline{K}$-beli v elemekkel, ahol $\Delta = ad - bc \neq 0$, a $v \mapsto \frac{av+b}{cv+d}$ leképezések összessége a $\mathcal{K}$ feletti **másodrendű projeketív lineáris csoport**, amelyet $PL_2(K)$, illetve q-elemű test esetén $PL_2(q)$ jelöl. A $\Delta = e$ feltételnek megfelelő leképezések halmaza, ahol e a test egységeleme, a $\mathcal{K}$ feletti **másodrendű projeketív speciális lineáris csoport**, és ezt $PSL_2(K)$ illetve $PSL_2(q)$ jelöli.

Δ

Fentebb már bizonyítottuk az alábbi tétel jórészét.

16.14. Tétel

$PL_2(K)$ minden eleme a $\overline{K}$ önmagára való bijekciója, és a kompozícióval mint binér művelettel csoportot alkot, amely háromszorosan tranzitív. $PSL_2(K)$ az előbbi csoport egy részcsoportja. Ez háromszorosan tranzitív, ha K-ban minden elem négyzetelem, ellenkező esetben kétszeresen tranzitív.

$PL_2(K)$ elemei az alábbi három típusú, $PL_2(K)$-beli transzformációk kompozíciói:

$$T_t: u \mapsto u + t$$
$$R_r: u \mapsto ru$$
$$V: u \mapsto -\frac{e}{u}$$

K-beli t és r elemekkel és a test e egységelemével. $PSL_2(K)$-beli leképezéseknél $r = s^2$, ahol s is K eleme. Amennyiben K prímszámelemű test, akkor az $u \mapsto u + t$ **eltolás**ok előállnak az $u \mapsto u + e$ eltolások kompozíciójaként.

Δ

Bizonyítás:

Már csak a transzformációk előállítására vonatkozó részt kell bizonyítani.

$c = 0$ esetén a transzformáció $u \mapsto \frac{au+b}{d} = \frac{a}{d}\left(u + \frac{b}{a}\right)$, ugyanis $0 \neq \Delta = ad - bc = ad$, tehát $a \neq 0$. Most $\frac{au+b}{d} = \left(\frac{a}{d}u\right) \circ \left(u + \frac{b}{a}\right) = \left(R_{\frac{a}{d}} \circ T_{\frac{b}{a}}\right)(u)$. Általános esetben $\frac{au+b}{cu+d} = \frac{a}{c} + \frac{ad-bc}{c^2} \cdot \frac{-e}{u+\frac{d}{c}}$, és ez $\left(u + \frac{a}{c}\right) \circ \left(\frac{\Delta}{c^2}u\right) \circ \left(-\frac{e}{u}\right) \circ \left(u + \frac{d}{c}\right) = \left(T_{\frac{a}{c}} \circ R_{\frac{\Delta}{c^2}} \circ V \circ T_{\frac{d}{c}}\right)(u)$.

Ha $\Delta = e$, akkor $\frac{\Delta}{c^2} = \frac{e}{c^2} = \frac{e^2}{c^2} = \left(\frac{e}{c}\right)^2 = s^2$, míg $\mathcal{K} = \mathbb{F}_p$ esetén, ahol p prímszám, a test additív csoportja is ciklikus, amelyet e generál, így a test bármely t elemére $t = ke$, ahol $p > k \in \mathbb{N}$.

□

Mivel számunkra nincs jelentősége, ezért nem bizonyítjuk, csak megemlítjük, hogy $PL_2(\mathbb{C})$ körtartó, ahol az egyenest egy végtelen sugarú, a végtelenben lévő középpont körüli körnek tekintünk.

Az $\mathbb{F}_q$ fölötti n-szóhosszúságú C lineáris kód esetén $MAut_{Pr}(C) = \{P | M = DP \in MAut(C)\}$, ahol P egy n-edrendű permutációs mátrix és D ugyanilyen rendű diagonálmátrix. Az előbbihez hasonló definícióval $\Gamma Aut_{Pr}(C) = \{P | M\gamma = DP\gamma \in \Gamma Aut(C)\}$, és itt γ a q-elemű test automorfizmusa. Azt mondjuk, hogy $MAut(C)$ tranzitív, ha $MAut_{Pr}(C)$ tranzitív, illetve $\Gamma Aut(C)$ tranzitív, amennyiben tranzitív a $\Gamma Aut_{Pr}(C)$ csoport. Az nyilvánvaló, hogy $PAut(C) \leq MAut_{Pr}(C) \leq \Gamma Aut_{Pr}(C)$, és amennyiben ezek bármelyike tranzitív, akkor az őt tartalmazó csoport(ok) is tranzitív(ak).

Megmutatjuk, hogy 2-nél nagyobb p szóhosszúságú kvadratikus maradékkód esetén az indexhalmaz $PSL_2(p)$ elemeivel való transzformációja, páratlan karakterisztika esetén kiegészítve a kód egyes indexekhez tartozó komponenseinek $\pm e$-val való szorzásával, automorfizmusa a kiterjesztett kódnak, vagyis páros elemszámú testnél ez permutáció-automorfizmus, míg a többi esetben monomiális automorfizmus. Másként mondva $PSL_2(p) \leq MAut_{Pr}(C)$, így a kód automorfizmus-csoportja tranzitív.

Az eltolás a ∞-indexű elemet nem érinti, a többi komponensből álló szó az eredeti kód eleme, és az eltolás C-beli elemet C egy elemébe viszi, mert a kód ciklikus. A kiegészítő jegy értéke a ciklikus eltolással nem változik, így az eltolás a kiterjesztett kód minden szavát ezen kód egy kódszavába tolja, az eltolás automorfizmusa a kiterjesztett kódnak.

Az indexek szorzása ismét nem érinti a kiterjesztésnél kapott elemet, az egyrészt helyben marad, másrészt nem változik az értéke, és helyben marad a 0-indexű elem is. Kvadratikus elemmel való szorzás kvadratikus maradékot kvadratikus maradékba, nemmaradékot nemmaradékba visz, így a kód idempotense nem változik, de ekkor a kód maga is immunis az ilyen transzformációval szemben.

Még azt kell belátni, hogy a V-típusú transzformáció, egyes komponensek esetleges szorzásával, szintén automorfizmusa a kódnak. Definiáljuk az ilyen átalakításokat.

16.15. Definíció

Legyen $\varepsilon \in \{1, -1\}$-gyel $p = 4k + \varepsilon$ prímszám, $\epsilon \in \{1, -1\}$, χ az $\mathbb{F}_p$ feletti kvadratikus karakter és $p \nmid q$ egy prímszám pozitív egész kitevős hatványa. Az $\mathbb{F}_q$ fölötti $p + 1$-dimenziós tér vektorainak komponenseit a $\{j \in \mathbb{N} | j < p\} \cup \{\infty\}$ halmaz elemeivel indexeljük, és az indexekkel $\mathrm{modulo}\, p$ számolunk (figyelembe véve a ∞-re adott szabályokat). Ha $c_0 = \epsilon e$, $p > j \in \mathbb{N}^+$-ra $c_j = \chi(j)e$ és $c_\infty = \varepsilon\epsilon e$, továbbá $u_0 \cdots u_i \cdots u_{p-1}u_\infty = \mathbf{u} \in \mathbb{F}_q^{p+1}$, akkor a $v_0 = c_\infty u_\infty$, $v_{-\frac{1}{j}} = c_j u_j$ $(p > j \in \mathbb{N}^+)$ és $v_\infty = c_0 u_0$ komponensekkel a $v_0 \cdots v_i \cdots v_{p-1}v_\infty = \mathbf{v} \in \mathbb{F}_q^{p+1}$ vektor az **u Gleason-Prange permutáltja**, és az így adott leképezés a **Gleason-Prange permutáció**. A permutációt $\mathcal{GP}$-vel, az $\mathbf{u}$ képét $\mathcal{GP}(\mathbf{u})$-val jelöljük.

Δ

16.16. Megjegyzés

Páros q esetén $\mathbb{F}_q$ minden u elemére $-u = u$, és így $c_j = e$ minden $\{j \in \mathbb{N} | j < p\} \cup \{\infty\}$ indexre.

Δ

16.17. Tétel

A 16.15. Definíció szerinti $\mathbf{u}$ vektorra $\mathcal{GP}^2(\mathbf{u}) = \mathcal{GP}\big(\mathcal{GP}(\mathbf{u})\big) = \varepsilon\mathbf{u}$.

Δ

Bizonyítás:

Legyen $\mathcal{GP}(\mathbf{u}) = \mathbf{v}$ és $\mathcal{GP}^2(\mathbf{u}) = \mathbf{w}$, ekkor $\mathbf{w} = \mathcal{GP}(\mathbf{v})$. Ezzel $w_0 = c_\infty v_\infty = c_\infty(c_0 u_0) = (c_\infty c_0)u_0 = (\varepsilon\epsilon e)(\epsilon e)u_0 = \varepsilon u_0$, $w_\infty = c_0 v_0 = c_0(c_\infty u_\infty) = (c_0 c_\infty)u_\infty = \varepsilon u_\infty$, valamint, figyelembe véve, hogy $\chi\left(-\frac{1}{j}\right) = \varepsilon\chi(j)$, azaz $\chi\left(-\frac{1}{j}\right)\chi(j) = \varepsilon$ és $-\frac{1}{-\frac{1}{j}} = j$, kapjuk, hogy a $p > j \in \mathbb{N}^+$ indexekre $w_j = c_{-\frac{1}{j}} v_{-\frac{1}{j}} = c_{-\frac{1}{j}}(c_j u_j) = \left(c_{-\frac{1}{j}} c_j\right) u_j = \left(\chi\left(-\frac{1}{j}\right) e\right)(\chi(j)e)u_j = \varepsilon u_j$, azaz **w** minden komponense az **u** megfelelő komponensének ε-szorosa, és így **w** is az **u** ε-szorosa.

□

16.18. Következmény

A Gleason-Prange permutáció $\mathbb{F}_q^{p+1}$ involúciója vagy egy involúció ellentettje.

Δ

Bizonyítás:

Egy $f: A \to A$ leképezés involúció, ha a négyzete a halmaz önmagára való identikus leképezése.

□

Megmutatjuk, hogy kvadratikus maradékkód Gleason-Prange permutációja automorfizmusa a kódnak. A tétel előtt még definiáljuk a Gleason-Prange-feltételt.

16.19. Definíció

Legyen p páratlan prímszám és $u_0 \cdots u_i \cdots u_{p-1} = \mathbf{u} \in \mathbb{F}_q^p$, ahol $p \nmid q$. Az **u** Fourier-spektruma kielégíti a **Gleason-Prange feltételt**, ha az $\mathbf{U} = U_0 \cdots U_j \cdots U_{p-1}$ diszkrét Fourier-transzformáltban vagy minden $j \in Q$-ra vagy valamennyi $j \in NQ$-ra $U_j = 0$.

Δ

16.20. Tétel

Legyen $p = 4k + \varepsilon$ prímszám $\varepsilon \in \{1, -1\}$-gyel, $C \leq \mathbb{F}_q$ p-szóhosszúságú kvadratikus maradékkód, $\hat{C}$ a kiterjesztett kód úgy, hogy az $a_0 \cdots a_i \cdots a_{p-1}a_\infty$ kódszóban $a_\infty = -y\sum_{i=0}^{p-1} a_i$ az $y = \frac{\epsilon\theta}{pe}$ jelöléssel, ahol $\epsilon \in \{1, -1\}$ és $\theta^2 = \varepsilon pe$. Ekkor a Gleason-Prange permutáció automorfizmusa a kódnak.

Δ

Bizonyítás:

Elegendő a generátorrendszer elemeit nézni, mert a transzformáció monomiális. A generátorrendszer elemei egyrészt a $\bar{C}$ idempotense eltoltjainak, másrészt a csupa e-t tartalmazó szónak a kierjesztései. Ezeket mint sorvektorokat egy mátrixba írtuk. Ennek a mátrixnak összesen $p + 1$ sora van, R_0-tól R_{p-1}-ig az idempotens eltoltjainak sorai, és R_∞ az e-k sora. Az i-indexű sor j indexű eleme, ahol az eredeti elemek indexe $p > j \in \mathbb{N}$, és a kiegészítő jegy a ∞-jelű indexhez tartozik, $a_{i,j}$. Véges i index esetén $a_{i,\infty} = 0$, míg $a_{\infty,\infty} = -py = -\epsilon\theta$.

Kvadratikus maradékok illetve nemmaradékok szorzata maradék, míg egy maradék és egy nemmaradék szorzata nemmaradék. Ebből következik, hogy $\chi(ij) = \chi(i)\chi(j)$, ahol χ egy $\mathrm{modulo}\, p$ kvadratikus karakter. Mivel 1 maradék, ezért i és $\frac{1}{i}$ azonos tulajdonságú, tehát $\chi\left(\frac{1}{i}\right) = \chi(i)$, másrészt $\chi(-i) = \chi(-1)\chi(i) = \varepsilon\chi(i)$, mert -1 pontosan akkor maradék, ha $p = 4k + 1$, azaz amikor $\varepsilon = +1$.

Elsőként legyen q páros. A ∞-indexű sor minden eleme e, így ez a sor nem változik, a transzformáció után is eleme a kódnak. Véges i és j index esetén $a_{i,i+j} = a_{0,j}$ (az indexet mindenütt $\mathrm{modulo}\, p$

számoljuk, ezt nem fogjuk külön jelezni), és $\psi(\mathbf{a}_i)_0 = a_{i,\infty} = 0$, $\psi(\mathbf{a}_i)_\infty = a_{i,0} = a_{0,-i}$, és a többi indexnél $\psi(\mathbf{a}_i)_{-\frac{1}{i+j}} = a_{i,i+j} = a_{0,j}$. $a_{0,0} = 0$, ha $\varepsilon = 1$ és $a_{0,0} = e$, ha $\varepsilon = -1$. Ez azt jelenti, hogy a 0-indexű sorban a két szélső elem helyére önmaga kerül, ha $\varepsilon = 1$, míg a másik esetben felcserélődik. De hasonló a helyzet az összes többi pozíción is, ugyanis $-\frac{1}{i}$ kvadratikusság szempontjából azonos i-vel poztiív ε-nál, míg eltérő a másik esetben. Ez azt jelenti, hogy R_0 transzformáltja önmaga az első esetben, míg a másik esetben R_0+R_∞= $\psi(R_0)$, vagyis $\psi(R_0)$ eleme a kódnak. Nézzük a többi esetet.

Tekintsük a $-\frac{1}{i}$-indexű sort is. A ∞-indexű elem most is 0, $a_{-\frac{1}{i},0} = a_{0,\frac{1}{i}}$, és $a_{-\frac{1}{i},j} = a_{0,\frac{1}{i}+j}$ minden más j-nél. Megmutatjuk, hogy $\psi(R_i) = R_0 + R_{-\frac{1}{i}}$, ha $\varepsilon = \chi(i)$ és $\psi(R_i) = R_0 + R_{-\frac{1}{i}} + R_\infty$, ha ε és $\chi(i)$ ellentétes előjelű (χ most is a modulo p kvadratikus karakter). A 0-, ∞-, $-\frac{1}{i}$ és $-\frac{1}{i+j}$-indexű pozíciókat nézzük, ahol $0 \neq j \neq (-i) \bmod p$. A tájékozódásban segít az 1. táblázat. Itt figyelembe vettük, hogy $\frac{1}{i}$ pontosan akkor maradék, amikor i, valamint azt, hogy $a_{-\frac{1}{i},-\frac{1}{i+j}} = a_{0,\frac{1}{i}-\frac{1}{i+j}}$ és $\frac{1}{i} - \frac{1}{i+j} = \frac{j}{i(i+j)}$.

	0	j	i	$i+j$	$-\frac{1}{i}$	$-\frac{1}{i+j}$	∞
R_0	$a_{0,0}$	$a_{0,j}$			$a_{0,-i}$	$a_{0,-(i+j)}$	0
R_i	$a_{0,-i}$		$a_{0,0}$	$a_{0,j}$			0
$\psi(R_i)$	0				$a_{0,0}$	$a_{0,j}$	$a_{0,-i}$
$R_{-\frac{1}{i}}$	$a_{0,i}$				$a_{0,0}$	$a_{0,ij(i+j)}$	0
R_∞	e				e	e	e

1. táblázat

$\psi(R_i)$ csak akkor lehet eleme a kódnak, ha a generátormátrix sorainak lineáris kombinációja. Amennyiben a ∞-indexű komponense nem 0, akkor R_∞ nem nulla együtthatóval kell, hogy álljon ebben a kombinációban, és mivel $a_{0,-i}$ csak 0 és e lehet, ezért ekkor ez az együttható e. $a_{0,-i}$ akkor és csak akkor 0, ha vagy $\varepsilon = +1$ és i kvadratikus maradék, vagy $\varepsilon = -1$ és i kvadratikus nemmaradék. Ez esetben $R = R_0 + \psi(R_i) + R_{-\frac{1}{i}}$-t, míg az ellenkezőben $R + R_\infty$-t fogjuk vizsgálni. Az összegben a ∞-indexű komponens ennek megfelelően mindig 0.

$R_0 + \psi(R_i) + R_{-\frac{1}{i}}$-ben a 0-indexű komponens $a_{0,0} + 0 + a_{0,i} = a_{0,0} + a_{0,i}$, a $-\frac{1}{i}$-hez tartozó érték $a_{0,-i} + a_{0,0} + a_{0,0} = a_{0,-i}$, és mindkettő ismét akkor és csak akkor 0, amikor $\varepsilon = \chi(i)$.

Maradt a $-\frac{1}{i+j}$-indexű oszlop $-i$-től és 0-tól különböző j-vel. Ebben az oszlopban a véges indexű sorokban álló elemek összege $a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)}$. $a_{0,-(i+j)} = a_{0,ij(i+j)}$ akkor és csak akkor, amikor $\varepsilon = \chi(-1) = \chi(ij) = \chi(i)\chi(j)$. A 2. táblázatból látható, hogy ezúttal is pontosan akkor 0 az említett három sorban az adott oszlop elemeinek összege, amikor $\varepsilon = \chi(i)$. Ezzel beláttuk, hogy az i-edik sor transzformáltja $R_0 + R_{-\frac{1}{i}}$ ebben az esetben, és $R_0 + R_{-\frac{1}{i}} + R_\infty$ a másik esetben, vagyis minden esetben a generátormátrix sorainak lineáris kombinációja, következésképpen eleme a kódnak.

ε	$\chi(i)$	$\chi(j)$			
1	1	1	$a_{0,-(i+j)} = a_{0,ij(i+j)}$	$a_{0,j} = 0$	$a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)} = 0$
1	1	−1	$a_{0,-(i+j)} \neq a_{0,ij(i+j)}$	$a_{0,j} = e$	$a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)} = 0$
1	−1	1	$a_{0,-(i+j)} \neq a_{0,ij(i+j)}$	$a_{0,j} = 0$	$a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)} = e$
1	−1	−1	$a_{0,-(i+j)} = a_{0,ij(i+j)}$	$a_{0,j} = e$	$a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)} = e$
−1	1	1	$a_{0,-(i+j)} \neq a_{0,ij(i+j)}$	$a_{0,j} = 0$	$a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)} = e$
−1	1	−1	$a_{0,-(i+j)} = a_{0,ij(i+j)}$	$a_{0,j} = e$	$a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)} = e$
−1	−1	1	$a_{0,-(i+j)} = a_{0,ij(i+j)}$	$a_{0,j} = 0$	$a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)} = 0$
−1	−1	−1	$a_{0,-(i+j)} \neq a_{0,ij(i+j)}$	$a_{0,j} = e$	$a_{0,-(i+j)} + a_{0,j} + a_{0,ij(i+j)} = 0$

2. táblázat

Ezek után következik a páratlan elemszámú test.

A $p = 4k + \varepsilon$ prím a kódszavak hossza, ahol $\varepsilon \in \{1, -1\}$, és az indexekkel $\mathrm{modulo}\, p$ számolunk. A transzformációnál a 0-indexű elem c_0-szorosa a végtelen indexű helyre, a végtelen indexű elem c_∞-szerese a 0-indexű helyre, míg $i + j \neq 0$ esetén az $i + j$-indexű helyen lévő elem c_{i+j}-szerese a $-\frac{1}{i+j}$-indexű helyre kerül (mindenütt $\mathrm{modulo}\, p$ értve a véges indexeket).

	0	j	$-\frac{1}{j}$	∞
R_0	$\frac{(p-1)e}{2pe}$	$-\frac{e}{2pe}(e + \varepsilon\chi(j)\theta)$	$-\frac{e}{2pe}(e + \chi(j)\theta)$	0
R_∞	e	e	e	$-\epsilon\theta$
$\psi(R_\infty)$	$-c_\infty\epsilon\theta$		$c_j e$	$c_0 e$
$\psi(R_0)$	0		$-c_j\frac{e}{2pe}(e + \varepsilon\chi(j)\theta)$	$c_0\frac{(p-1)e}{2pe}$

3. táblázat

Nézzük ennek megfelelően R_∞ és R_0 transzformáltját. A 3. táblázatban $p > j \in \mathbb{N}^+$. Keressünk olyan λ_0 és λ_∞ illetve μ_0 és μ_∞ együtthatókat, amelyekkel $\psi(R_\infty)$ és $\psi(R_0)$ sora az első két sor lineáris kombinációja. A 0-, $-\frac{1}{j}$- és ∞-indexű oszlopokkal az együtthatókra az alábbi egyenleteket kapjuk.

$$\lambda_0\frac{(p-1)e}{2pe} + \lambda_\infty e = c_\infty(-\epsilon\theta)$$
$$\lambda_\infty(-\epsilon\theta) = c_0 e$$
$$\lambda_0\left(-\frac{e}{2pe}(e + \chi(j)\theta)\right) + \lambda_\infty e = c_j e$$
$$\mu_0\frac{(p-1)e}{2pe} + \mu_\infty e = 0$$
$$\mu_\infty(-\epsilon\theta) = c_0\frac{(p-1)e}{2pe}$$
$$\mu_0\left(-\frac{e}{2pe}(e + \chi(j)\theta)\right) + \mu_\infty e = c_j\left(-\frac{e}{2pe}(e + \varepsilon\chi(j)\theta)\right)$$

A második és ötödik egyenletből $\mu_\infty = \frac{(p-1)e}{2pe}\lambda_\infty$, és ebből, valamint a negyedik egyenletből $\mu_0 = -\lambda_\infty$. A hatodik egyenlet bal oldala az előbb kapott összefüggésekkel

$$\mu_0\left(-\frac{e}{2pe}(e + \chi(j)\theta)\right) + \mu_\infty e = \lambda_\infty\frac{e}{2pe}\big((e + \chi(j)\theta) + (p-1)e\big)$$
$$= \lambda_\infty\frac{e}{2pe}(pe + \chi(j)\theta) = \lambda_\infty\chi(j)\theta\frac{e}{2pe}(e + \varepsilon\chi(j)\theta),$$

és ezt egybevetve az egyenlet jobb oldalával kapjuk, hogy $c_j = -\chi(j)\theta\lambda_\infty$. Az eddigi eredményekből és a harmadik egyenletből $\lambda_0 = 2p\lambda_\infty$. Végül az első egyenlettel kapjuk, hogy $c_\infty = -\varepsilon\epsilon\theta\lambda_\infty$. Az eredményeket összefoglalóan mutatja a 4. táblázat.

c_0, c_j és c_∞ egyikét tetszőleges, 0-tól különböző elemnek választhatjuk, hiszen helyettük az előbbi sorrendben ac_0, ac_j és ac_∞ együtthatókkal minden kódszó helyett az a-szorosát kapjuk, és a két vektor egyszerre eleme vagy nem eleme a kódnak, hiszen a kód lineáris. Legyen tehát $c_0 = \epsilon e$. Ekkor $-\lambda_\infty\theta = e$, és ezzel $c_j = \chi(j)e$ és $c_\infty = \varepsilon\epsilon e$ (láthatóan mindegyik oszlop együtthatója „1-abszolút értékű"). Most meg kellene még nézni, hogy a kapott c_0, c_j és c_∞ szorzókkal megkapjuk-e az i-edik sor

transzformáltját a generátorrendszer sorainak valamilyen lineáris kombinációjaként. E helyett egy másik utat választunk.

$c_0 = \epsilon(-\lambda_\infty\theta)$	$\lambda_0 = (-2\varepsilon\theta)(-\lambda_\infty\theta)$
$c_j = \chi(j)(-\lambda_\infty\theta)$	$\mu_0 = \varepsilon\frac{\theta}{pe}(-\lambda_\infty\theta)$
$c_\infty = \varepsilon\epsilon(-\lambda_\infty\theta)$	$\mu_\infty = -\frac{(p-1)e}{2p\theta}(-\lambda_\infty\theta)$

4. táblázat

Emlékeztetünk a diszkrét Fourier-transzformációra. Legyen a pozitív egész n a q prímhatványhoz relatív prím, és ω egy primitív n-edik egységgyök a q-elemű test fölött. Ha $\mathbf{u}$ egy n-dimenziós vektor a test fölött, akkor a diszkrét Fourier-transzformáltjának i-indexű komponense $U_i = \sum_{j=0}^{n-1}\omega^{ij}u_j$ (máshol ω^{-ij} volt az u_j együtthatója, de ez csupán formális eltérést jelent). Az $\mathbf{u}$ k-val való ciklikus eltoltjának a transzformáltja $U_i^{\overrightarrow{(k)}} = \sum_{j=0}^{n-1}\omega^{ij}\left(\mathbf{u}_{\overrightarrow{(k)}}\right)_j = \sum_{j=0}^{n-1}\omega^{ij}u_{(j-k)^{(n)}} = \sum_{j=0}^{n-1}\omega^{i(j+k)}u_j = \left(\omega^k\right)^i U_i$, és így az eltolt transzformáltjának i-indexű komponense akkor és csak akkor 0, amikor az eredeti vektor ezen indexű komponense 0. Ha most $\mathbf{u}$ egy polinom együtthatóinak vektora, akkor $U_i = \sum_{j=0}^{n-1}\omega^{ij}u_j = \sum_{j=0}^{n-1}u_j\left(\omega^i\right)^j = \hat{u}\left(\omega^i\right)$, ami azt jelenti, hogy U_i pontosan akkor 0, ha ω^i gyöke a polinomnak. Ez egyben azt is jelenti, hogy az eltolthoz tartozó polinomnak akkor és csak akkor gyöke ω^i, ha az alap-polinomnak gyöke.

Visszatérünk a tétel bizonyításához úgy, hogy valamivel többet látunk be. Megmutatjuk, hogy ha az $u_0\cdots u_i\cdots u_{p-1}u_\infty = \mathbf{u} \in \mathbb{F}_q^{p+1}$ vektorhoz tartozó $u_0\cdots u_i\cdots u_{p-1}$ vektor Fourier-transzformáltjában a kvadratikus maradékokkal indexelt komponensek értéke nulla, és $u_\infty = -\frac{\epsilon\theta}{pe}\sum_{i=0}^{p-1}u_i$, akkor $\mathbf{v} = \mathcal{GP}(\mathbf{u})$ is hasonló tulajdonságú (hasonlóan bizonyítható a nemmaradékok esete).

Az előbbiek szerint két dolgot kell bizonyítani: egyrészt, ha $\mathbf{u}$ kielégíti a Gleason-Prange feltételt, akkor ez $\mathbf{v}$-re is igaz, másrészt $v_\infty = -\frac{\epsilon\theta}{pe}\sum_{i=0}^{p-1}v_i$.

Az első állítás azt jelenti, hogy ha modulo p kvadratikus maradék r-re $U_r = 0$, akkor V_r is 0, azaz ekkor $\left(\mathcal{F}\left(\mathcal{GP}\left(\mathcal{F}^{-1}(\mathbf{U})\right)\right)\right)_r = 0$.

$$U_0 = \sum_{i=0}^{p-1}u_i = -\frac{pe}{\epsilon\theta}u_\infty,$$

így

$$u_i = \frac{e}{pe}\left(U_0 + \sum_{j=1}^{p-1}\omega^{-ij}U_j\right) = \frac{e}{pe}\left(-\frac{pe}{\epsilon\theta}u_\infty + \sum_{j=1}^{p-1}\omega^{-ij}U_j\right) = -\frac{e}{\epsilon\theta}u_\infty + \frac{e}{pe}\sum_{j=1}^{p-1}\omega^{-ij}U_j.$$

Most $p > i \in \mathbb{N}^+$-ra

$$v_i = \chi\left(-\frac{1}{i}\right)u_{-\frac{1}{i}} = \chi(-i)\left(-\frac{e}{\epsilon\theta}u_\infty + \frac{e}{pe}\sum_{k=1}^{p-1}\omega^{\frac{1}{i}k}U_k\right)$$

és

$$v_0 = \varepsilon\epsilon u_\infty.$$

Innen

$$V_j = v_0 + \sum_{i=1}^{p-1} \omega^{ij} v_i = \varepsilon\epsilon u_\infty + \sum_{i=1}^{p-1} \omega^{ij} \chi(-i) \left(-\frac{e}{\epsilon\theta} u_\infty + \frac{e}{pe} \sum_{k=1}^{p-1} \omega^{\frac{1}{i}k} U_k \right)$$
$$= \varepsilon\epsilon u_\infty \left(e - \frac{e}{\theta} \sum_{i=1}^{p-1} \chi(i)\omega^{ij} \right) + \frac{e}{pe} \sum_{i=1}^{p-1} \omega^{ij} \chi\left(-\frac{1}{i}\right) \sum_{k=1}^{p-1} \omega^{\frac{1}{i}k} U_k$$
$$= \varepsilon\epsilon u_\infty \left(e - \chi(j)\frac{e}{\theta}\theta \right) + \varepsilon \frac{e}{pe} \sum_{i=1}^{p-1} \omega^{ij} \sum_{k=1}^{p-1} \omega^{\frac{1}{i}k} \chi\left(\frac{1}{i}k\right) \chi(k) U_k.$$

$p > k \in \mathbb{N}^+$ esetén $\chi(k)U_k = -U_k$, mert ha $\chi(k) \neq -1$, akkor $U_k = 0$. Ezt alkalmazva

$$V_j = \varepsilon \left(\epsilon\big(1 - \chi(j)\big) u_\infty - \frac{e}{pe} \sum_{i=1}^{p-1} \omega^{ij} \sum_{k=1}^{p-1} \omega^{\frac{1}{i}k} \chi\left(\frac{1}{i}k\right) U_k \right).$$

Ha $j \in Q$, akkor $\chi(j) = 1$, tehát $\epsilon\big(1 - \chi(j)\big)u_\infty = 0$, és ekkor

$$V_j = -\varepsilon \frac{e}{pe} \sum_{i=1}^{p-1} \omega^{ij} \sum_{k=1}^{p-1} \omega^{\frac{1}{i}k} \chi\left(\frac{1}{i}k\right) U_k.$$

Legyen most a egy primitív p-edik gyök. Ekkor $i = a^r$, $j = a^{-s}$ és $k = a^t$ alakban írható, ahol r, s és t mindegyike $p-1$-nél kisebb nemnegatív egész szám. Ezzel

$$V_{a^{-s}} = -\varepsilon \frac{e}{pe} \sum_{r=0}^{p-2} \omega^{a^r a^{-s}} \sum_{t=0}^{p-2} \omega^{a^{-r}a^t} \chi(a^{-r}a^t) U_{a^t}$$
$$= -\varepsilon \frac{e}{pe} \sum_{r=0}^{p-2} \omega^{a^{-s+r}} \sum_{t=0}^{p-2} (-1)^{-r+t} \omega^{a^{-r+t}} U_{a^t},$$

ahol felhasználtuk, hogy $\chi(a^{-r}a^t) = \chi(a^{-r+t})$ akkor és csak akkor 1, ha a^{-r+t} maradék, ami pontosan akkor következik be, amikor a kitevője páros. Tekintsük az 5. táblázat négy polinomját.

$V' = \sum_{i=0}^{p-2} V'_i x^i$	$V'_i = -\varepsilon p V_{a^i}$	$U' = \sum_{i=0}^{p-2} U'_i x^i$	$U'_i = U_{a^i}$
$g = \sum_{i=0}^{p-2} g_i x^i$	$g_i = \omega^{a^{-i}}$	$h = \sum_{i=0}^{p-2} h_i x^i$	$h_i = (-1)^i \omega^{a^{-i}}$

5. táblázat

Most $V'_{-s} = \sum_{r=0}^{p-2} g_{s-r} \sum_{t=0}^{p-2} h_{r-t} U'_t$. A jobb oldalon ghU', a bal oldalon $V' \circ x^{-1}$ s-edfokú tagjának együtthatója áll, így $V' \circ x^{-1} = ghU'$. A táblázatból az is látszik, hogy $h = g \circ (-x)$, amiből következik, hogy $(gh) \circ (-x) = \big(g \circ (-x)\big)\big(h \circ (-x)\big) = hg = gh$, így gh-ban a páratlan indexű együtthatók mindegyike nulla. Ugyanakkor U'-nél fordított a helyzet, tehát $U' \circ (-x) = -U'$. Ennélfogva

$$(ghU') \circ (-x) = \big((gh) \circ (-x)\big)\big(U' \circ (-x)\big) = gh(-U') = -(ghU'),$$

ezért $V' \circ x^{-1}$-ben a páros fokszámú tagok együtthatója, és így páros r-nél $V_{a^{-r}}$ nulla. De ez éppen azt jelenti, hogy ha i egy modulo p kvadratikus maradék, akkor $V_i = 0$, és éppen ezt akartuk bizonyítani.

Még azt kell belátni, hogy $v_\infty = -\frac{\epsilon\theta}{pe}\sum_{i=0}^{p-1} v_i$, azaz $\sum_{i=0}^{p-1} v_i = -\frac{pe}{\epsilon\theta} v_\infty$.

$$\sum_{i=0}^{p-1} v_i = v_0 + \sum_{i=1}^{p-1} v_i = \varepsilon\epsilon u_\infty + \sum_{i=1}^{p-1} \chi\left(-\frac{1}{i}\right) u_{-\frac{1}{i}} = \varepsilon\epsilon u_\infty + \sum_{i=1}^{p-1} \chi(i) u_i.$$

u_i-t a spektrumából számolva

$$\begin{aligned}\sum_{i=1}^{p-1} \chi(i) u_i &= \frac{e}{pe}\sum_{i=1}^{p-1} \chi(i)\left(U_0 + \sum_{k=1}^{p-1} \omega^{-ik} U_k\right) \\ &= \frac{e}{pe}\left(U_0 \sum_{i=1}^{p-1} \chi(i) + \sum_{k=1}^{p-1}\left(\sum_{i=1}^{p-1} \chi(i)\omega^{-ik}\right) U_k\right) \\ &= \frac{\theta}{pe}\sum_{k=1}^{p-1} \chi(-k) U_k = -\varepsilon\frac{\theta}{pe}\sum_{k=1}^{p-1} U_k,\end{aligned}$$

ahol ismét kihasználtuk, hogy $U_k = 0$, amikor $\chi(k) \neq -1$, és azt, hogy a $\sum_{i=1}^{p-1} \chi(i)$ összegben azonos számú tag értéke $+1$ illetve -1. A fenti eredménnyel

$$\begin{aligned}\sum_{i=0}^{p-1} v_i &= \varepsilon\epsilon u_\infty - \varepsilon\frac{\theta}{pe}\sum_{k=1}^{p-1} U_k = -\varepsilon\frac{\theta}{pe} U_0 - \varepsilon\frac{\theta}{pe}\sum_{k=1}^{p-1} U_k \\ &= -\varepsilon\frac{\theta}{pe}\sum_{k=0}^{p-1} U_k = -\varepsilon\theta u_0 = -\varepsilon\epsilon\theta v_\infty = -\frac{pe}{\epsilon\theta} v_\infty.\end{aligned}$$

□

Ha egy kód automorfizmus-csoportja tranzitív, akkor ennek fontos következménye az alábbi tétel.

16.21. Tétel

1. Legyen a C kód automorfizmus-csoportja tranzitív. Ekkor a kódot bármely pozíción átszúrva, a kapott kódok ekvivalensek;

2. ha a C lineáris kód $\hat{C}$ kiterjesztésében minden $\mathbf{u} \in C_e$ kiterjesztése párosszerű, és $Aut(\hat{C})$ tranzitív, akkor C súlya $w(C_o)$, és C minden minimális súlyú kódszava páratlanszerű.

Δ

A bizonyítás előtt megjegyezzük, hogy egy kiterjesztett kódot a kiterjesztésnek megfelelő helyen átszúrva az eredeti kódot kapjuk (a másik irányban ez nem feltétlenül igaz, azaz egy kódot átszúrva, majd ugyanezen helyen kiterjesztve általában nem kapjuk vissza az eredeti kódot).

Bizonyítás:

1. Elegendő azt megmutatni, hogy tetszőleges $n > k \in \mathbb{N}$-re a kódot a k-indexű helyen átszúrva a kapott kód ekvivalens a 0-indexnél átszúrt kóddal. A feltétel szerint van az indexeknek olyan π permutációja, amely k-t a 0-ba viszi. Írjuk fel a C kódszavait tetszőleges sorrendben. Alkalmazva π-t, a C-vel azonos $C^{(\pi)}$ kódot, és ennek a kódnak a szavait alkalmas sorrendben írva az eredeti kódszósorozatot kapjuk. Ez pedig éppen azt jelenti, hogy az eredeti kód k-adik oszlopát törölve ugyanazt a kódot kapjuk, mint amikor a 0-indexű oszlopot hagyjuk el.

2. Tegyük fel, hogy C-ben van minimális súlyú, párosszerű kódszó. A kiterjesztésnél ezt a szót 0-val egészítjük ki, és ennek a szónak a súlya nem változik. Ha most a kiterjesztett kódot egy olyan helyen szúrjuk át, ahol a megfelelő komponense nem nulla, akkor a szó súlya 1-gyel csökken, vagyis kisebb lesz, mint az eredeti kód súlya, ami nem lehet, mert az átszúrt kód azonos azzal a kóddal, amelyet a kiterjesztésnek megfelelő helyen szúrunk át, az így kapott kód viszont az eredeti kód.

□

A 16.6. Tétellel rögtön kapjuk az alábbi eredményt.

16.22. Következmény

n-szóhosszúságú kvadratikus maradékkód d távolsága nagyobb, mint $\sqrt{n}$. Ha $n \bmod 4 = -1$, akkor $d^2 - d + 1 \geq n$, és ha e mellett a kód bináris, akkor $d \equiv 3\ (4)$.

Δ

17. A Golay-kód

Elsőként egy, látszólag a kódolástól távol eső kérdéssel foglalkozunk.

17.1. Definíció

Legyen v, k, t és λ nemnegatív egész szám, X egy v-elemű halmaz, és $\mathcal{B}$ az X k-elemű részhalmazai összességének egy részhalmaza. Az $(X, \mathcal{B})$ párt $t-(v,k,\lambda)$-**rendszer**nek mondjuk, ha az X minden t-elemű részhalmaza a $\mathcal{B}$ pontosan λ elemének részhalmaza. Ekkor X elemeit **pont**nak, $\mathcal{B}$ elemeit **blokk**nak nevezzük.

A $2-(v,k,\lambda)$-rendszer **blokkrendszer**, a $t-(v,k,1)$-rendszer a **Steiner-rendszer**, ez utóbbit $S(t,k,v)$-vel is jelöljük.

Δ

Máris mutatunk egy példát, ahol az előbbi rendszerek és a kódolás összekapcsolódik. Előtte bevezetünk két fogalmat. Egy additív Abel-csoport S alaphalmaza mint szimbólumhalmaz fölötti $n \in \mathbb{N}$ szóhosszúságú szavak halmazában **egy u szó** $Sp(\mathbf{u})$ **tartója** a nem nulla komponensek indexeinek halmaza. A **v szó fedi az u szót**, ha $Sp(\mathbf{u}) \subseteq Sp(\mathbf{v})$, és ezt $\mathbf{u} \leq \mathbf{v}$ jelöli.

17.2. Tétel

Legyen C egy bináris, n-szóhosszúságú, pontosan t-hibajavító tökéletes kód, és legyen $\hat{C}$ a párosra kiterjesztett kód. Ekkor C $2t+1$-súlyú kódszavainak tartóhalmazai $S(t+1,2t+1,n)$-, míg a kiterjesztett kód $2t+2$-súlyú kódszavainak tartóhalmazai $S(t+2,2t+2,n+1)$-rendszert alkotnak.

Δ

Bizonyítás:

Legyen X a szavak indexeinek halmaza, a blokkok az első esetben C minimális súlyú kódszavainak, a második esetben a kiterjesztett kód minimális súlyú kódszavainak (ezek biztosan $2t+2$-súlyúak, mert a $2t+1$-súlyú kódszavakat e-vel terjesztettük ki) a tartóhalmazai. A C kód tökéletes, így a tér minden pontja egy és csak egy kódszó-középpontú, t-sugarú gömb eleme. Egy $t+1$-súlyú szótól legfeljebb t távolságra csak olyan kódszó lehet, amelynek a súlya $1 \leq w \leq 2t+1$, és az adott kódban ilyen csak $w = 2t+1$-re van. Legyen $\mathbf{u}$ egy $t+1$-súlyú szó és $\mathbf{v}$ az $\mathbf{u}$-t tartalmazó egyetlen t-sugarú, kódszó-középpontú gömb középpontja. Ekkor

$$t \geq d(\mathbf{u},\mathbf{v}) = w(\mathbf{u}-\mathbf{v}) = w(\mathbf{u}+\mathbf{v}) = w(\mathbf{u}) + w(\mathbf{v}) - 2w(\mathbf{u}\cap\mathbf{v})$$
$$= (t+1) + (2t+1) - 2w(\mathbf{u}\cap\mathbf{v}),$$

és ebből $w(\mathbf{u}\cap\mathbf{v}) \geq t+1$. Ugyanakkor $w(\mathbf{u}\cap\mathbf{v}) \leq \min\{w(\mathbf{u}), w(\mathbf{v})\} = t+1$, és egyenlőség akkor és csak akkor van, amikor $\mathbf{v}$ fedi $\mathbf{u}$-t. De a két egyenlőtlenségből $w(\mathbf{u}\cap\mathbf{v}) = t+1$, $\mathbf{v}$ fedi $\mathbf{u}$-t, $\mathbf{u}$ tartóhalmaza része $\mathbf{v}$ tartóhalmazának, azaz egy blokknak, és csak egyetlen ilyen blokk van, amiből következik az első állítás.

A második állítás bizonyításánál két esetet kell megkülönböztetni attól függően, hogy a $t+2$-súlyú szóban a paritásbitnek megfelelő helyen álló jegynek mi az értéke. Ha ez e, akkor ezt elhagyva egy $t+1$-súlyú szót kapunk, és ez egy és csak egy C-beli, $2t+1$-súlyú kódszóhoz tartozik. Mivel ennek a súlya páratlan, ezért a hozzá tartozó paritásjegy e, és az őt tartalmazó kódszóban is ugyanez a paritásjegy, vagyis ez egy $2t+2$-súlyú kódszó a kiterjesztett kódban. A másik esetben C-ben egy esetleges $2t+2$-súlyú kódszó is csak t távolságra van, vagyis a kódszó súlya most $2t+1+\varepsilon$, ahol ε értéke 0 vagy 1. Ekkor $2w(\mathbf{u}\cap\mathbf{v}) \geq 2t+3+\varepsilon$, és ebből $t+2 \geq w(\mathbf{u}\cap\mathbf{v}) \geq t+2$, vagyis az adott kódszó fedi $\mathbf{u}$-t. De C-ben $2t+1$-súlyú kódszó paritásjegye e, míg a $2t+2$-súlyú kódszavaké – ha vannak ilyenek – 0, így a $t+2$-súlyú szavunkat tartalmazó kódszó súlya mindkét esetben $2t+2$.

□

Most a t-rendszerek néhány tulajdonságával foglalkozunk.

17.3. Tétel

Az $(X, \mathcal{B})$ $t-(v,k,\lambda)$-rendszerben legyen A az X egy i-elemű részhalmaza, ahol $t \geq i \in \mathbb{N}$. Ekkor azon blokkok száma, amelyek tartalmazzák A-t, független az A-beli pontoktól, csak i-től függ, és a számuk $\lambda_i = \frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$.

Δ

Bizonyítás:

Egészítsük ki A-t az X egy t-elemű A' részhalmazává. Ehhez $t-i$ elemet kell az $X \backslash A$ halmaz $v-i$ eleméből kiválasztani, ami $\binom{v-i}{t-i}$-féle módon lehetséges. A' pontosan λ számú blokk részhalmaza, és minden ilyen blokknak részhalmaza A is. A a pótlólagosan választott elemekkel akkor és csak akkor lesz ugyanazon blokk része, ha a kiválasztott pontok mindegyike ugyanazon blokk eleme. Ez $\binom{k-i}{t-i}$ esetben fordul elő, amiből következik, hogy az A-t tartalmazó különböző blokkok száma a tételben megadott érték, azaz $\lambda_i = \frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$.

□

A tételből speciális esetként kapjuk, hogy $\lambda_t = \lambda$. További speciális eset $i = 0$ és $i = 1$.

17.4. Következmény

1. Csak akkor létezik $t-(v,k,\lambda)$-rendszer, ha minden $t \geq i \in \mathbb{N}$-re $\lambda_i = \frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$ egész szám;
2. $t > i \in \mathbb{N}$-re $\lambda_{i+1} = \lambda_i \frac{k-i}{v-i}$;
3. egy $t-(v,k,\lambda)$-rendszer minden $t \geq i \in \mathbb{N}$-re $i-(v,k,\lambda_i)$-rendszer;
4. $t-(v,k,\lambda)$-rendszerben $b = \lambda_0 = \frac{\lambda\binom{v}{t}}{\binom{k}{t}}$, $bk = vr$, és $t = 2$ esetén $\lambda(v-1) = r(k-1)$, ahol $b = |\mathcal{B}|$ a blokkok, r pedig az X egyes pontjait tartalmazó blokkok száma.

Δ

Bizonyítás:

Az első három állítás közvetlenül adódik a tételből, ezért csak a negyedik pontot kell bizonyítani.

$\lambda_0 = \frac{\lambda\binom{v}{t}}{\binom{k}{t}}$ azt adja meg, hogy az üres halmaz hány blokknak része. De az üres halmaz minden halmaznak, tehát minden blokknak részhalmaza, így $\lambda_0 = b$.

r az egyelemű részhalmazokat tartalmazó blokkok száma, így $r = \lambda_1 = \frac{\lambda\binom{v-1}{t-1}}{\binom{k-1}{t-1}}$. A b előbbi kifejezéséből $b = \frac{\lambda\binom{v}{t}}{\binom{k}{t}} = \frac{\lambda\binom{v-1}{t-1}v}{\binom{k-1}{t-1}k} = \lambda_1 \frac{v}{k}$, és átrendezéssel ez $bk = vr$. $t = 2$ esetén $r = \frac{\lambda\binom{v-1}{t-1}}{\binom{k-1}{t-1}} = \lambda\frac{v-1}{k-1}$, és ebből megkapjuk a $\lambda(v-1) = r(k-1)$ egyenlőséget.

□

A 4. pontból látjuk, hogy X minden pontja $\frac{bk}{v}$ blokk eleme. Abban a speciális esetben, amikor a blokkok és pontok száma azonos, a pontot tartalmazó blokkok száma megegyezik a blokkok méretével.

Azt, hogy egy $t-(v,k,\lambda)$ rendszerben a blokkok b számára $b\binom{k}{t}=\lambda\binom{v}{t}$, közvetlenül is meg tudjuk határozni. Egy-egy blokk $\binom{k}{t}$-számú, t-elemű részhalmazt tartalmaz, így a b blokkban összesen $b\binom{k}{t}$ t-elemű – nem feltétlenül különböző – részhalmaz van. Az X halmaznak $\binom{v}{t}$ különböző t-elemű részhalmaza van, és mindenegyes ilyen részhalmaz λ blokknak része, így $b\binom{k}{t}=\lambda\binom{v}{t}$.

17.5. Tétel

Legyen v, k, t és λ nemnegatív egész szám, X egy v-elemű halmaz, $\mathcal{B}$ az X k-elemű részhalmazai összességének egy részhalmaza úgy, hogy a $\mathcal{B}$-beli B halmazok száma megegyezik egy $t-(v,k,\lambda)$-rendszer blokkjainak b számával. Ha az X minden t-elemű részhalmaza legfeljebb λ számú $B\in\mathcal{B}$-nek része, akkor az $(X,\mathcal{B})$ pár egy $t-(v,k,\lambda)$-rendszer.

Δ

Bizonyítás:

Legyen az X egy t-elemű U részhalmazára $\lambda(U)$ az U-t tartalmazó, $\mathcal{B}$-hez tartozó B-k száma. Ekkor, a tétel feltételeit figyelembe véve, $b\binom{k}{t}=\sum_{\substack{U\subseteq X\\|U|=t}}\lambda(U)\leq\lambda\binom{v}{t}=b\binom{k}{t}$. Itt egyenlőség csak úgy lehet, ha minden t-elemű $U\subseteq X$-re $\lambda(U)=\lambda$.

□

Egy t-rendszerhez megadható az **illeszkedési mátrix**a, azaz egy olyan $b\times v$-méretű mátrix, ahol b a blokkok száma, a sorok a blokkokhoz, az oszlopok a pontokhoz tartoznak, és ahol az i-edik sor j-edik eleme 1, ha az adott pont eleme a blokknak, az ellenkező esetben pedig ez a bejegyzés 0.

Ezek után rátérünk a kódok vizsgálatára.

23 és 11 prímszám, és $23=8\cdot 3-1$, $11=12\cdot 1-1$, így létezik $n=23$ szóhosszúsággal bináris és $n=11$ hosszúságú szavakkal ternáris kvadratikus maradékkód. Az előbbit a továbbiakban $\mathcal{G}_{23}$-mal, míg az utóbbit $\mathcal{G}_{11}$-gyel fogjuk jelölni. Az előbbi generátor-polinomja 11-edfokú, a másiké 5-ödfokú, tehát $11=23-k$-ból $k=12$ és $5=11-k$-ból $k=6$, ennélfogva $\mathcal{G}_{23}$ egy $[23{,}12,d]_2$-paraméterű, $\mathcal{G}_{11}$ pedig $[11{,}6,d]_3$-paraméterű kód. A kódok távolságát a 16.22. Következményből tudjuk meghatározni. E szerint a bináris kód d távolsága legalább 6, és $d\equiv 3\ (4)$, tehát a bináris kód távolsága $d\geq 7$, míg a ternáris kódnál egyrészt $d\geq 4$, másrészt $d \bmod 3$ értéke 0 vagy 2, ahonnan $d\geq 5$. Megmutatjuk, hogy mindkét esetben az egyenlőség teljesül.

17.6. Tétel

Ha C egy $(23,M,d)$-paraméterű bináris kód, ahol $M\geq 2^{12}$ és $d\geq 7$, akkor a kód tökéletes, és a kód mérete $M=2^{12}$, a távolsága $d=7$. Hasonlóan, $(11,M\geq 3^6,d\geq 5)_3$ kódnál $M=3^6,d=5$, és a kód tökéletes.

Δ

Bizonyítás:

A Hamming-korlátot alkalmazzuk, amely szerint a q-elemű ábécé feletti (n,M,d)-kódra teljesül az $M\sum_{i=0}^{t}\binom{n}{i}(q-1)^i\leq q^n$ feltétel, ahol $t=\left\lfloor\frac{d-1}{2}\right\rfloor$. A tételben $t=\left\lfloor\frac{d-1}{2}\right\rfloor\geq\left\lfloor\frac{7-1}{2}\right\rfloor=3$ a bináris kódnál, $q-1=2-1=1$ és $q^n=2^{23}$, míg a másik esetben $t=\left\lfloor\frac{d-1}{2}\right\rfloor\geq\left\lfloor\frac{5-1}{2}\right\rfloor=2$, $q-1=3-1=2$ és $q^n=3^{11}$.

$\sum_{i=0}^{3}\binom{23}{i} = 1 + 23 + \frac{23\cdot 22}{2} + \frac{23\cdot 22\cdot 21}{2\cdot 3} = 1 + 23 + 253 + 1771 = 2048 = 2^{11}$, és $t \geq 3$ következtében $\sum_{i=0}^{t}\binom{23}{i} \geq \sum_{i=0}^{3}\binom{23}{i}$, ezért a bináris kódnál $M \leq 2^{12}$. Ugyanakkor a tételben megadott feltétel szerint $M \geq 2^{12}$, így a kód mérete $M = 2^{12}$. Ekkor $2^{23} \leq M\sum_{i=0}^{3}\binom{23}{i} \leq M\sum_{i=0}^{t}\binom{23}{i} \leq 2^{23}$, tehát $\sum_{i=0}^{3}\binom{23}{i} = \sum_{i=0}^{t}\binom{23}{i}$, ennélfogva $t = 3$. E szerint $d = 7$ vagy $d = 8$. Mivel tökéletes kód távolsága páratlan, ezért a kód távolsága pontosan 7.

A másik kódnál $\sum_{i=0}^{2}\binom{11}{i}2^i = 1 + 11\cdot 2 + \frac{11\cdot 10}{2}\cdot 4 = 1 + 22 + 220 = 243 = 3^5,\ M \leq 3^6$. Másrészt a tételben $M \geq 3^6$, így $M = 3^6$. Ekkor $3^5 \leq \sum_{i=0}^{2}\binom{11}{i}(3-1)^i \leq \sum_{i=0}^{t}\binom{11}{i}(3-1)^i \leq 3^5$, tehát $\sum_{i=0}^{2}\binom{11}{i}(3-1)^i = \sum_{i=0}^{t}\binom{11}{i}(3-1)^i$, következésképpen $t = 2$. Ekkor $d = 5$ vagy $d = 6$, és a kód tökéletes, amiből az is következik, hogy a távolsága pontosan 5.

□

Egy Abel-csoport mint szimbólumhalmaz fölötti kódnál fontos információt ad a **súlyeloszlás**. Ha C egy ilyen halmazon értelmezett (n, M)-paraméterű kód, akkor a súlyeloszlása egy $A_0, \cdots, A_i, \cdots, A_n$ sorozat, ahol A_i a kód i-súlyú szavainak száma. Nyilván teljesül a $\sum_{i=0}^{n} A_i = M$ egyenlőség. Ha a kód tartalmazza a $\mathbf{0}$ kódszót, és a kód súlya w_C, akkor $A_0 = 1$, $A_1 = \cdots = A_{w_C-1} = 0$ és $A_{w_C} > 0$. q-elemű test fölötti lineáris kód esetén az is közvetlenül adódik, hogy minden $i > 0$-ra A_i a $q-1$ többszöröse.

A kódnak sem a sebessége, sem a hibajavító képessége nem függ a kódábécétől, ezért feltehetjük, hogy az mindig egy additív Abel-csoport.

Tökéletes kód esetén a súlyeloszlás csak a kód paramétereitől függ, amint az alábbiak mutatják.

Legyen A egy $q \in \mathbb{N}^+$-elemű szimbólumhalmaz, n pozitív egész szám és $C \subseteq A^n$ egy A feletti, n-hosszúságú kódszavakat tartalmazó kód. Ha a kód távolsága d, és $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, akkor a kódszó-középpontú, t-sugarú gömbök páronként diszjunktak, így a tér minden eleme legfeljebb egy ilyen gömbben van benne, és ebből kapjuk a gömbkitöltési, gömbpakolási vagy másként Hamming-korlátot, amely szerint $M\sum_{i=0}^{t}\binom{n}{i}(q-1)^i \leq q^n$, ahol M a kódszavak száma. Amennyiben az előbbi egyenlőtlenség egyenlőséggel teljesül, akkor a kód tökéletes. Ebben az esetben minden szó egy és csak egy gömb eleme, és ekkor az A_i értékeket sorban egymás után meg tudjuk határozni, feltéve, hogy $\mathbf{0}$ eleme a kódnak. Azt már leírtuk, hogy $A_0 = 1$, és a kód távolságából az is következett, hogy $w_C > i \in \mathbb{N}^+$-ra $A_i = 0$, ahol w_C most is a kód súlya (ha $C - C \subseteq C$, akkor $w_C = d$, egyébként pedig $w_C \geq d$, hiszen ha $w(\mathbf{u}) = w_C$, akkor $d \leq d(\mathbf{u}, \mathbf{0}) = w(\mathbf{u}) = w_C$). A további értékek meghatározása az alábbi módon történik.

$n \geq w \in \mathbb{N}$-súlyú szó összesen $\binom{n}{w}$ van, és minden ilyen szó egy és csak egy olyan kódszó-középpontú, t-sugarú gömbben van, amelynek a súlya legalább $w - t$ és legfeljebb $w + t$. Ha egy adott w'-nél minden w'-súlyú kódszó mint középpont körüli t-sugarú gömbben azonos számú w-súlyú szó van, és ez a szám $N(w, w')$, akkor $\binom{n}{w} = \sum_{w'=w-t}^{w+t} N(w, w')A_{w'}$, feltéve, hogy $t \leq w \leq n - t$. Ebből $d \leq r \leq n$-re $A_r = \frac{\binom{n}{w} - \sum_{w'=r-2t}^{r-1} N(r-t, w')A_{w'}}{N(r-t, r)}$, és ez meghatározható, amennyiben minden $i < r$-re ismerjük az A_i-k értékét. Ez igaz a $d = 2t + 1$-nél kisebb i-kre, és ebből kiindulva a többi érték is kiszámítható. Meg kell mutatnunk, hogy kódszótól független a gömbben lévő w-súlyú szavak száma, és meg kell adnunk $N(w, w')$-t.

Tekintsünk egy $t \leq w' \leq n - t$-súlyú szót, és határozzuk meg, hogy hány olyan w-súlyú szó van, amely az előbbi ponttól legfeljebb t távolságra van. Az előbbi feltétellel $w - t \leq w' \leq w + t$ A w'-súlyú $\mathbf{u}$ és a w-súlyú $\mathbf{v}$ szó egymáshoz viszonyított helyzetében négy rész különíthető el. Van egy közös, p-hosszúságú rész, ahol mindkét szóban 0-tól különböző elem áll, és ezen belül van s olyan pozíció, ahol a két szó különbözik. A p helyet $\binom{w'}{p}$-féleképpen választhatjuk, és az s pozíció ezek között $\binom{p}{s}$-féleképpen helyezkedhet el. A $\mathbf{v}$ további nem nulla komponenseinél $\mathbf{u}$-ban 0 áll. Ilyen hely $w - p$ van, és ezek $n - w'$ pozícióból kerülnek ki, tehát ezen rész $\binom{n-w'}{w-p}$ különböző alakzatban fordulhat elő.

u-ban még $w' - p$ olyan hely van, ahol 0-tól különböző elem van, és **v** ezen komponensei 0-k. Együttvéve $\binom{w'}{p}\binom{n-w'}{w-p}\binom{p}{s}(q-2)^s(q-1)^{w-p}$ a keresett érték egy adott p és s mellett, hiszen a $w-p$ pozíción **v**-ben bármi állhat, kivéve a 0-t, és az s-számú helyen is szinte bármi lehet **v**-ben a 0-t és azt az egyetlen karaktert leszámítva, amely **u**-ban ezen a pozíción van. Láthatóan a kapott érték nem függ **u** konkrét választásától. Az így kapott értéket kell összegezni a p és s lehetséges értékeire. A képletből p-re a $\max\{0, w' + w - n\} \leq p \leq \min\{w', w\}$ intervallumot kapjuk. A két szó távolsága $w - p + s + w' - p = w + w' - (2p - s)$, és ez nem lehet nagyobb t-nél, ahonnan megkapjuk az s-re vonatkozó, p-től függő korlátot, ami $\max\{0, 2p - (w' + w)\} \leq s \leq \min\{p, t, t + (2p - (w' + w))\}$. Ezek szerint az összegzések tartományai, és ekkor a teljes összeg sem függ **u**-tól, amit igazolni akartunk.

$q = 2$ esetén a kifejezés egyszerűsödik, hiszen ekkor $s = p$, így $N(w, w')$ a $\binom{w'}{p}\binom{n-w'}{w-p}$ szorzatok összege.

A **0**-t tartalmazó bináris tökéletes kód párosra való kiterjesztésének is könnyen megkapjuk a súlyeloszlását, hiszen a páros súlyú szó változatlan, a páratlan súlyú szó súlya eggyel nő, és így $A'_0 = 1$, $A'_{2l+1} = 0$ és $A'_{2l+2} = A_{2l+1} + A_{2l+2}$ ($\left\lfloor \frac{n-1}{2} \right\rfloor \geq l \in \mathbb{N}$, és A_i az eredeti, A'_i a kiterjesztett kód eloszlásának az eleme, hozzátéve, hogy $A_{n+1} = 0$).

Az előbbi összefüggés felhasználásával az általunk megismert tökéletes kódokra az alábbi eredményeket kapjuk (csak a nullától különböző értékeket írjuk ki).

$n = 7$, $q = 2$ és $d = 3$ esetén $A_0 = 1 = A_7$ és $A_3 = 7 = A_4$ (például egy $[7,4,3]_2$-paraméterű Hamming-kód);

$n = 23$, $q = 2$ és $d = 7$ esetén $A_0 = 1 = A_{23}$, $A_7 = 253 = A_{16}$, $A_8 = 506 = A_{15}$ és $A_{11} = 1288 = A_{12}$ (például $\mathcal{G}_{23}$);

$n = 11, q = 3$ és $d = 5$ esetén $A_0 = 1, A_5 = 132 = A_6, A_8 = 330, A_9 = 110$ és $A_{11} = 24$ (például $\mathcal{G}_{11}$).

$\mathcal{G}_{23}$ és $\mathcal{G}_{11}$ kiterjesztése $\mathcal{G}_{24}$ és $\mathcal{G}_{12}$. Mivel mind 23, mind $11 - 1$-gyel kongruens modulo 4, ezért a kiterjesztett kódok önduálisak. Mindkét kód esetén a $-y\sum_{i=0}^{n-1} a_i$ kiterjesztésnél $y = e$, ennélfogva a kiterjesztés a szokásos paritásjeggyel történik. A fenti eredmények alapján meg tudjuk határozni a két kiterjesztett kód súlyeloszlását is. Csak azt kell figyelembe venni, hogy egyrészt minden kódszó súlya legfeljebb eggyel nő, és a kiterjesztett önduális bináris illetve ternáris QR-kód esetén a szó súlya osztható 4-gyel illetve 3-mal. Ezt alkalmazva a bináris kód súlyeloszlása $A_0 = 1 = A_{24}$, $A_8 = 759 = A_{16}$ és $A_{12} = 2576$, és a ternárisé $A_0 = 1$, $A_6 = 264$, $A_9 = 440$ és $A_{12} = 24$.

17.7. Definíció

A 23-szóhosszúságú bináris kvadratikus maradékkód a **bináris Golay-kód**, a háromelemű test fölötti 11-szóhosszúságú kvadratikus maradékkód a **ternáris Golay-kód**. A kódok kiterjesztései a **kiterjesztett bináris Golay-kód** és a **kiterjesztett ternáris Golay-kód**.

Δ

A 17.2. Tétel alapján a minimális súlyú kódszavak tartói $\mathcal{G}_{23}$ esetén egy $4 - (23,7,1)$-, míg $\mathcal{G}_{24}$-nél egy $5 - (24,8,1)$ Steiner-rendszert képeznek.

A Hamming-kód konstrukciójából azonnal látható, hogy ekvivalenciától eltekintve nincs más, tőle különböző olyan lineáris kód, amely $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right]_q$-paraméterű. A Golay-kódokra még még erősebb állítás igaz, ugyanis ha egy kód paraméterei megegyeznek valamely Golay-kód paramétereivel, akkor ekvivalens is az adott paraméterekhez tartozó Golay-kóddal. Ezt a bináris kódokra igazoljuk.

Előbb még belátjuk, hogy nemtriviális, három-hibajavító bináris tökéletes kód csak $n = 23$ szóhosszúsággal létezhet (most az ismétléses kódot is triviálisnak tekintjük).

Ismét a Hamming-korlátot alkalmazzuk. Ha a kód tökéletes, akkor $\sum_{i=0}^{3}\binom{n}{i}$ osztója 2^n-nek. Az összeg $1 + n + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)}{6}$, és ezt 6-tal szorozva

$$6(n+1) + 3n(n-1) + n(n-1)(n-2) = (n+1)(n(n-1)+6)$$
$$= (n+1)\big((n+1)(n-2)+8\big).$$

Mivel az eredeti összeg osztója 2^n-nek, ezért ez egy nemnegatív, n-nél nem nagyobb egész k-val 2^k, és ekkor a hatszorosa $3 \cdot 2^{k+1}$. $n+1$ is 2-hatvány, vagy egy ilyen hatvány háromszorosa. Ha $n+1$ osztható 2^4-nel, akkor $(n+1)(n-2)+8 = 2^3(2l(n-2)+1) = 8(2m+1)$. Mivel ez osztója $3 \cdot 2^{k+1}$-nek, ezért $2m+1$ csak 1 illetve 3 lehetne. Ám ekkor $216 = 16 \cdot 13 + 8 \leq (n+1)(n-2)+8 = 8(2m+1) \leq 24$, ami ellentmondás. Ekkor $n+1$ a $3 \cdot 2^3 = 24$ osztója, tehát $n = 0, 1, 2, 3, 5, 7, 11$ vagy 23. A megfelelő kódok mérete az előbbi sorrendben $1, 1, 1, 1, -, 2, -$ és 2^{12} ($a -$ azt jelenti, hogy az adott n-nel nem teljesül a Hamming-korlátnál az egyenlőség). Egyetlen szóból álló kód felesleges, hiszen átvitel nélkül is tudjuk, hogy mi az üzenet. Ha egy bináris kódban összesen két szó van, és a távolságuk azonos a szóhosszúsággal, akkor feltehető, hogy egyikük a csupa 0-t, a másik a csupa e-t tartalmazó szó, de ez egy ismétléses kód, és így valóban csak egyetlen nem triviális kód marad.

17.8. Tétel

Ha egy bináris, (n, M, d)-paraméterű C kódban $n = 23$, $M \geq 2^{12}$ és $d \geq 7$, akkor a kód ekvivalens a bináris Golay-kóddal, míg egy, a $\mathbf{0}$-t tartalmazó, $(24, M \geq 2^{12}, d \geq 8)_2$-paraméterű C' kód $\mathcal{G}_{24}$-gyel ekvivalens.

Δ

Bizonyítás:

Legyen egy n-szóhosszúságú C kód S szimbólumhalmaza egy additív Abel-csoport, és legyen $\mathbf{u}$ az S^n egy tetszőleges eleme. Ekkor a C **$\mathbf{u}$-val való eltoltja** $C^{(\mathbf{u})} = \mathbf{u} + C$. Az eltolásnál a szavak hossza nem változott, és különböző szó képe különböző (mert a szavak összeadása csoportművelet, mivel komponensenként végezzük az összeadást), így a kód mérete is azonos az eredeti kód méretével. A kód távolsága sem változik. Legyen ugyanis $\mathbf{c}^{(1)} \in C$ és $\mathbf{c}^{(2)} \in C$ a kód két eleme. Ekkor az eltoltak távolsága $d\big(\mathbf{u}+\mathbf{c}^{(1)}, \mathbf{u}+\mathbf{c}^{(2)}\big) = w\Big(\big(\mathbf{u}+\mathbf{c}^{(1)}\big) - \big(\mathbf{u}+\mathbf{c}^{(2)}\big)\Big) = w\big(\mathbf{c}^{(1)} - \mathbf{c}^{(2)}\big) = d\big(\mathbf{c}^{(1)}, \mathbf{c}^{(2)}\big)$, vagyis azonos az eredeti két kódszó távolságával. Ezek alapján egy kód eltoltja ekvivalens magával kóddal. Ha e mellett $\mathbf{c} \in C$, akkor $\mathbf{0} = -\mathbf{c} + \mathbf{c} \in C^{(-\mathbf{c})}$.

A kódábécét egy vele azonos elemszámú ábécével kicserélve úgy, hogy a kódban mindenütt azonos betűt azonos, különböző betűt különbözőre cserélünk, a kód lényegi tulajdonságai nem változnak, így a konkrét esetben feltehetjük, hogy az ábécé a kételemű test, $\mathbb{F}_2$, és a két eleme 0 és e.

Láttuk, hogy feltehetjük, $\mathbf{0} \in C$. Azt már beláttuk, hogy ekkor $M = 2^{12}$, $d = 7$, a kód tökéletes, és meghatároztuk a kód súlyeloszlását. Most szúrjuk át a hosszabbik C' kódot egy tetszőleges pozíción. A kódszavak száma nem változik, hiszen bármely két különböző kódszó legalább 8 helyen különbözik, a hossz eggyel csökken, és a távolság legfeljebb eggyel lesz kisebb, így egy olyan bináris kódot kapunk, amelyben a kódszavak hossza 23, a kód mérete legalább 2^{12} és a távolság minimum 7, azaz a C paramétereivel rendelkezik a kód. Ekkor a méretnél és a távolságnál is egyenlőséget kapunk. Az eredeti kód nem lehet más, mint a rövidebb kód párosra való kiterjesztése. Ha ugyanis ez nem igaz, akkor a hosszabb kódban van $2l+1$-súlyú szó, $\mathbf{u}$. Szúrjuk át a kódot egyszer egy olyan i pozíción, ahol $u_i = 0$, majd egy olyan j helyen, ahol $u_j = e$. Az első esetben az átszúrt $\mathbf{u}'$ súlya továbbra is $2l+1$, míg a másik esetben $w(\mathbf{u}') = 2l$. Mindkét esetben olyan kódunk van, amelynek a súlyeloszlása azonos a C-beli eloszlással. Ám ez lehetetlen, mert C-ben nincs olyan kódszó, amely egy páratlan súlyú kódszónál eggyel kisebb súlyú. A hosszabb kód tehát lényegében véve C párosra való kiterjesztése, azaz $\hat{C}$.

$\hat{C}$-ben minden szó súlya osztható 4-gyel. Tekintsük most $\hat{C}$ két elemét, $\mathbf{u}$-t és $\mathbf{v}$-t. $\mathbf{w} = \mathbf{u} + \mathbf{v}$ tekinthető $\hat{C}^{(\mathbf{u})} = \mathbf{u} + \hat{C}$ elemének. $\hat{C}^{(\mathbf{u})}$ ekvivalens $\hat{C}$-vel, és tartalmazza $\mathbf{0}$-t, így a súlyeloszlása is azonos a $\hat{C}$-beli eloszlással. Ekkor $\mathbf{w}$ súlya is többszöröse 4-nek, vagyis $\hat{C}$ bármely elemének, és bármely két eleme összegének a súlya osztható 4-gyel. Ebből következik, hogy $\hat{C}$ tetszőleges két (nem feltétlenül különböző) elemének skalárszorzata 0, vagyis bármely két kódszó ortogonális, $\hat{C} \subseteq \hat{C}^{\perp}$, ahol $\hat{C}^{\perp}$ a $\hat{C}$ minden elemére merőleges szavak összessége. Könnyen belátható, hogy $\hat{C}^{\perp}$ lineáris tér, és így a $\hat{C}$ által generált lineáris tér, $\langle \hat{C} \rangle$, altere $\hat{C}^{\perp}$-nek. $\hat{C} \subseteq \langle \hat{C} \rangle$-ből $2^{12} = |\hat{C}| \leq |\langle \hat{C} \rangle|$, és ebből $\langle \hat{C} \rangle$ legalább 12-dimenziós. Mivel $\langle \hat{C} \rangle \leq \hat{C}^{\perp}$, ezért $\hat{C}^{\perp}$ is minimum 12-dimenziós, ám ekkor $\langle \hat{C} \rangle$ dimenziója nem lehet nagyobb, mint $24 - 12 = 12$, tehát $\langle \hat{C} \rangle$ pontosan 12-dimenziós. 12-dimenziós bináris térnek 2^{12} eleme van, vagyis $\hat{C}$-nek és az általa generált lineáris térnek azonos az elemszáma, és az előbbi része az utóbbinak, amiből következik, hogy ez a két halmaz megegyezik, $\hat{C} = \langle \hat{C} \rangle$, tehát $\hat{C}$ lineáris kód. Lineáris kód átszúrtja is lineáris, amiből következik, hogy C is lineáris kód.

$\hat{C}$ súlyeloszlása szerint van a kódban 12-súlyú szó. Legyen $\mathbf{c}$ a $\hat{C}$ egy 12-súlyú kódszava. A kód pozícióinak permutációja ekvivalens kódot ad, így feltehetjük, hogy $\mathbf{c}$ első tizenkét pozíciójában 0 áll, és akkor a jobb oldali tizenkét pozíció mindegyikében a szó komponense e. Egy lineáris kód bármely, a $\mathbf{0}$-tól különböző eleme kiegészíthető a kód egy bázisává, tehát a kódnak van olyan generátorrendszere, amelynek egy sora az adott kódszó. Legyen $\mathbf{G}$ a $\hat{C}$ olyan generátorrendszere, amelynek legfelső sora $\mathbf{c}$, és legyen C' a megfelelő maradékkód, azaz az a kód, amelyet a G legfelső sorának és jobb oldali tizenkét oszlopának törlésével kapott mátrix generál. Ennek a lineáris kódnak a szóhosszúsága 12, 11-dimenziós, és a d' távolsága legalább $d - \left\lfloor \left(1 - \frac{1}{q}\right) w(\mathbf{c}) \right\rfloor = 8 - \frac{1}{2} \cdot 12 = 2$. Másrészt a Singleton-korlát felhasználásával $d' \leq n' - k' + 1 = 12 - 11 + 1 = 2$, tehát $d' = 2$. Ezekből az adatokból kapjuk, hogy C' $\mathbf{H}'$ ellenőrző mátrixa egy csupa e-ből álló, egy sort és 11 oszlopot tartalmazó mátrix (mert a távolságból következik, hogy bármely oszlop lineárisan független, így nem lehet 0). Innen a kód egy lehetséges $\mathbf{G}'$ generátormátrixa $\left(\mathbf{e}^{(11)}\ \mathbf{I}^{(11)}\right)$ ($\mathbf{e}^{(11)}$ a csupa e-t tartalmazó oszlopvektor, és $\mathbf{I}^{(11)}$ a 11-edrendű egységmátrix). Magának $\hat{C}$-nek vannak olyan kódszavai, amelyek bal oldali felei éppen $\mathbf{G}'$ megfelelő sorai, és ha ezek jobb oldali feléből álló mátrix $\mathbf{A}$, akkor $\hat{C}$-nek van $\begin{pmatrix} 0 & \mathbf{0}^{(11)^T} & e & \mathbf{e}^{(11)^T} \\ \mathbf{e}^{(11)} & \mathbf{I}^{(11)} & \mathbf{0}^{(11)} & \mathbf{A}' \end{pmatrix}$-alakú generátormátrixa úgy, hogy $\left(\mathbf{0}^{(11)}\ \mathbf{A}'\right)$-t $\mathbf{A}$-ból kapjuk a $\mathbf{c}^T = \left(e\ \mathbf{e}^{(11)^T}\right)$-nek az $\mathbf{A}$ legfelső sora alatti soraihoz való hozzáadásával.

$\mathbf{A}'$ minden sorában pontosan hatszor áll e, és bármely két különböző indexű sorának három helyén található mindkét sorban e. Azt tudjuk, hogy a generátormátrix minden sorának súlya csak 8, 12 vagy annál nagyobb lehet, és a legfelső sort leszámítva minden sor bal felében két darab nullától különböző elem áll. Ha az $\mathbf{A}'$ egy sorának súlya w, akkor a teljes sor súlya $2 + w$, és a legfelső sor, valamint ezen sor összegének súlya $2 + (12 - w) = 14 - w$. Mindkettő legalább 8, így $6 \leq w \leq 6$, tehát $\mathbf{A}'$ minden sorának súlya 6. Hasonló gondolattal kapjuk, hogy $\mathbf{A}'$ bármely két különböző sorában pontosan három olyan pozíció van, ahol mindkét sorban e áll. Legyen ugyanis valamely két különböző sor metszetében t darab e. Most a két sor összegének súlya $2 + (6 + 6 - 2t) = 14 - 2t$, míg az összeghez hozzáadva a legfelső sort, a kapott szó súlya $2 + \big(12 - (6 + 6 - 2t)\big) = 2 + 2t$. Mindkét esetben a kapott szóban van nem nulla elem, így a súly legalább 8, azaz $6 \leq 2t \leq 6$, és így t csak 3 lehet.

Megmutatjuk, hogy a fenti feltételeknek lényegében véve egyetlen 11-edrendű mátrix felel meg.

A mátrixot tekinthetjük egy olyan $(X, \mathcal{B})$ pár illeszkedési mátrixának, ahol X egy 11-elemű halmaz, $\mathcal{B}$ az X 11 darab hatelemű részhalmazából álló blokkok halmaza úgy, hogy bármely két különböző blokk közös elemeinek száma három. Ez akkor és csak akkor lényegében véve egyértelmű, ha lényegében véve egyértelmű a blokkok komplementereiből álló rendszer. A komplementer blokkok mindegyikének öt eleme van, és bármely két különböző blokk pontosan két közös elemet tartalmaz, hiszen az eredeti blokkoknál a két sorban a tizenegy pozícióból háromban mindkét sorban, majd három-három, az előbbitől és egymástól diszjunkt pozícióban pontosan az egyik sorban áll 1, így marad két olyan pozíció, ahol mindkét sorban 0, tehát a komplementer blokkokban 1-es áll.

Először belátjuk, hogy az így kapott mátrix egy $2 - (11,5,2)$-rendszer illeszkedési mátrixa, vagyis bármely két különböző pontból álló pontpár pontosan két blokknak része. Kettőnél több blokkhoz nem tartozhat azonos pontpár. Ha ugyanis ez nem igaz, és tekintünk három olyan blokkot, amelyek

mindegyikének része az adott két pont, akkor, figyelembe véve, hogy két-két blokknak pontosan két közös eleme van, a három blokknak a két közös ponttól különböző részei páronként diszjunktak. Mivel mindegyik blokknak öt pontja és összesen tizenegy pont van, ezért mindhárom blokknak három-három további pontja van, és ezek, a két közös ponttal együtt, a teljes tizenegy elemű halmazt lefedik. Nézzünk most egy negyedik blokkot. Ez vagy tartalmazza mindkét pontot, vagy közülük pontosan egyet, vagy egyiket sem. Az első esetben ennek a blokknak más eleme már nem lehetne, mert egyetlen további közös pontja sem lehetne a három blokk egyikével sem. A második esetben egyrészt ez a pont lenne mindhárom blokkal közös pont, és ezen kívül mindegyikkel kellene még egy és csak egy közös pont, de a három blokk esetén három különböző pont. Ez most azt adná, hogy a blokknak összesen négy pontja van. Végül az utolsó esetben mindegyik blokkal lenne két-két közös pont, minden blokk esetén más-más pontpárral, és más pontja nem lenne ennek a blokknak, azaz most a blokk hat pontot tartalmazna. De mindhárom esetben a pontok száma különbözik öttől, a blokkok közös méretétől, így egyik eset sem lehetséges, nem lenne a három blokkon kívül egyetlen további blokk sem. E szerint bármely pontpár legfeljebb két blokknak része. Ekkor viszont a 17.5. Tétel szerint a rendszerünk egy $2-(11,5,2)$-paraméterű blokkrendszer, figyelembe véve, hogy egy ilyen blokkrendszer blokkjainak száma $b\binom{k}{t}=\lambda\binom{v}{t}$-ből $b=11$, és ez megegyezik a sorok számával, vagyis minden kételemű részhalmaz pontosan két blokknak része.

Már csak az egyértelműséget kell belátnunk[1] (ilyen mátrix létezése következik $\mathcal{G}_{23}$ létezéséből).

Legyen B_1 egy blokk, és legyenek ennek pontjai $a_1.\cdots,a_5$, a blokkhoz nem tartozó pontok pedig $p_1.\cdots,p_6$. Minden p_i-re szerkesztünk egy $\Gamma_{p_i}=\left(B_1,E_{p_i}\right)$ egyszerű, irányítatlan gráfot (mindegyik gráf csúcshalmaza a B_1 blokk pontjainak összessége). Ekkor az élhalmaz lényegében véve a csúcsok bizonyos párjaiból álló halmaz. $r\neq s$-re $\{a_r,a_s\}\in E_{p_i}$ legyen akkor és csak akkor, ha van olyan B_u blokk, amely tartalmazza a_r, a_s és p_i mindegyikét. Ilyen blokk legfeljebb egy van (mert különben az első két pont legalább három blokk közös eleme lenne), és valamely p_i-re van ilyen blokk, hiszen minden pontpár pontosan két blokk része, vagyis van egy és csak egy olyan u, hogy a pontpár benne van B_u-ban, ez a blokk pedig tartalmaz pontosan három, nem B_1-beli pontot. Ez egyben azt is jelenti, hogy ha valamelyik gráf tartalmaz egy élt, akkor az az él pontosan három gráfnak éle.

Az nyilvánvaló, hogy B_1 egyértelműen meghatározza mind a hat gráfot. A gráfok mindegyike 2-reguláris, és különböző ponthoz tartozó bármely két gráfnak pontosan két közös éle van, amelyek emellett nem szomszédosak. Először is, minden a_r, p_i párhoz van két blokk, amely ezt a két pontot tartalmazza, és mindkettőnek van a_r-től és egymástól különböző pontosan egy B_1-beli pontja, a_s illetve a_t. Ekkor Γ_{p_i}-nek éle $\{a_r,a_s\}$ és $\{a_r,a_t\}$, az a_r Γ_{p_i}-beli foka legalább kettő. Három szomszédja viszont nem lehet, mert az azt jelentené, hogy a_r és p_i legalább három blokkban fordul együtt elő.

Nézzünk két különböző ponthoz, p_i-hez és p_j-hez tartozó gráfot. Ha a két gráfnak (a_r,a_s) közös éle, akkor van olyan blokk, amely tartalmazza a_r-et, a_s-t és p_i-t és olyan blokk, amely az első két pontot és p_j-t tartalmazza. Ez a két blokk azonos, mert különben a B_1-en kívül még két különböző blokknak is része lenne az $\{a_r,a_s\}$ halmaz. Van még egy és csak egy olyan blokk, amelynek eleme p_i és p_j. Ennek a blokknak két közös pontja van B_1-gyel. Ez a két pont azonban különbözik mind a_r-től, mind a_s-től, mert különben ennek a két, p_i-t és p_j-t tartalmazó blokknak lenne még legalább egy közös pontja, ami nem igaz. Ebből az is következik, hogy több közös él nem lehet a két gráfban, mert a B_1-beli újabb két pont már nem tudná teljesíteni az előbbi diszjunktsági feltételt, hiszen B_1-nek csupán öt pontja van.

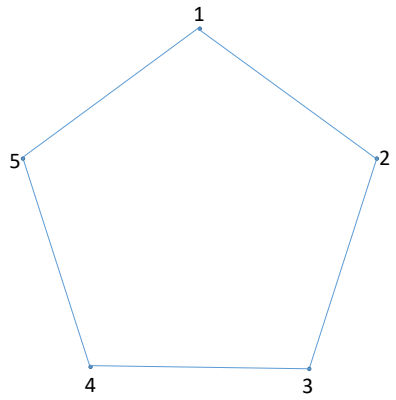
Ha $i\neq j$, akkor $E_{p_i}\neq E_{p_j}$, tehát a két gráf is különböző, mert láttuk, hogy a két gráfnak két közös éle van, de ha a két gráf azonos lenne, akkor legfeljebb csak egy másodfokú csúcs lenne.

Az eddigiekből következik, hogy ez a hat gráf együtt meghatározza a teljes blokkrendszert. Vegyünk ugyanis egy p_i, p_j és p_k ponthármast. Ez a három pont együtt legfeljebb egy blokkban lehet benne. Ha ez a három pont része valamely blokknak, akkor ennek a blokknak a maradék két pontja B_1 pontja, mert kell, hogy legyen két közös pont ezzel a blokkal.

Mindegyik gráf 2-reguláris, tehát egy 5-hosszúságú kör (ha egy egyszerű gráf minden csúcsának foka 2, akkor a gráf páronként diszjunkt körök uniója, egy körnek legalább három pontja van, és minden gráfunk öt pontból áll, így nem lehet egynél több komponens). Most már csak azt kell belátnunk, hogy

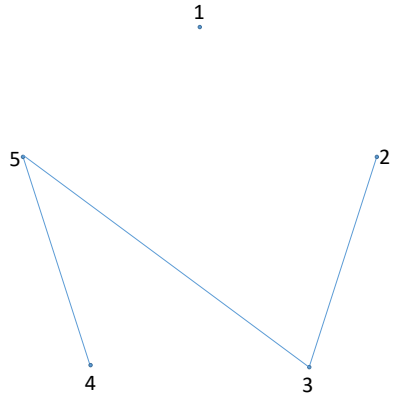
[1] Az egyértelműség bizonyításánál az Interneten a http://www.cs.elte.hu/~csiki/golay.pdf címen található, Csikvári Péter által írt Golay-kód és Witt-design című munkára támaszkodunk.

öt ponton öt-hosszúságú kör úgy, hogy bármely két különböző körnek pontosan két közös éle van, amelyek e mellett nem is szomszédosak, lényegében véve csak egyetlen módon lehetséges. Egy kör tetszőleges sorrendben tartalmazza a pontokat. Az előbbi feltételeknek megfelelő további kört úgy kapunk, ha kiválasztjuk a kör egy élét, ezt ötféleképpen tehetjük meg, és ehhez a kör további négy éléből veszünk egyet, amelynek nincs közös pontja az előbbi éllel. Ilyen él kettő van, tehát az előbb kiválasztott élhez kettőt választhatunk, így az összes választás száma $5 \cdot 2 = 10$. De így minden élpárt kétszer neveztünk meg, tehát végül legfeljebb öt további, a kívánalmakat kielégítő kör létezik. A körök, azaz a különböző gráfok száma tehát egyrészt legalább hat, mert csináltunk hat különböző gráfot, másrészt a körök alapján legfeljebb hat gráfot tudunk így konstruálni, azaz pontosan hat gráf létezik.



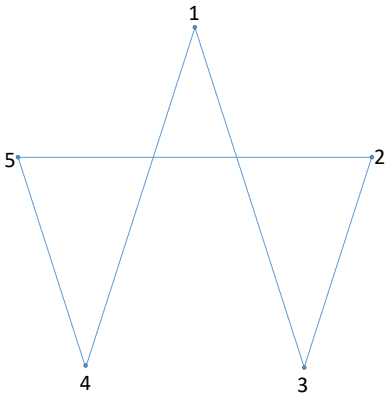
12. ábra

Legyen az egyik gráf olyan, ahol a kör pontjai az indexek sorrendjében követik egymást, amint az 12. ábra mutatja. A következő gráfnak az előzővel két közös oldala van, amelyek nem szomszédosak. Legyen ez a két oldal például a $\{2,3\}$ és a $\{4,5\}$ él. Ezt a két élt kell úgy kiegészíteni, hogy kört kapjuk, de az előbbi gráf egyetlen további élét se tartalmazza. A 3-jelű csúcsból ekkor csak az 5- vagy az 1-jelű csúcs felé indulhatunk. Az első esetben a 13. ábra jön létre. Most a feltételeket kielégítő módon csak a $\{4,1\}$ él következhet, de az 1-es pontból csupán az $\{1,2\}$ élen zárhatnánk a kört, ám ekkor már három közös él lenne az alapgráffal.



13. ábra

Nem marad más lehetőség, mint az első két él után a 3-as csúcsból az 1-es csúcs felé haladni, onnan tovább csupán a 4-es pont következhet, és az így kapott vonal csak az $\{5,2\}$ éllel zárható körré. Ez a kör, amelyet a 14. ábra mutat, viszont kielégíti a feltételeket, így az alapként kiválasztott két él egy és csak egyféleképpen volt kiegészíthető úgy körré, hogy ne legyen több közös él az eredeti körrel. A többi gráf ebből egyszerű elforgatással kapható.



14. ábra

Az előbbi gráfok egyértelműen meghatározzák a blokkrendszert, így $\mathbf{A}'$ is lényegében véve egyértelmű, csupán az oszlopok és sorok sorrendje szabad. Az oszlopok sorrendjének változtatásával a fölötte álló sor nem változik, hiszen minden eleme e, és a változással ekvivalens kódot kapunk. A sorok permutálása sem okoz problémát, mert a sor legelején minden sorban e, közvetlenül $\mathbf{A}'$ bal oldalán mindenütt 0 áll, a többi rész pedig egységmátrix, amelynek sorait permutálva az oszlopok ugyanezen permutációjával visszanyerjük az egységmátrixot, e fölött pedig minden elem 0. Ezek alapján a kiterjesztett kód egyértelmű, ebből pedig következik az átszúrt kód egyértelműsége, hiszen bárhol átszúrva, ekvivalens kódot kapunk. A kód teljes generátormátrixa

$$\mathbf{G} = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1\\
1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&1&1&0&0\\
1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&0&1&1&0\\
1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&0&1&1&1&0\\
1&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&0&0&1&1&0&0&1\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1\\
1&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&1&0&1&1&0&1\\
1&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&1&0&1&0&0&1&1\\
1&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&0&1&0&1&1\\
1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&0&0&0&0&1&1&1
\end{pmatrix}$$

□

Korábban már találkoztunk az Hadamard-mátrixokkal és a belőlük közvetlenül származtatott kódokkal. Most majd a Golay-kódokhoz fogjuk ezeket a mátrixokat alkalmazni.

17.9. Definíció

$\mathbb{F}_q$ **kvadratikus karaktere** $\nu(a) = \begin{cases} 1, & \text{ha } a \text{ kvadratikus} \\ 0, & \text{ha } a = 0 \\ -1, & \text{ha } a \neq 0 \text{ és } a \text{ nem kvadratikus} \end{cases}$, ahol $a \in \mathbb{F}_q$.

Δ

Korábban már találkoztunk prímszám-modulusra a kvadratikus karakterrel, ez most lényegében véve ugyanaz tetszőleges véges testre. ν a test multiplikatív félcsoportjának karaktere, hiszen a test minden eleméhez egyértelműen hozzárendel egy komplex számot úgy, hogy nem mindegyiknek a 0-t feleltteti meg, és az alábbi tételben megmutatjuk, hogy a leképezés szorzattartó. Ettől függetlenül, a ν jelenleg fontos tulajdonságait közvetlenül a definíciója alapján bebizonyítjuk.

17.10. Tétel

a) $\sum_{a\in\mathbb{F}_q} \nu(a) = 0$;

b) ha q páratlan és $h \in \mathbb{F}_q$, akkor $\sum_{a\in\mathbb{F}_q} \nu\big(a(a+h)\big) = -1 + \delta_{h,0} q = \begin{cases} q-1, & \text{ha } h = 0 \\ -1, & \text{ha } h \neq 0. \end{cases}$

Δ

Bizonyítás:

a) $\sum_{a\in\mathbb{F}_q} \nu(a) = \sum_{a\in\mathbb{F}_q^*} \nu(a)$, mert $\nu(0) = 0$, és a test nem nulla elemeinek fele kvadratikus, a másik fele nem kvadratikus, így $\sum_{a\in\mathbb{F}_q^*} \nu(a) = \frac{q-1}{2} \cdot 1 + \frac{q-1}{2} \cdot (-1)$, és ez valóban 0.

b) Először belátjuk, hogy $\nu(a)\nu(b) = \nu(ab)$. Ha a vagy b egyike 0, akkor ez igaz. Nézzük a többi esetet. q páratlan, tehát $2|q-1$, így $(2, q-1) = 2$ és $\frac{q-1}{(2,q-1)} = \frac{q-1}{2}$. Ismét azért, mert q páratlan, e és $-e$ különböző, és mindkettő négyzete e, így e két négyzetgyöke e és $-e$. Mivel bármely elem $q-1$-edik hatványa e, ezért a $\frac{q-1}{2}$-dik hatvány vagy e vagy $-e$; az előbbi esetben a kvadratikus, az utóbbiban nem kvadratikus. Innen viszont könnyen adódik, hogy ab pontosan akkor kvadratikus, ha vagy mindkét tényező kvadratikus, vagy egyikük sem az.

$h = 0$ esetén ha $a \neq 0$, akkor a^2 kvadratikus, tehát $\nu(a^2) = 1$, és az összeg értéke $q-1$. Most legyen $h \neq 0$. Ekkor

$$\sum_{a\in\mathbb{F}_q} \nu\big(a(a+h)\big) = \sum_{a\in\mathbb{F}_q} \nu\big(a^2(e+a^{-1}h)\big) = \sum_{a\in\mathbb{F}_q} \nu(a^2)\nu(e+a^{-1}h)$$
$$= \sum_{a\in\mathbb{F}_q} \nu(e+a^{-1}h) = \sum_{b\in\mathbb{F}_q\setminus\{e\}} \nu(b) = \sum_{b\in\mathbb{F}_q} \nu(b) - \nu(e) = -1,$$

mert a nem nulla elemeknek pontosan a fele kvadratikus, és $e = e^2$, tehát e kvadratikus.

□

Az alábbiakban $n \in \mathbb{N}$-re $\mathbf{I}_n$ az n-méretű egységmátrix, és ^{T} a transzponálás jele.

17.11. Definíció

Legyen q egy páratlan prímhatvány, és rendezzük sorba tetszőleges módon az $\mathbb{F}_q$ test elemeit, azaz legyen $\mathbb{F}_q = \{a_0, \cdots, a_{q-1}\}$. Ekkor az a q-adrendű kvadratikus $\mathbf{P}_q$ mátrix, amelyben a $q > i \in \mathbb{N}$, $q > j \in \mathbb{N}$ indexpárra $p_{i,j} = (\mathbf{P}_q)_{i,j} = \nu(a_i - a_j)$, a q-**adrendű Paley-mátrix**.

Δ

17.12. Tétel

$\mathbf{P}_q \mathbf{P}_q^T = -\mathbf{1}^{(q\times q)} + q\mathbf{I}_q$, és $\mathbf{P}_q$ szimmetrikus, ha $q = 4k+1$, míg $\mathbf{P}_q^T = -\mathbf{P}_q$, ha $q = 4k-1$ ($\mathbf{1}^{(q\times q)}$ azon q-adrendű mátrix, amelynek minden eleme 1).

Δ

Bizonyítás:

$$p_{i,j}^T = p_{j,i} = \nu(a_j - a_i) = \nu\left(-e(a_i - a_j)\right) = \nu(-e)\nu(a_i - a_j) = (-1)^{\frac{q-1}{2}} p_{i,j},$$

mivel $\nu(-e) = 1$, ha $q = 4k+1$ és $\nu(-e) = -1$, ha $q = 4k+3$, vagyis $\nu(-e) = (-1)^{\frac{q-1}{2}}$, így igazoltuk a szimmetrikussággal kapcsolatos állításokat. Az első rész igazolása van még hátra.

$$\left(\mathbf{P}_q\mathbf{P}_q^T\right)_{i,k} = \sum_{j=0}^{q-1} p_{i,j}p_{j,k}^T = \sum_{j=0}^{q-1} p_{i,j}p_{k,j} = \sum_{j=0}^{q-1} \nu(a_i - a_j)\nu(a_k - a_j) = \sum_{j=0}^{q-1} \nu\left((a_i - a_j)(a_k - a_j)\right)$$
$$= \sum_{j=0}^{q-1} \nu\left((a_i - a_j)\left((a_i - a_j) + (a_k - a_i)\right)\right) = \sum_{c\in\mathbb{F}_q} \nu\big(c(c+h)\big) = -1 + \delta_{h,0}q,$$

így valóban igaz, hogy $\mathbf{P}_q\mathbf{P}_q^T = -\mathbf{1}^{(q\times q)} + q\mathbf{I}_q$.

□

A Paley-mátrixból új, fontos mátrixot konstruálunk.

17.13. Tétel

Legyen q egy $4k+3$ alakú prímszám páratlan kitevős hatványa és $\mathbf{P}_q$ a q-adrendű Paley-mátrix. Ekkor a

$$\mathbf{H}_{q+1} = \begin{pmatrix} 1 & \mathbf{1}_q^T \\ \mathbf{1}_q & -\left(\mathbf{P}_q + \mathbf{I}_q\right) \end{pmatrix}$$

mátrixra, ahol $\mathbf{1}_q$ a csupa 1-et tartalmazó q-méretű oszlopmátrix, $\mathbf{H}_{q+1}\mathbf{H}_{q+1}^T = (q+1)\mathbf{I}_{q+1}$.

Δ

Bizonyítás:

$$\mathbf{H}_{q+1}\mathbf{H}_{q+1}^T = \begin{pmatrix} 1 + \mathbf{1}_q^T\,\mathbf{1}_q & \mathbf{1}_q^T - \mathbf{1}_q^T\left(\mathbf{P}_q^T + \mathbf{I}_q\right) \\ \mathbf{1}_q - \left(\mathbf{P}_q + \mathbf{I}_q\right)\mathbf{1}_q & \mathbf{1}_q\mathbf{1}_q^T + \left(\mathbf{P}_q + \mathbf{I}_q\right)\left(\mathbf{P}_q^T + \mathbf{I}_q\right) \end{pmatrix}$$
$$= \begin{pmatrix} q+1 & \mathbf{0}_q^T \\ \mathbf{0}_q & (q+1)\mathbf{I}_q \end{pmatrix} = (q+1)\mathbf{I}_{q+1},$$

mert $\mathbf{P}_q \cdot \mathbf{1}_q$ a $\mathbf{P}_q$ oszlopainak összege, és ez $\mathbf{0}_q$, és $\mathbf{P}_q + \mathbf{P}_q^T$ a q-adrendű $\mathbf{0}$-mátrix, ha q $4k+3$ alakú, hiszen ekkor $\mathbf{P}_q$ antiszimmetrikus.

□

17.14. Definíció

Legyen $n \in \mathbb{N}$. Az 1 és -1 elemekből álló n-edrendű $\mathbf{H}_n$ kvadratikus mátrixot **Hadamard-mátrix**nak nevezzük, ha $\mathbf{H}_n\mathbf{H}_n^T = n\mathbf{I}_n$.

Δ

Önmagában is fontos, és az Hadamard-mátrixok esetén hasznos mátrixműveletet ad meg a következő definíció.

17.15. Definíció

Ha $\mathbf{A}$ egy $p \times q$ és $\mathbf{B}$ egy $r \times s$ méretű mátrix, akkor az $\mathbf{A}$ és $\mathbf{B}$ $\mathbf{A} \otimes \mathbf{B}$-vel jelölt **Kronecker-szorzat**a az a $pr \times qs$-méretű $\mathbf{C}$ mátrix, amelyben $p > i \in \mathbb{N}$, $q > j \in \mathbb{N}$, $r > k \in \mathbb{N}$, $s > m \in \mathbb{N}$-re $C_{ir+k,js+m} = a_{i,j}b_{k,m}$.

Δ

Szemléletesen a Kronecker-szorzat alakja az alábbi:

$$\mathbf{A}\otimes\mathbf{B}=\begin{pmatrix} a_{0,0}\mathbf{B} & \cdots & a_{0,j}\mathbf{B} & \cdots & a_{0,q-1}\mathbf{B} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i,0}\mathbf{B} & \vdots & a_{i,j}\mathbf{B} & \vdots & a_{i,q-1}\mathbf{B} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{p-1,0}\mathbf{B} & \cdots & a_{p-1,j}\mathbf{B} & \cdots & a_{p-1,q-10}\mathbf{B} \end{pmatrix},$$

vagyis egy olyan $p\times q$-méretű hipermátrix, amelynek minden eleme egy $r\times s$-méretű mátrix, és amelyben a $p>i\in\mathbb{N}$, $q>j\in\mathbb{N}$ indexpárhoz tartozó elem $a_{i,j}\mathbf{B}$.

Legyen $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ és $\mathbf{D}$ olyan mátrix, hogy $\mathbf{A}$ a $\mathbf{C}$-vel és $\mathbf{B}$ a $\mathbf{D}$-vel összeszorozható. Ekkor

$$\sum_j\left(a_{i,j}\mathbf{B}\right)\left(c_{j,k}\mathbf{D}\right)=\mathbf{BD}\sum_j a_{i,j}c_{j,k}=(\mathbf{AC})_{i,k}\,\mathbf{BD},$$

ami azt mutatja, hogy $(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D})=\mathbf{AC}\otimes\mathbf{BD}$. Speciális esetként

$$(\mathbf{A}\otimes\mathbf{B})(\mathbf{A}\otimes\mathbf{B})^{\boldsymbol{T}}=(\mathbf{A}\otimes\mathbf{B})(\mathbf{A}^T\otimes\mathbf{B}^T)=(\mathbf{A}\mathbf{A}^T)\otimes(\mathbf{B}\mathbf{B}^T),$$

mert $(\mathbf{A}\otimes\mathbf{B})^{\boldsymbol{T}}$-ben mint hipermátrixban az i,j indexpárhoz tartozó elem $a_{j,i}\mathbf{B}^T$, és ez az $\mathbf{A}^T\otimes\mathbf{B}^T$ mint hipermátrix i,j indexpárhoz tartozó eleme, amint alább látható:

$$(\mathbf{A}\otimes\mathbf{B})^{\boldsymbol{T}}=\begin{pmatrix} a_{0,0}\mathbf{B} & \cdots & a_{0,j}\mathbf{B} & \cdots & a_{0,q-1}\mathbf{B} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i,0}\mathbf{B} & \vdots & a_{i,j}\mathbf{B} & \vdots & a_{i,q-1}\mathbf{B} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{p-1,0}\mathbf{B} & \cdots & a_{p-1,j}\mathbf{B} & \cdots & a_{p-1,q-1}\mathbf{B} \end{pmatrix}^{\boldsymbol{T}}=\begin{pmatrix} a_{0,0}\mathbf{B}^T & \cdots & a_{i,0}\mathbf{B}^T & \cdots & a_{p-1,0}\mathbf{B}^T \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{0,j}\mathbf{B}^T & \vdots & a_{i,j}\mathbf{B}^T & \vdots & a_{p-1,j}\mathbf{B}^T \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{0,q-1}\mathbf{B}^T & \cdots & a_{i,q-1}\mathbf{B}^T & \cdots & a_{p-1,q-1}\mathbf{B}^T \end{pmatrix}$$

$$=\begin{pmatrix} a_{0,0}^T\mathbf{B}^T & \cdots & a_{0,i}^T\mathbf{B}^T & \cdots & a_{0,p-1}^T\mathbf{B}^T \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{j,0}^T\mathbf{B}^T & \vdots & a_{j,i}^T\mathbf{B}^T & \vdots & a_{j,p-1}^T\mathbf{B}^T \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{q-1,0}^T\mathbf{B}^T & \cdots & a_{q-1,i}^T\mathbf{B}^T & \cdots & a_{q-1,p-1}^T\mathbf{B}^T \end{pmatrix}=\mathbf{A}^T\otimes\mathbf{B}^T.$$

17.16. Tétel

$n=1$ és $n=2$ esetén létezik n-edrendű Hadamard-mátrix, és ha valamely m-re és n-re van m-edrendű és n-edrendű Hadamard-mátrix, akkor van mn-edrendű Hadamard-mátrix is.

Δ

Bizonyítás:

$\mathbf{H}_1=(1)$, $\mathbf{H}_2=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ kielégítik a definíciót. Most tegyük fel, hogy $\mathbf{H}_m$ és $\mathbf{H}_n$ Hadamard-mátrix, megmutatjuk, hogy a Kronecker-szorzatuk is Hadamard-mátrix.

Ha $\mathbf{A}$ és $\mathbf{B}$ egyaránt Hadamard-mátrix, akkor mindkettő négyzetes, és így négyzetes a Kronecker-szorzatuk is, továbbá minden eleműk $+1$ és -1, és ilyen számok szorzata is a két érték valamelyike, tehát $\mathbf{H}_m\otimes\mathbf{H}_n$ minden eleme is csak ezen két szám egyike lehet. A tétel előtti eredménnyel

$$(\mathbf{H}_m\otimes\mathbf{H}_n)(\mathbf{H}_m\otimes\mathbf{H}_n)^T=\mathbf{H}_m\mathbf{H}_m^T\otimes\mathbf{H}_n\mathbf{H}_n^T=(m\mathbf{I}_m)\otimes(n\mathbf{I}_n)=(mn)\mathbf{I}_{mn},$$

így a Kronecker-szorzat is Hadamard-mátrix, és a rendje a két Hadamard-mátrix rendjének a szorzata.

□

Az előző tételből következik, hogy ha $n = 2^m$, ahol $m \in \mathbb{N}$, akkor van n-edrendű Hadamard-mátrix, hiszen $2^0 = 1$-re és $2^1 = 2$-re már láttuk a megfelelő mátrixot, míg bármely nemnegatív egész m-re $\mathbf{H}_{2^{m+1}} = \mathbf{H}_2 \otimes \mathbf{H}_{2^m}$:

$$\mathbf{H}_{2^{m+1}} = \mathbf{H}_2 \otimes \mathbf{H}_{2^m} = \begin{pmatrix} 1 \cdot \mathbf{H}_{2^m} & 1 \cdot \mathbf{H}_{2^m} \\ 1 \cdot \mathbf{H}_{2^m} & -1 \cdot \mathbf{H}_{2^m} \end{pmatrix} = \begin{pmatrix} \mathbf{H}_{2^m} & \mathbf{H}_{2^m} \\ \mathbf{H}_{2^m} & -\mathbf{H}_{2^m} \end{pmatrix}.$$

$n = 2^m$-elemű Hadamard-mátrix közvetlenül is konstruálható. Az $n = 2^m$-nél kisebb nemnegatív egész számok, és csak ezen nemnegatív egész számok egy és csak egy alakban felírhatóak m jeggyel a 2-es alapú számrendszerben. Legyen $\mathbf{i}_m$ a $2^m > i \in \mathbb{N}$ bináris felírásában szereplő jegyekből álló vektor, és legyen a 2^m-edrendű $\mathbf{A}$ mátrix i, j indexpárhoz tartozó eleme, ahol i és j egyaránt 2^m-nél.kisebb nemnegatív egész, $(-1)^{\mathbf{i}_m^T \mathbf{j}_m} = (-1)^{\sum_{k=0}^{m-1} i_k j_k} = \prod_{k=0}^{m-1} (-1)^{i_k j_k}$. $m = 0$ esetén egyetlen eleme van $\mathbf{A}$-nak, és ez 1, hiszen $\prod_{k=0}^{-1} a_k = 1$, így ez a mátrix $\mathbf{H}_1$. Most tegyük fel, hogy ha valamely nemnegatív egész m esetén a 2^m-edrendű $\mathbf{A}$ mátrixban az i-edik sor j-indexű eleme $(-1)^{\mathbf{i}_m^T \mathbf{j}_m}$, akkor ez a mátrix $\mathbf{H}_{2^m}$.

$$(-1)^{\mathbf{i}_{m+1}^T \mathbf{j}_{m+1}} = \prod_{k=0}^{m} (-1)^{i_k j_k} = \left(\prod_{k=0}^{m-1} (-1)^{i_k j_k} \right) \cdot (-1)^{i_m j_m} = (-1)^{i_m j_m} (-1)^{\mathbf{i}_m^T \mathbf{j}_m}.$$

Itt $i_m j_m = 0$, ha a két tényező bármelyike 0, míg az egyetlen további esetben a szorzat értéke 1, és így az első esetben $(-1)^{i_m j_m} = 1$, a másik esetben pedig $(-1)^{i_m j_m} = -1$. De ekkor a megfelelő 2^{m+1}-edrendű mátrix $\begin{pmatrix} \mathbf{H}_{2^m} & \mathbf{H}_{2^m} \\ \mathbf{H}_{2^m} & -\mathbf{H}_{2^m} \end{pmatrix}$-alakú, ennél fogva az így konstruált mátrix valóban egy 2^{m+1}-edrendű Hadamard-mátrix.

Eddig azt láttuk, hogy minden nemnegatív egész m-re van 2^m-edrendű, és ha egy $4k + 3$ alakú n szám egy prímszám hatványa, akkor $n + 1$-edrendű Hadamard-mátrix. $n = 1$-et és $n = 2$-t nem számítva minden előbb említett n néggyel osztható, és, ha a Kronecker-szorzatban legalább az egyik mátrix rendje osztható néggyel, akkor a szorzatmátrix rendje is ilyen tulajdonságú, tehát az előbbi két kivétellel minden eddigi ismereteink szerinti Hadamard-mátrix rendje 4 többszöröse. Ez nem véletlen.

17.17. Tétel

Ha $2 < n \in \mathbb{N}$-re van n-edrendű Hadamard-mátrix, akkor $4|n$.

Δ

Bizonyítás:

Legyen $\mathbf{H}_n$ az n-edrendű Hadamard-mátrix, ekkor a feltétel szerint van legalább három sora. Legyen az első három sor sorban $\mathbf{h}_1$, $\mathbf{h}_2$ és $\mathbf{h}_3$, és nézzük a $(\mathbf{h}_1 + \mathbf{h}_2)(\mathbf{h}_1 + \mathbf{h}_3)$ szorzatot. Ez egyrészt $\mathbf{h}_1\mathbf{h}_1 + \mathbf{h}_1\mathbf{h}_2 + \mathbf{h}_1\mathbf{h}_3 + \mathbf{h}_2\mathbf{h}_3$, aminek az értéke n, hiszen a három utolsó tag a mátrix két-két különböző sorának a szorzata, tehát 0, míg az első tag az első sor négyzete, és ez valóban n, hiszen $\mathbf{h}_1\mathbf{h}_1$ n darab 1-es összege. Most vegyük figyelembe, hogy $(\mathbf{h}_1 + \mathbf{h}_2)(\mathbf{h}_1 + \mathbf{h}_3)$ mindkét tényezője olyan n-komponensű vektor, amelyben minden komponens 2, 0 és -2 egyike, vagyis 2-vel osztható. Ám ekkor a két vektor egy-egy ilyen komponensének szorzata osztható néggyel, és így ezek összege, tehát $n = (\mathbf{h}_1 + \mathbf{h}_2)(\mathbf{h}_1 + \mathbf{h}_3)$ is néggyel osztható.

□

Egy sejtés szerint minden $4|n$-re van n-edrendű Hadamard-mátrix, de ezt bizonyítani még nem sikerült (igaz, cáfolni sem).

Hadamard-mátrix sorai és/vagy oszlopai sorrendjének testszőleges permutációja, illetve bármely sorának, oszlopának -1-gyel való szorzása által nyert mátrix is Hadamard-mátrix, így egy Hadamard-

mátrix előbbi átalakításával elérhető, hogy a kapott mátrix első sorának minden eleme $+1$ legyen. Ennek a sornak a mátrix egy ettől különböző indexű sorával való szorzata akkor és csak akkor lesz 0, ha abban a sorban a $+1$-ek és -1-ek száma azonos, vagyis, ha $n = 2k$, akkor az azonos elemek száma k. Ha most két, az elsőtől és egymástól különböző sort tekintünk, akkor az előbbi eredmény mindkét sorra érvényes, és a két sor azonos pozícióin álló elempárok $+1, +1$; $+1, -1$; $-1, +1$ és $-1, -1$. Ha mondjuk a $+1, +1$-ek száma r, akkor összesen $k - r$ helyen lesz $+1, -1$ és ugyanennyi helyen található $-1, +1$, és ebből következően a $-1, -1$ párok száma is r. A két sor szorzata ezekkel az adatokkal $0 = r - (k - r) - (k - r) + r = 4r - 2k$, vagyis $r = k - r$, tehát az elsőtől különböző bármely két, nem azonos indexhez tartozó sor esetén a négy lehetséges párosítás mindegyikéből ugyanannyi lesz.

Ha $(-j)^{(q)} = (-j) \bmod q$, akkor a $j \mapsto (-j)^{(q)}$ megfeleltetés a q-nál kisebb nemnegatív egész számok halmazának egy permutációja, olyan permutációja, ahol a 0 képe önmaga, míg a 0-tól különböző j-re $(-j)^{(q)} = q - j$. Legyen $\mathbf{Q}_q$ olyan q-adrendű mátrix, amelyben $q_{i,j} = p_{i,(-j)^{(q)}}$. Egy kvadratikus mátrixnak a transzponáltjával vett szorzatában az i, k-indexű elem az eredeti mátrix i-edik és k-adik sorának skalárszorzata, és ez nem változik, ha mindkét sorban azonos módon változtatjuk meg az elemek sorrendjét, következésképpen $\mathbf{Q}_q\mathbf{Q}_q^T = \mathbf{P}_q\mathbf{P}_q^T = -\mathbf{1}^{(q\times q)} + q\mathbf{I}_q$. Amennyiben $\mathbb{F}_q$ elemeit úgy rendezzük sorba, hogy a q-nál kisebb minden nemnegatív egészre $a_{(-j)^{(q)}} = -a_j$ (következésképpen páratlan q esetén $a_0 = 0$), akkor

$$q_{i,j} = p_{i,(-j)^{(q)}} = \nu\left(a_i - a_{(-j)^{(q)}}\right) = \nu\left(a_i - (-a_j)\right) = \nu(a_i + a_j)$$

minden i, j indexdpárra, így $q_{i,j} = \nu(a_i + a_j) = \nu(a_j + a_i) = q_{j,i}$, a mátrix szimmetrikus. $\mathbf{I}_q$ oszlopainak hasonló átrendezésével kapott $\mathbf{I}_{(-q)}$ is szimmetrikus, így szimmetrikus a $-(\mathbf{P}_q + \mathbf{I}_q)$-ból hasonlóan kapott $-(\mathbf{Q}_q + \mathbf{I}_{(-q)})$, és ezzel a $\mathbf{H}_{q+1}$-ből nyert $\begin{pmatrix} 1 & \mathbf{1}_q^T \\ \mathbf{1}_q & -(\mathbf{Q}_q + \mathbf{I}_{(-q)}) \end{pmatrix}$ mátrix is.

Most rátérünk a Golay-kódok Hadamard-mátrixos megkonstruálására.

Legyen $\mathbf{H}_{q+1}$ a $\mathbf{P}_q$ Paley-mátrixból nyert Hadamard-mátrix. Megszorozva ennek fődiagonálisát -1-gyel, majd az utolsó $q - 1$ oszlopot fordított sorrendben írva, végül a -1-eket 0-val helyettesítve, a kapott mátrixot jelöljük $\mathbf{A}_{q+1}$-gyel, és legyen $\mathbf{G} = (\mathbf{I}_{q+1}, \mathbf{A}_{q+1})$. Ez a mátrix tekinthető $\mathbb{F}_2$ fölötti mátrixnak. $\mathbf{H}_{q+1}$ 0-indexű sorában $q + 1$ darab $+1$ állt, ebből a jobb felső sarokban a $+1$ előbb -1-re, majd 0-ra változott, így $\mathbf{A}_{q+1}$ legfelső sorában az 1-esek száma q. $\mathbf{G}$-ben ehhez még hozzá jön a főátlóbeli 1-es, így ezen mátrix legfelső sorában $q + 1$ darab, azaz páros számú 1 lesz. A többi sorban eredetileg $\mathbf{H}_{q+1}$ minden sorában a $+1$-ek száma $\frac{q+1}{2}$ volt úgy, hogy a főátló egyetlen eleme sem volt közöttük. Ebből adódóan a változtatások után egy ilyen sorban, a bal oldali egységmátrixot is figyelembe véve, $\frac{q+1}{2} + 2 = \frac{q+5}{2}$ lesz az 1-esek száma. Mivel q $4k + 3$-alakú, ezért $\frac{q+5}{2} = 2k + 4$, tehát páros, a $\mathbf{G}$ mint a kételemű test fölötti mátrix minden sorának önmagával vett skalárszorzata 0, minden sor ortogonális önmagára. Ha még k is páros, akkor minden sor súlya néggyel osztható. Az eddigiekből az következik, hogy a 0-indexű sornak bármely sorral vett skalárszorzata 0, a legfelső sor merőleges minden más sorra. Még azt kell megnézni, hogy mi a helyzet a nem a legfelső sorban álló két különböző indexű sor skalárszorzatával. Itt csak az $\mathbf{A}_{q+1}$-beli rész számít, hiszen az egységmátrixban különböző indexű sorokban azonos pozíción legalább az egyik elem 0. fentebb azt láttuk, hogy $\mathbf{H}_{q+1}$-ben a $+1, +1$ párok száma $\frac{q+1}{4}$ volt. Mindkét sorban a főátló -1-ese $+1$-re változott. $4k + 3$-alakú q esetén $\mathbf{P}_q$ antiszimmetrikus, így a két főátlóbeli elem egyikével $+1$, a másikkal -1 állt párban, tehát a két érintett oszlopban egy $-1, -1$ vagy $-1, +1$ pár, valamint az előbbi sorrendben $+1, -1$ illetve $-1, -1$ pár állt. A cserék után így az előbb álló oszlopban $1, 0$ vagy $1, 1$, a másik pozícióban pedig $1, 1$ vagy $0, 1$ lesz. A cserék után a skalárszorzatban azok a pozíciók érdekesek, amelyeknél mindkét oszlopban 1 áll. Ezek azok a helyek, ahol eredetileg $+1, +1$ volt, és ehhez, az előbbiek szerint még hozzá jön egy új hely, vagyis összesen $\frac{q+1}{4} +$

1 helyen lesz mindkét sorban 0-tól különböző elem. A két sor skalárszorzata akkor és csak akkor lesz 0, ha az 1,1 párok száma, azaz $\frac{q+1}{4}+1$ páros. Ez akkor és csak akkor teljesül, ha q nyolccal való osztásánál a maradék 3, vagyis ha $q = 8l + 3$, ahol l nemnegatív egész szám. Ezzel az is teljesül, hogy a $\mathbf{G}$ minden sorának súlya osztható 4-gyel, így a $\mathbf{G}$ által generált bináris lineáris kód önortogonális, és, mivel az oszlopok száma kétszerese a sorok számának, ezért a kód önduális. Ha még azt is tekintetbe vesszük, hogy az oszlopcserékkel nyert $\mathbf{A}_{q+1}$ szimmetrikus, akkor a kód ellenőrző mátrixa $\mathbf{H} = \left(-\mathbf{A}_{q+1}^T, \mathbf{I}_{q+1}\right) = \left(\mathbf{A}_{q+1}, \mathbf{I}_{q+1}\right) = \mathbf{G}$.

17.18. Tétel

A $\mathbf{G} = (\mathbf{I}_{12}, \mathbf{A}_{12})$ által generált lineáris kód a bináris Golay-kód.

Δ

Bizonyítás:

Mivel a Golay-kódot egyértelműen meghatározzák a paraméterei, ezért elegendő megmutatni, hogy a generált kód $[24,12,8]_2$-paraméterű.

A szavak hossza nyilván 24, a mátrix sorainak száma 12, és a sorok lineárisan függetlenek, hiszen a bal oldali félmátrix egy 12-edrendű egységmátrix, így csak a távolsággal kell foglalkoznunk.

A $\mathbf{P}_{11}$-ből származtatott $\mathbf{H}_{12}$ első sora csupa 1, ebből az első -1-re változott, ezért ebből 0 lesz $\mathbf{A}_{12}$-ben, a többi 1. Minden más sorban 6 darab $+1$ volt, és bármely két ilyen különböző sorban három helyen $+1$, $+1$, három helyen $+1$, -1, hármon -1, $+1$, és ismét hármon -1, -1 állt, ahol az első oszlopban $+1$ volt mindenütt. A változás után ezért minden sorban hét darab 1 és öt darab 0 lesz, és a párosítás: négyszer 1, 1, háromszor 1, 0, háromszor 0, 1 és kétszer 0, 0. Ebből adódik, hogy $\mathbf{I}_{12}$-t hozzávéve valamennyi sorban nyolc darab 1-es áll, kivéve az elsőt, ahol tizenkettő, továbbá, hogy bármely két sor szorzatában páros számú 1 van, tehát a kód önortogonális, és mivel $24 = 2 \times 12$, ezért önduális. Ha egy $\mathbf{G} = (\mathbf{I}, \mathbf{P})$ mátrixszal generált kód önduális, akkor ezt a kódot generálja a $\mathbf{G}' = (-\mathbf{P}^T, \mathbf{I})$ mátrix is. Bináris esetben $-\mathbf{P}^T = \mathbf{P}^T$, és mivel $\mathbf{A}_{12}$ szimmetrikus, ezért $(\mathbf{A}_{12}, \mathbf{I}_{12})$ is generálja G_{24}-et. Az öndualtás alapján mindkét mátrix egyben a kód ellenőrző mátrixa is

$\mathbf{G}$ minden sorának súlya osztható 4-gyel, és G_{24} önduális, így G_{24} valamennyi szavának súlya 4 többszöröse. Belátjuk, hogy nincs olyan nem $\mathbf{0}$ kódszó, amelynek a súlya 4. Legyen ugyanis $\mathbf{c}$ olyan, hogy $w(\mathbf{c}) = 4$. $\mathbf{c}$-t két részre bontjuk: $\mathbf{c} = \left(\mathbf{c}_b, \mathbf{c}_j\right)$, ahol mindkét rész 12-bites. $\mathbf{c}_b$-t is $\mathbf{I}_{12}$-ből kaphatjuk nemtriviális kombinációval, $\mathbf{c}_j$-t is, ezért $w(\mathbf{c}_b) \neq 0 \neq w\left(\mathbf{c}_j\right)$. Ha $w(\mathbf{c}_b) = 1$, akkor $\mathbf{c}$ a $\mathbf{G}$ egy sora, de ezek súlya legalább 8, ezért $w(\mathbf{c}_b) \neq 1$, hasonlóan $w\left(\mathbf{c}_j\right) \neq 1$, tehát $w(\mathbf{c}_b) \geq 2$ és $w\left(\mathbf{c}_j\right) \geq 2$. De $w(\mathbf{c}) = 4$ a feltételezés szerint, így csak $w(\mathbf{c}_b) = 2 = w\left(\mathbf{c}_j\right)$ lehet. $w(\mathbf{c}_b) = 2$ szerint $\mathbf{c}$ $\mathbf{G}$-beli két sor összege. De ekkor $w(\mathbf{c}) = w(\mathbf{g}_1) + w(\mathbf{g}_2) - 2w(\mathbf{g}_1 \cap \mathbf{g}_1)$. Ha a $\mathbf{g}_1$ és a $\mathbf{g}_2$ egyike, mondjuk $\mathbf{g}_1$ az első sor, akkor $w(\mathbf{g}_1) = 12$, $w(\mathbf{g}_2) = 8$ és $w(\mathbf{g}_1 \cap \mathbf{g}_1) = 6$, míg az ellenkező esetben $w(\mathbf{g}_1) = 8 = w(\mathbf{g}_2)$, $w(\mathbf{g}_1 \cap \mathbf{g}_1) = 4$, tehát $w(\mathbf{c})$ az első esetben $12 + 8 - 2 \cdot 6 = 8$, a másodikban $2 \cdot 8 - 2 \cdot 4 = 8$, vagyis mindkét alkalommal $w(\mathbf{c}) = 8$, így $w(\mathbf{c}) = 4$ nem lehetséges, ennélfogva $w(G_{24}) = d(G_{24}) \geq 8$, és mivel van 8-súlyú kódszó, ezért egyenlőség áll.

□

Megmutatjuk, hogy a bináris Golay-kód visszafejtésére alkalmazható a korábban már tárgyalt hibacsapda-dekódolás.

G_{24} egy 8-távolságú önduális kód, és az Hadamard-mátrixos alakjában az ellenőrző- és a generátormátrix $\mathbf{H} = (\mathbf{P}, \mathbf{I})$ és $\mathbf{G} = (\mathbf{I}, -\mathbf{P}^T) = (\mathbf{I}, \mathbf{P})$ alakú. A konkrét esetben az alábbi $\mathbf{G}$ mátrixban a jobb alsó 11-edrendű részben láthatóan ismét minden sor súlya 6 és bármely két különböző sor metszetében pontosan három helyen áll 1-es. A szimmetria miatt ez igaz az oszlopokra is. Ebből következik, hogy ezen 11-edrendű részmátrix bármely két különböző indexű oszlopának összegében is hat darab helyen áll 1, az összeg súlya is 6. A legfölső sorban minden elem 1, így két oszlop összegében ott 0 lesz.

$$\mathbf{G} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&1&1&0&1&1&0&1&1&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&1&1&0&1&1&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&1&1&0&1&1&1\\
0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&1&0&1&1&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&1&1&1&0&0&0&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&1&1&1&1&0&0&0&1&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&1&0&1
\end{pmatrix}$$

Tegyük fel, hogy a hibák száma legfeljebb 3. Az öndualitás miatt $\mathbf{G}$ is paritásellenőrző mátrixa a kódnak, így mindkét mátrixszal számolható egy beérkezett szó szindrómája. Ha a legfeljebb 3 hiba mindegyike a kód egyik felében lép fel, akkor valamelyik ellenőrzésnél a szindróma súlya legfeljebb 3, mert az egységmátrix legfeljebb három oszlopának összege a szindróma. Most a másik ellenőrzésnél a mátrix másik felében lévő oszlopok összegét nézzük. A jobb oldali fél szimmetrikusságának köszönhetően ez ugyanaz, mintha $\mathbf{G}$ sorainak összegében az utolsó tizenkét jegyből álló részt néznénk. A sorok lineárisan függetlenek, így legfeljebb három sor összege nem lehet a csupa 0-t tartalmazó sor. Ekkor viszont legalább nyolc 1-est tartalmaz, amelyből legfeljebb három esik a bal oldali félre, így a legalább egy, de legfeljebb három oszlop összegének súlya legalább 5. Ha tehát legfeljebb három hiba van, és mindegyik a vett szó azonos felében van, akkor a két ellenőrzéssel kapott szindrómák egyikének súlya legfeljebb 3, a másiké pedig legalább 5. A hiba (ha egyáltalán volt, tehát a szindróma egyik esetben sem 0) most könnyen javítható. Ha mondjuk a $\mathbf{H} = (\mathbf{P}, \mathbf{I})$-vel való szorzásnál kapjuk a legfeljebb 3-súlyú szindrómát, akkor a hibátlan adatrész a bal oldali fele a vett szónak, és ezt mint sorvektort jobbról szorozva a $\mathbf{G} = (\mathbf{I}, \mathbf{P})$ mátrixszal megkapjuk az eredeti üzenetet.

A legfeljebb három hiba felléphet úgy is, hogy mindkét félre esik hiba. Ekkor az egyik félben lévő hibahelyek száma biztosan 1, a másik félben pedig 1 vagy 2 hiba van. Az első esetben mindkét ellenőrzésnél egy 1-súlyú és egy legalább 7-súlyú oszlopot adunk össze, és így az összeg súlya legalább 6. A másik esetben az egyik ellenőrzésnél az egységmátrix két oszlopának összegéhez adjuk hozzá a másik fél egyetlen oszlopát, ezért most az összeg legalább $7 - 2 = 5$ darab 1-et tartalmaz, a súly ez esetben is legalább 5. A másik ellenőrzésnél az egységmátrixból egy oszlop van az összegben egy darab 1-essel. A másik oldalon két oszlopot adunk össze. A két oszlop összege minden esetben hat nullától különböző komponenst tartalmaz, és ehhez hozzáadva az előbbi 1-súlyú oszlopot, az összeg súlya ismét legalább 5. Összesítve az eredményeket azt kaptuk, hogy amikor a legfeljebb három hibából mindkét félre jut legalább egy, akkor a szindróma súlya mindkét ellenőrzésnél legalább 5.

Az előbbi esetek láthatóak táblázatos formában a 6. táblázatban, ha $w(\mathbf{s}) = u$ és $w(\mathbf{s}') = v$.

u	v	a hiba
0	0	nincs hiba
$0 < u \leq 3$	$5 \leq v$	legfeljebb 3 hiba a paritásrészben, az adatrész hibátlan
$5 \leq u$	$0 < v \leq 3$	legalább 1 és legfeljebb 3 hiba az adatrészben, és ez azonos $\mathbf{s}'$-vel
$5 \leq u$ és egy $\mathbf{u}^{(i)}$-vel pontosan az egyikre 1 és 3 közé esik (a határok is jók), míg a másiknál legalább 5	$5 \leq v$	az egyik részben pontosan 1 hiba, a másikban legfeljebb 2, és $\mathbf{u}^{(i)}$-vel korrigálhatunk
minden más esetben		3-nál több hiba

6. táblázat

Most a következő módon történik a korrigálás. Valamelyik félben egyetlen hiba van. Ha ezen a pozíción a vett szóhoz hozzáadunk e-t, akkor ebben a szóban a hibák száma legfeljebb kettő, és csak az egyik fél lesz hibás. Ám ez már javítható hibaminta, és javítás után az előbbi helyen ismét megfordítva az ott található jegyet, a hibátlan üzenetet kapjuk. Ezek szerint az ilyen hiba úgy javítható, hogy sorban egymás után megváltoztatjuk a vett szó egy-egy jegyét és elvégezzük az ellenőrzéseket egészen addig, míg éppen az egy hiba helyén történik a módosítás, amikor már tudunk javítani. Ha egyik változtatásnál sem vagyunk eredményesek (vagyis egyszer sem kapunk olyan eredményt, hogy a két ellenőrzés egyikénél a szindróma súlya legfeljebb 3, a másiknál legalább 5), akkor a hibák száma meghaladja a hármat. □

18. A Reed-Muller kód

Legyen m nemnegatív egész szám, és f az $\mathbb{F}_q$ testet önmagába képező m-változós függvény. A véges testek elméletéből ismeretes, hogy ekkor van egy és csak egy m-határozatlanú, minden határozatlanban legfeljebb $q-1$-edfokú, $\mathbb{F}_q$ fölötti olyan p polinom, hogy a p-hez tartozó $\hat{p}$ polinomfüggvény azonos f-fel. Az f-hez tartozó polinom például $p=\sum_{\mathbf{u}\in\mathbb{F}_q^m} f(\mathbf{u})\prod_{i=0}^{m-1}(e-(x_i-u_i)^{q-1})$ alakban írható fel. $\mathbb{F}_q[x_0,\cdots,x_{m-1}]$ q^m-dimenziós lineáris tér $\mathbb{F}_q$ fölött, és a tér egy bázisa a monomok összessége, azaz az $S_k=\prod_{i=0}^{m-1}x_i^{k_i}$ polinomok, ahol $k=\sum_{i=0}^{m-1}k_iq^i$. Hasonlóan, az $f\colon \mathbb{F}_q^m\to\mathbb{F}_q$ függvények is q^m-dimenziós teret alkotnak a q-elemű test fölött, és ennek a térnek egy bázisát azok a függvények alkotják, amelyek értéke pontosan egy pontban e. Az is ismeretes, hogy az előbbi két tér között invertálható lineáris kapcsolat van, amely p-t $\hat{p}$-re képezi. Az előbb megadott bázisokkal a transzformáció mátrixát rekurzívan is megadhatjuk. Rendezzük a test elemeit tetszőleges sorrendbe, azaz legyen a test j-indexű eleme a_j, azzal a megkötéssel, hogy $a_0=0$. Ekkor $m=0$-nál a mátrix $\mathbf{A}_q^{(0)}=(e)$, $\mathbf{A}_q^{(1)}$-ben a $q>i\in\mathbb{N}$, $q>j\in\mathbb{N}$ indexpárhoz tartozó elem $a_{i,j}^{(1)}=\delta_{i,0}e-a_j^{q-1-i}$, és $\mathbf{A}_q^{(m+1)}=\mathbf{A}_q^{(1)}\otimes\mathbf{A}_q^{(m)}$, ahol $\otimes$ a Kronecker-szorzást jelöli.

A $q=2$ esetben a polinomok a Zsegalkin- vagy Boole-polinomok, és a függvények a Boole-függvények. Ez esetben $a_0=0$ és $a_1=e$, $\mathbf{A}^{(1)}=\mathbf{A}_2^{(1)}=\begin{pmatrix}e & 0\\ e & e\end{pmatrix}$ és $\mathbf{A}^{(m+1)}=\mathbf{A}_2^{(m+1)}=\begin{pmatrix}\mathbf{A}^{(m)} & \mathbf{0}^{(m)}\\ \mathbf{A}^{(m)} & \mathbf{A}^{(m)}\end{pmatrix}$ ($\mathbf{0}^{(m)}$ a 2^m-edrendű nullmátrix). $\mathbf{A}^{(m)}$ inverze önmaga.

Az $m+1$-határozatlanú p Zsegalkin-polinom $p=p^{(0)}+x_mp^{(1)}$ alakban írható, ahol a $p^{(0)}$ és $p^{(1)}$ polinom egyaránt az m darab $x_0,\cdots,x_{m-1}$ határozatlanok polinomja. Ha $\mathbf{u}^{(0)}$ és $\mathbf{u}^{(1)}$ a két polinom együtthatóiból álló vektor, akkor a p-t meghatározó vektor $\mathbf{u}^{(0)}|\mathbf{u}^{(1)}$, vagyis az a 2^{m+1}-komponensű vektor, amelynek a $0\cdots 2^m-1$-indexhez tartozó komponenseiből álló vektor $\mathbf{u}^{(0)}$, és $\mathbf{u}^{(1)}$ a többi indexhez tartozó komponens vektora. A megfelelő polinomfüggvény vektora ennek megfelelően

$$\mathbf{v}=\begin{pmatrix}\mathbf{v}^{(0)}\\ \mathbf{v}^{(1)}\end{pmatrix}=\begin{pmatrix}\mathbf{A}^{(m)} & \mathbf{0}^{(m)}\\ \mathbf{A}^{(m)} & \mathbf{A}^{(m)}\end{pmatrix}\begin{pmatrix}\mathbf{u}^{(0)}\\ \mathbf{u}^{(1)}\end{pmatrix}=\begin{pmatrix}\mathbf{A}^{(m)}\mathbf{u}^{(0)}\\ \mathbf{A}^{(m)}\mathbf{u}^{(0)}+\mathbf{A}^{(m)}\mathbf{u}^{(1)}\end{pmatrix}=\begin{pmatrix}\mathbf{w}^{(0)}\\ \mathbf{w}^{(0)}+\mathbf{w}^{(1)}\end{pmatrix}.$$

A fenti eredményeket felhasználjuk a most definiálandó kód tulajdonságainak vizsgálatánál.

18.1. Definíció

Legyen m nemnegatív egész szám és $m\geq r\in\mathbb{N}$. Az $\mathbb{F}_2$ fölötti, m-határozatlanú, legfeljebb r-edfokú polinomokhoz tartozó polinomfüggvények összessége az (r,m)-**paraméterű**, vagy másképpen a 2^m-**szóhosszúságú**, r-**edrendű Reed-Muller kód**, röviden RM-**kód** A kódot $\mathcal{RM}(r,m)$-mel jelöljük. Δ

A kódot más módon is lehet definiálni, a további lehetőségek közül majd látunk megoldásokat.

Mivel egy legfeljebb r-edfokú polinom ugyanazon határozatlanok legfeljebb $r+1$-edfokú polinomja is, ezért a definícióból adódik, hogy $m>r\in\mathbb{N}$ esetén $\mathcal{RM}(r,m)$ lineáris altere $\mathcal{RM}(r+1,m)$-nek. Az is igaz, hogy ha az $m+1$-határozatlanú polinomgyűrűben rögzítünk egy határozatlant, akkor olyan polinomok összege és konstansszorosa, amelyben a rögzített határozatlan kitevője 0, szintén ilyen tulajdonságú, vagyis az ilyen polinomok összessége lineáris altere a teljes térnek, és ebben az altérben alteret alkotnak a legfeljebb $r+1$-edfokú polinomok. Ez pedig azt jelenti, hogy $\mathcal{RM}(r+1,m)$ ekvivalens $\mathcal{RM}(r+1,m+1)$ egy lineáris részkódjával. Az első megállapítás szerint $\mathcal{RM}(r+1,m+1)$-ben van $\mathcal{RM}(r,m)$-mel ekvivalens részkód is.

Határozzuk meg a Reed-Muller kódok paramétereit.

18.2. Tétel

$\mathcal{RM}(r,m)$ egy 2^m-szóhosszúságú lineáris kód. $\mathcal{RM}(0,m)$ a $[2^m,1,2^m]_2$-paraméterű ismétléses kód, míg $\mathcal{RM}(m,m)$ a $[2^m,2^m,1]_2$-paraméterű kód, azaz a teljes tér.

Δ

Bizonyítás:

Az m-határozatlanú Boole-polinomok lineáris teret alkotnak, és összeadásnál, valamint konstanssal való szorzásnál a fokszám biztosan nem nő, így a legfeljebb r-edfokú polinomok összege és konstansszorosa is ilyen tulajdonságú, az ilyen polinomok összessége alteret alkot. A tér bázisa a monomok összessége. A monomok száma az m határozatlant tartalmazó halmaz összes lehetséges részhalmazának halmaza (mert Boole-polinomban minden határozatlan kitevője 0 vagy 1), azaz 2^m, így az együtthatók vektora a kételemű test fölötti 2^m-dimenziós tér egy eleme, egy 2^m-komponensű vektor.

A legfeljebb 0-fokú polinomok a konstans polinomok, az ezekhez tartozó függvények értéke minden pontban az adott konstans, vagyis a két kódszó a csupa 0-t tartalmazó szó és a minden pontban 1-értékű szó. A kódnak két eleme van, azaz a kód egydimenziós altér, és a kód két különböző kódszava minden komponensében különbözik, amiből kapjuk a kód távolságát.

A másik szélső esetben $r = m$. Mivel minden határozatlan legfeljebb az első fokon áll a polinomban, így minden monom, következésképpen minden polinom legfeljebb m-edfokú, és van m-edfokú polinom, például az összes határozatlan szorzatából álló monom. Ennek megfelelően $\mathcal{RM}(m,m)$ a kételemű test fölötti minden m-határozatlanú polinom polinomfüggvényét tartalmazza, azaz ez a kód a teljes tér. A kód távolsága most 1, hiszen például a $\prod_{i=0}^{m-1} x_i$ polinomhoz tartozó függvény egy és csak egy pontban nem nulla, abban a pontban, ahol minden változó értéke e (ez $m = 0$ esetén is igaz, mert ekkor csak a két konstans polinom van).

□

A tétel alapján a 0-adrendű kód generátormátrixa az 1×2^m-méretű $\mathbf{G}^{(0,m)} = (e \ \cdots \ e)$ mátrix, ellenőrzőmátrixa $\mathbf{H}^{(0,m)} = \begin{pmatrix} e \\ \mathbf{I}^{(2^m-1)} \ \vdots \\ e \end{pmatrix}$, míg $\mathbf{G}^{(m,m)} = \mathbf{I}^{(2^m)}$, $\mathbf{H}^{(m,m)} = (\ \ )$ (azaz nincs ellenőrzés, hiszen ez esetben a tér minden eleme kódszó). $\mathbf{I}^{(t)}$ a nemnegatív egész t-vel a t-edrendű egységmátrix.

A fentebbi speciális paraméterű kódok alapján könnyen kapjuk általános esetben is a kódot.

18.3. Tétel

Legyen $0 < m$ egész szám és $m > r \in \mathbb{N}$. Ekkor $\mathcal{RM}(r+1,m+1)$ a 2^m-szóhosszúságú $r+1$-edrendű, valamint az ugyanilyen szóhosszúságú, r-edrendű RM-kód $\mathbf{u}, \mathbf{u}+\mathbf{v}$-konstrukciója.

Δ

Bizonyítás:

A fejezet elején láttuk, hogy az $m+1$-határozatlanú, legfeljebb $r+1$-edfokú Boole-polinom felírható $p = p^{(0)} + x_m p^{(1)}$ alakban, ahol $p^{(0)}$ és $p^{(1)}$ egyaránt az m darab $x_0, \cdots, x_{m-1}$ határozatlanok polinomja. Azt is láttuk, hogy ennek következtében a p-hez tartozó polinomfügvény spektruma, azaz a megfelelő kódszó $\mathbf{v} = \begin{pmatrix} \mathbf{v}^{(0)} \\ \mathbf{v}^{(1)} \end{pmatrix} = \begin{pmatrix} \mathbf{w}^{(0)} \\ \mathbf{w}^{(0)} + \mathbf{w}^{(1)} \end{pmatrix}$, és ez éppen az $\mathbf{u}, \mathbf{u}+\mathbf{v}$-konstrukció. De $\mathbf{w}^{(0)}$ a $p^{(0)}$ és $\mathbf{w}^{(1)}$ a $p^{(1)}$ polinom által meghatározott kódszó. p-ben minden monom legfeljebb $r+1$-edfokú, így mind $p^{(0)}$, mind $x_m p^{(1)}$ is legfeljebb $r+1$-edfokú polinom. Ekkor viszont $p^{(1)}$ nem lehet r-nél magasabb fokú (mert még szorozzuk az elsőfokú x_m polinommal). Az előbbi megállapítások azt jelentik, hogy $\mathbf{w}^{(0)}$ az $\mathcal{RM}(r+1,m)$ kód eleme, míg $\mathbf{w}^{(1)} \in \mathcal{RM}(r,m)$.

□

A 18.2. és 18.3. Tétel alapján meg tudjuk határozni a Reed-Muller kódok generátor- és ellenőrző mátrixát és paramétereit. Ezt írja le a következő tétel.

18.4. Tétel

Legyen $m \in \mathbb{N}$ és $m \geq r \in \mathbb{N}$. $\mathcal{RM}(r,m)$ egy $\left[2^m, \sum_{i=0}^{r}\binom{m}{i}, 2^{m-r}\right]_2$-paraméterű kód, továbbá $\mathbf{G}^{(r+1,m+1)} = \begin{pmatrix} \mathbf{G}^{(r+1,m)} & \mathbf{G}^{(r+1,m)} \\ \mathbf{0}^{(k^{(r)},2^m)} & \mathbf{G}^{(r,m)} \end{pmatrix}$ és $\mathbf{H}^{(r+1,m+1)} = \begin{pmatrix} \mathbf{H}^{(r+1,m)} & \mathbf{0}^{(2^m-k^{(r+1)},2^m)} \\ -\mathbf{H}^{(r,m)} & \mathbf{H}^{(r,m)} \end{pmatrix}$ a kód generátor- és ellenőrző mátrixa, ha $m > r \geq 0$.

Δ

A tételben $k^{(r)}$ az $\mathcal{RM}(r,m)$ kód dimenziója, és $\mathbf{0}^{(s,t)}$ az $s \times t$-méretű nullmátrix, ahol s és t nemnegatív egész szám. Egyébként, tekintettel arra, hogy a kód bináris, $\mathbf{H}^{(r+1,m+1)}$-ben $-\mathbf{H}^{(r,m)}$ helyett $\mathbf{H}^{(r,m)}$ írható.

Bizonyítás:

A szóhosszúság következik a definícióból, a genetátor- és ellenőrző mátrix pedig az $\mathbf{u}, \mathbf{u}+\mathbf{v}$ konstrukcióból. A k_1-dimenziós, d_1 távolságú C_1 és k_2-dimenziós, d_2 távolságú C_2 kódból a konstrukcióval kapott kód egy $k_1 + k_2$-dimenziós, $\min(2d_1, d_2)$-távolságú kód. A 0-adrendű kód 1-dimenziós, és $1 = \sum_{i=0}^{0}\binom{m}{i}$, a távolsága $2^m = 2^{m-0}$, és az m-edrendű kódnál a dimenzió $2^m = \sum_{i=0}^{m}\binom{m}{i}$ és a távolság $1 = 2^{m-m}$. Indukcióként tegyük fel, hogy egy nemnegatív egész m esetén minden lehetséges r-nél igaz, hogy a kód $k^{(r,m)} = \sum_{i=0}^{r}\binom{m}{i}$-dimenziós és $d^{(r,m)} = 2^{m-r}$-távolságú. Ekkor a 2^{m+1}-szóhosszúságú, $r+1$-edrendű kód dimenziója

$$\begin{aligned} k^{(r+1,m+1)} = k^{(r+1,m)} + k^{(r,m)} &= \sum_{i=0}^{r+1}\binom{m}{i} + \sum_{i=0}^{r}\binom{m}{i} \\ &= \binom{m}{0} + \sum_{i=1}^{r+1}\binom{m}{i} + \sum_{i=1}^{r+1}\binom{m}{i-1} \\ &= \binom{m+1}{0} + \sum_{i=1}^{r+1}\binom{m+1}{i} = \sum_{i=0}^{r+1}\binom{m+1}{i}, \end{aligned}$$

és a távolsága $d^{(r+1,m+1)} = \min\left(2 \cdot 2^{m-(r+1)}, 2^{m-r}\right) = 2^{m-r}\left(= 2^{(m+1)-(r+1)}\right)$.

□

$r = 0$-ra és $r = m$-re már láttuk a 2^m-szóhosszúságú, r-edrendű RM-kódokat. Az $r = m-1$-edrendű kód is egyszerű. $2^{m-(m-1)} = 2^1 = 2$ és $\sum_{i=0}^{m-1}\binom{m}{i} = \sum_{i=0}^{m}\binom{m}{i} - \binom{m}{0} = 2^m - 1$, így ez a kód $[2^m, 2^m-1, 2]_2$-paraméterű. Ekkor a kód ellenőrző mátrixa 1×2^m-alakú, és minden eleme e. Valóban, a kód távolsága 2, tehát az ellenőrző mátrix minden oszlopa lineárisan független. Ez egyetlen komponens esetén csak úgy lehetséges, ha ez az egyetlen komponens nem 0, és ez kételemű test esetén pontosan akkor igaz, ha ez az elem e. Ezek szerint a kételemű test fölötti 2^m-dimenziós tér azon és csak azon elemei kódszavak, amelyek komponenseinek összege 0, vagyis a páros súlyú és csak a páros súlyú szavak kódszavak. Ez egyben azt is jelenti, figyelembe véve a korábbi eredményeket, hogy valahányszor $r < m$, $\mathcal{RM}(r,m)$ minden kódszava páros súlyú.

Az mindig igaz, hogy egy kódot kiterjesztve, majd ugyanezen komponensnél átszúrva az eredeti kódot kapjuk. Fordítva ez általában még akkor sem igaz, ha a kiterjesztett kódban minden szó komponenseinek összege 0, vagyis az n-hosszúságú kódban a kiterjesztés jegye $u_n = -\sum_{i=0}^{n-1} u_i$. Ha azonban egy kód minden kódszavában a komponensek összege 0, akkor bárhol átszúrva a kódot, majd utána ugyanitt az átszúrt kódszó komponensei összegének ellentettjével kiegészítve a kódot, az eredeti kódra jutunk. Bináris esetben ez azt jelenti, hogy ha minden kódszó súlya páros, akkor bárhol átszúrva a kódot, ugyanezen pozíción egy párosra kiegészítő jeggyel kiterjesztve a kódot visszajutunk az eredeti kódhoz. Ezen ismeret birtokában nézzük meg $m \geq 2$ esetén az $m-2$-edrendű Reed-Muller kódot.

A kód paramétereinek meghatározásával kezdjük. A távolság $2^{m-(m-2)} = 2^2 = 4$, a kód dimenziója $\sum_{i=0}^{m-2}\binom{m}{i} = \sum_{i=0}^{m}\binom{m}{i} - \left(\binom{m}{0} + \binom{m}{1}\right) = 2^m - (1+m) = 2^m - 1 - m$, és a kód szóhosszúsága 2^m. A kód minden kódszava páros súlyú, és bárhol átszúrva egy $[2^m - 1, 2^m - 1 - m, 3]_2$-paraméterű lineáris kódot kapunk. Ám az m ellenőrző jegyet tartalmazó bináris Hamming-kódnak ugyanezek a paraméterei, és minden olyan lineáris kód, amelynek a paraméterei megegyeznek egy Hamming-kód paramétereivel, ekvivalens az adott paraméterű Hamming-kóddal. Ebből viszont következik, hogy ha $m \geq 2$, azaz létezik $\mathcal{RM}(m-2, m)$, akkor ez a kód ekvivalens a 2^m-szóhosszúságú kiterjesztett Hamming-kóddal, tehát lényegében véve meg is egyezik vele.

A Reed-Muller kódok egy fontos tulajdonsága, hogy van olyan generátormátrixuk, amelynek minden eleme minimális súlyú kódszó. Ezt ismét indukcióval tudjuk könnyen bizonyítani. A 0-adrendű kód ismétléses kód, egyetlen nem nulla kódszava van, ez generálja a kódot, és ez nyilván minimális súlyú. Az m-edrendű kód a teljes tér, egy lehetséges generátormátrixa az egységmátrix, amelynek minden sora 1-súlyú, azaz minimális súlyú kódszó. $m = 1$ esetén tehát minden érvényes r-re igaz az állítás. Tegyük most fel ugyanezt egy adott pozitív egész m esetén, és nézzük az eggyel nagyobb m-hez tartozó kódokat. $\mathcal{RM}(0, m+1)$-re és $\mathcal{RM}(m+1, m+1)$-re már láttuk, hogy igaz az állítás. Ha $0 \leq r < m$ egész szám, akkor $\mathcal{RM}(r+1, m+1)$ generátormátrixa $\mathbf{G}^{(r+1,m+1)} = \begin{pmatrix} \mathbf{G}^{(r+1,m)} & \mathbf{G}^{(r+1,m)} \\ \mathbf{0}^{(k^{(r)},2^m)} & \mathbf{G}^{(r,m)} \end{pmatrix}$. Az indukciós feltevés szerint $\mathbf{G}^{(r,m)}$ és $\mathbf{G}^{(r+1,m)}$ választható úgy, hogy minden sora az adott kód minimális súlyú kódszava. $\mathcal{RM}(r+1, m+1)$ távolsága 2^{m-r}, ugyanennyi az $\mathcal{RM}(r, m)$ távolsága , valamint az $\mathcal{RM}(r+1, m)$ kód távolságának kétszerese. De ekkor $\left(\mathbf{0}^{(k^{(r)},2^m)} \;\; \mathbf{G}^{(r,m)}\right)$ minden sorának súlya 2^{m-r}, és, mivel $\mathbf{G}^{(r+1,m)}$-ben minden sorban 2^{m-1-r} nem nulla elem van, ezért $\left(\mathbf{G}^{(r+1,m)} \;\; \mathbf{G}^{(r+1,m)}\right)$ minden sorában a nem nulla elemek száma $2 \cdot 2^{m-1-r}$, azaz ismét 2^{m-r}.

Nézzük a kódok duálisát. $\mathcal{RM}(m, m)$ a teljes tér, így a duálisa a 0-dimenziós tér, azaz a nullvektort és csak a nullvektort tartalmazó tér. Az ezen tér szerinti kód egyetlen kódszót tartalmaz, a $\mathbf{0}$-t.

$\mathcal{RM}(0, m)$ ellenőrző mátrixa egyetlen sort tartalmaz, és a sor minden eleme e. Ekkor az ellenőrzés eredménye akkor és csak akkor 0, ha a vizsgált szó komponenseinek összege 0, azaz a kételemű test esetén pontosan akkor, ha a nem nulla komponensek száma páros. A 0-drendű kód duálisa tehát a teljes tér páros súlyú elemeit és csak ezeket tartalmazza. Ez a kód viszont, mint már korábban láttuk, éppen $\mathcal{RM}(m-1, m)$. Ebből természetesen $\mathcal{RM}(m-1, m)$ duálisát is megkaptuk, hiszen duális duálisa az eredeti kód, vagyis $\mathcal{RM}(m-1, m)$ duálisa $\mathcal{RM}(0, m)$. Egyúttal azt is látjuk, hogy a 0-adrendű kód ellenőrző mátrixa generálja az $m-1$-edrendű kódot, és ez a másik irányban is igaz.

Megmutatjuk, hogy általában is, $\mathcal{RM}(r, m)$ duálisa $\mathcal{RM}(m-1-r, m)$, ha $r < m$.

Mivel lineáris kód duálisának generátormátrixa az eredeti kód ellenőrző mátrixa, ezért azt kell igazolni, hogy ha r kisebb, mint m, akkor $\mathbf{H}^{(m-1-r,m)}$ $\mathcal{RM}(r, m)$-et generálja.

$r = 0$-ra és $r = m-1$-re már láttuk, hogy ez igaz. Nézzük a többi esetet. Tegyük fel, hogy egy pozitív egész m-nél $m > r \in \mathbb{N}$-re $\mathcal{RM}(r, m)$-nek generátormátrixa $\mathbf{H}^{(m-1-r,m)}$. Megmutatjuk, hogy ekkor $0 \leq r < m$ esetén $\mathcal{RM}(r+1, m+1)$-et generálja $\mathbf{H}^{((m+1)-1-(r+1),m+1)}$.

Mivel $\mathcal{RM}(r, m)$ lineáris altere az $r+1$-edrendű kódnak, ha $r < m$, ezért az utóbbi kódnak van olyan $\mathbf{G}^{(r+1,m)}$ generátormátrixa, amely $\begin{pmatrix} \mathbf{G}^{(r,m)} \\ \mathbf{B} \end{pmatrix}$ alakú. Ekkor

$$\begin{aligned}
\mathbf{G}^{(r+1,m+1)} &= \begin{pmatrix} \mathbf{G}^{(r+1,m)} & \mathbf{G}^{(r+1,m)} \\ \mathbf{0}^{(k^{(r)},2^m)} & \mathbf{G}^{(r,m)} \end{pmatrix} = \begin{pmatrix} \mathbf{G}^{(r,m)} & \mathbf{G}^{(r,m)} \\ \mathbf{B} & \mathbf{B} \\ \mathbf{0}^{(k^{(r)},2^m)} & \mathbf{G}^{(r,m)} \end{pmatrix} \sim \begin{pmatrix} \mathbf{G}^{(r,m)} & \mathbf{G}^{(r,m)} \\ \mathbf{B} & \mathbf{B} \\ \mathbf{G}^{(r,m)} & \mathbf{0}^{(k^{(r)},2^m)} \end{pmatrix} \\
&= \begin{pmatrix} \mathbf{G}^{(r+1,m)} & \mathbf{G}^{(r+1,m)} \\ \mathbf{G}^{(r,m)} & \mathbf{0}^{(k^{(r)},2^m)} \end{pmatrix} \sim \begin{pmatrix} \mathbf{G}^{(r,m)} & \mathbf{0}^{(k^{(r)},2^m)} \\ \mathbf{G}^{(r+1,m)} & \mathbf{G}^{(r+1,m)} \end{pmatrix} = \begin{pmatrix} \mathbf{H}^{(m-1-r,m)} & \mathbf{0}^{(k^{(r)},2^m)} \\ \mathbf{H}^{(m-1-(r+1),m)} & \mathbf{H}^{(m-1-(r+1),m)} \end{pmatrix} \\
&= \mathbf{H}^{(m-1-r,m+1)} = \mathbf{H}^{((m+1)-1-(r+1),m+1)}.
\end{aligned}$$

Bebizonyítottuk tehát a következő tételt.

18.5. Tétel

Legyen $m \in \mathbb{N}^+$ és $m > r \in \mathbb{N}$. Ekkor $\mathcal{RM}(r,m)$ duálisa $\mathcal{RM}(m-1-r,m)$.

Δ

Legyen p egy m-határozatlanú polinom egy tetszőleges $\mathcal{R}$ gyűrű fölött, és legyen $m > i \in \mathbb{N}$-re $p^{(i)}$ ugyanazon gyűrű fölötti, ugyanazon határozatlanok polinomja (ez a feltevés semmiben nem korlátoz, mert tekinthetjük p és minden $p^{(i)}$ határozatlanjainak összességét, és valamennyi polinom felírható ezen összes határozatlan polinomjaként úgy, hogy ha valamely határozatlant eredetileg nem tartalmazta, akkor az 0-kitevővel álljon). Ha $\mathbf{p}$ a $p^{(i)}$ polinomok rendezett m-ese, a polinomok vektora, akkor képezhetjük p és $\mathbf{p}$ kompozícióját, $p \circ \mathbf{p}$-t. Azonban $m > 1$ esetén nem mindegy, hogy ezt a kompozíciót hogyan képzeljük el. Az eléggé nyilvánvaló, hogy $p^{(i)}$-t az x_i határozatlan helyére írjuk. Lényeges azonban, hogy a helyettesítés valamennyi határozatlanra egyszerre történik. Ha ugyanis nem így teszünk, akkor a végeredmény függhet a helyettesítések sorrendjétől is.

Speciális esetként legyen $\mathbf{A}$ az $\mathcal{R}$ gyűrű fölötti m-edrendű mátrix, és $\mathbf{a}$ szintén a gyűrű feletti m-komponensű vektor. Ha $\mathbf{p} = \mathbf{Ax} + \mathbf{a}$, ahol $\mathbf{x}$ a határozatlanokat tartalmazó vektor, akkor könnyen látható, hogy r-edfokú tagból legfeljebb r-edfokú tagot kapunk, hiszen a helyettesítésnél minden határozatlant, azaz minden, legfeljebb elsőfokú polinomot egy legfeljebb elsőfokú polinommal helyettesítünk. Ebből következik, hogy helyettesítésnél a polinom fokszáma nem nő. Abban az esetben, ha $\mathbf{A}$ invertálható, akkor ez visszafelé is igaz, és ebből következően ilyen esetben a kompozíció során az eredetivel megegyező fokszámú polinomot kapunk. Invertálható esetben az inverz transzformáció is hasonló alakú, hiszen $(\mathbf{Ax} + \mathbf{a}) \circ \left(\mathbf{A}^{-1}\mathbf{x} + (-\mathbf{A}^{-1}\mathbf{a})\right) = \mathbf{x}$. Két ilyen transzformáció kompozíciója is ilyen alakú: $(\mathbf{Ax} + \mathbf{a}) \circ (\mathbf{Bx} + \mathbf{b}) = (\boldsymbol{AB})\mathbf{x} + (\mathbf{Ab} + \mathbf{a}) = \mathbf{Cx} + \mathbf{c}$, és invertálható mátrixok szorzata is invertálható. Ezek szerint az $\mathcal{R}$ fölötti m-edrendű, invertálható $\mathbf{A}$ mátrixokkal és $\mathbf{a}$ m-komponensű vektorokkal az $\mathbf{x} \mapsto \mathbf{Ax} + \mathbf{a}$ alakú transzformációk csoportot alkotnak. Ez a csoport az $\mathcal{R}$ **fölötti** m**-edrendű általános affin csoport**, elemei az **affin transzformáció**k, vagy **affin leképezés**ek, és ennek a csoportnak részcsoportja az $\mathbf{x} \mapsto \mathbf{Ax}$ leképezések összessége, az $\mathcal{R}$ **fölötti** m**-edrendű általános lineáris csoport** a **lineáris transzformáció**kkal, **lineáris leképezés**ekkel. A két csoportot az előbbi sorrendben $AGL(m,\mathcal{R})$ és $GL(m,\mathcal{R})$ jelöli. Abban a speciális esetben, amikor a gyűrű a q-elemű test, szokásosabb az előbbiek helyett az $AGL(m,q)$ és $GL(m,q)$ jelölés.

Könnyű meghatározni $AGL(m,q)$ és $GL(m,q)$ elemeinek számát. Az utóbbi a q-elemű test fölötti m-edrendű, reguláris mátrixok száma. A mátrixnak m sora van. Az első sor bármi lehet a csupa 0-t tartalmazó sor kivételével. Ilyen sor $q^m - 1$ van. A második sor csupán az első sor konstansszorosa nem lehet. Mivel a sornak q különböző konstansszorosa van, ezért a második sor választási lehetőségeinek száma $q^m - q$. Legyen t az m-nél kisebb nemnegatív egész szám. Ha már megválasztottuk az első t sort úgy, hogy a sorok lineárisan függetlenek, akkor a következő sor választásánál a már meglévő sorok által kifeszített altér elemein kívül bármely sor választható. Az altér t-dimenziós, és a sorok együtthatói összesen q^t-féleképpen választhatóak, vagyis a tér összes vektora, a q^m vektor közül ennyit nem választhatunk, ha azt akarjuk, hogy a sorok továbbra is legyenek lineárisan függetlenek. A választási lehetőségek száma ennek megfelelően $q^m - q^t$. Az egyes sorok választási lehetőségeinek száma szorzódik, így a q-elemű test fölötti reguláris, m-edrendű mátrixok száma $|GL(m,q)| = \prod_{i=0}^{m-1}\left(q^m - q^i\right)$. Ebből már könnyen adódik az affin transzformációk száma, hiszen minden mátrixhoz, attól teljesen függetlenül bármely vektor választható. Ezzel $|AGL(m,q)| = q^m|GL(m,q)| = q^m \prod_{i=0}^{m-1}\left(q^m - q^i\right)$, mert a vektorok száma q^m.

$AGL(m,q)$ kétszeresen tranzitív, míg $GL(m,q)$ nem tranzitív, de egyszeresen tranzitív, ha csak $\mathbb{F}_q^m \setminus \{\mathbf{0}\}$ pontjait tekintjük.

Az, hogy $GL(m,q)$ nem tranzitív, rögtön következik abból, hogy lineáris transzformációnál a $\mathbf{0}$ képe csak $\mathbf{0}$ lehet. Ugyanakkor nem nulla vektor mindig kiegészíthető a tér egy bázisává, és van egy és csak egy olyan lineáris transzformáció, amely a tér egy bázisát a tér egy másik – az előbbitől nem feltétlenül különböző – másik bázisára képezi. Ha tehát $\mathbf{u}$ és $\mathbf{v}$ tetszőleges nem nulla vektorok, akkor az előbbit tartalmazó bázist az utóbbi kiegészítésével nyert bázisra képező lineáris transzformáció $\mathbf{u}$-t $\mathbf{v}$-be transzformálja, a csoport a $\mathbf{0}$-tól különböző elemek halmazán legalább egyszeresen tranzitív. Általában azonban nem lehet kétszeresen tranzitív, mert egy vektort és ennek egy tőle különböző, nem nulla konstansszorosát nem tudjuk két lineárisan független vektorba átvinni. De kétszeresen tranzitív, ha $q = 2$

és $m > 1$, mert ekkor egy nem nulla vektor akkor és csak akkor konstansszorosa egy másik nem nulla vektornak, ha a két vektor azonos. Ám ez esetben is csak $m = 2$ esetén lesz háromszorosan tranzitív. Ekkor összesen három nem nulla vektor van, így a megfeleltetés egy permutáció. $m > 2$ esetén viszont egy síkban fekvő három pontot csak egy síkba eső három pontba tudunk átvinni, így már nem igaz, hogy tetszőleges három különböző pontot bármely három különböző pontba át tudunk vinni.

$q = 3$ és $m = 1$ esetén is igaz, hogy két nem nulla vektor átvihető bármely két nem nulla vektorba, hiszen ekkor egy nem nulla vektor csupán a test egy nem nulla eleme, és ilyen pontosan kettő van, vagyis a leképezés most is egyszerűen egy permutáció. Mivel csak két nem nulla elem van, ezért nyilván nem értelmezhető a legalább háromszoros tranzitivitás. És $m > 1$ esetén már a kétszeres tranzitivitás sem igaz, hasonló okból, mint az általános esetben.

Nézzük $AGL(m, q)$-t. Egy $1 < n \in \mathbb{N}$-re adott $\mathbf{u}_0, \cdots, \mathbf{u}_i, \cdots, \mathbf{u}_{n-1}$ és $\mathbf{v}_0, \cdots, \mathbf{v}_i, \cdots, \mathbf{v}_{n-1}$, mindkét esetben páronként különböző pontokkal akkor és csak akkor van olyan $\mathbf{A}$ mátrix és $\mathbf{a}$ vektor, hogy $n > i \in \mathbb{N}$-re $\mathbf{v}_i = \mathbf{A}\mathbf{u}_i + \mathbf{a}$, ha egyrészt $\mathbf{v}_0 = \mathbf{A}\mathbf{u}_0 + \mathbf{a}$, másrészt $i > 0$-ra $\mathbf{v}_i - \mathbf{v}_0 = \mathbf{A}(\mathbf{u}_i - \mathbf{u}_0)$. De ez azt jelenti, hogy $AGL(m, q)$ tranzitivitása éppen eggyel nagyobb, mint $GL(m, q)$ nullától különböző elemekre vonatkozó tranzitivitása, azaz $AGL(m, 2)$ $m > 2$ esetén, valamint $AGL(1,3)$ pontosan háromszorosan, $AGL(2,2)$ pontosan négyszeresen tranzitív, és minden más esetben $AGL(m, q)$ pontosan kétszeresen tranzitív.

Az előbbiekből kitűnik, hogy az affin transzformáció nem vezet ki az $\mathcal{RM}(r, m)$ kódból, vagyis affin transzformáció Reed-Muller kódot vele ekvivalens kódba transzformál. De ekkor a kód automorfizmus-csoportja tartalmaz tranzitív részcsoportot, következésképpen a kódot bárhol átszúrva, a kapott kódok ekvivalensek.

Most nézzük a Reed-Muller kódok dekódolását.

Legyen P egy $\mathbb{F}_2$ fölötti, m-határozatlanú, legfeljebb r-edfokú polinom, ahol m és az m-nél nem nagyobb r pozitív egész szám, és legyen f a polinomhoz tartozó Boole-függvény. A feltételek alapján a polinom $P = \sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|\le r}} c_U \mathbf{x}^U$ alakú, ahol $\mathbb{N}_m = \{k \in \mathbb{N} | m > k\}$, $\mathbf{x} = (x_0, \cdots, x_{m-1})$ és $\mathbf{x}^U = \prod_{i\in U} x_i$. P felírható $P = \sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|\le r}} c_U \mathbf{x}^U = \sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|= r}} c_U \mathbf{x}^U + \sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|< r}} c_U \mathbf{x}^U = P^{(r)} + P^{(<r)}$ alakban. Ha a $P^{(r)}$ által meghatározott Boole-függvény $f^{(r)}$, akkor nyilvánvaló, hogy az $f - f^{(r)}$ függvény a $P^{(<r)}$ polinomhoz, vagyis egy legfeljebb $r - 1$-edfokú polinomhoz tartozik.

Legyen most az előbbi, legfeljebb r-edfokú P polinomhoz S az $\mathbb{N}_m$ egy r-elemű részhalmaza. Ekkor

$$U = U \cap \mathbb{N}_m = U \cap (S \cup \bar{S}) = U \cap (S \Delta \bar{S}) = (U \cap S) \Delta (U \cap \bar{S}) = (U \cap S) \Delta (U \backslash S),$$

és ezt alkalmazva

$$P = \sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|\le r}} c_U \mathbf{x}^U = \sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|\le r}} c_U \mathbf{x}^{(U\cap S)\Delta(U\backslash S)} = \sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|\le r}} c_U \mathbf{x}^{U\backslash S} \mathbf{x}^{U\cap S}$$

$$= \sum_{T\subseteq S} \left(\sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|\le r \wedge U\cap S = T}} c_U \mathbf{x}^{U\backslash S} \right) \mathbf{x}^T = c_S \mathbf{x}^S + \sum_{T\subsetneq S} \left(\sum_{\substack{U\subseteq\mathbb{N}_m \\ |U|\le r \wedge U\cap S = T}} c_U \mathbf{x}^{U\backslash S} \right) \mathbf{x}^T.$$

Az utolsó egyenlőséget úgy kapjuk, hogy S-nek egyetlen olyan részhalmaza van, amelynek r eleme van, maga az S halmaz. $\mathbf{a} \in 2^{\mathbb{N}_m}$-re jelölje $\mathbf{a}^U$ az $\widehat{\mathbf{x}^U}(\mathbf{a}) = \prod_{i\in U} a_i$ értéket és $\mathbf{b} = \mathbf{a}|_U \in 2^U$ azt a Boole-vektort, amelynél $i \in U$-ra $b_i = a_i$. Ha

$$P^{(\mathbf{a}|_{\bar{S}})} = c_S\mathbf{x}^S + \sum_{T\subsetneq S}\left(\sum_{\substack{U\subseteq\mathbb{N}_m\\ |U|\le r\wedge U\cap S=T}} c_U(\mathbf{a}|_{\bar{S}})^{U\setminus S}\right)\mathbf{x}^T = c_S\mathbf{x}^S + \sum_{T\subsetneq S} v_T^{(S)}\mathbf{x}^T,$$

akkor tetszőleges, rögzített $\mathbf{b}\in 2^{\bar{S}}$ esetén

$$\sum_{\substack{\mathbf{a}\in 2^{\mathbb{N}m}\\ \mathbf{a}|_{\bar{S}}=\mathbf{b}}}\hat{P}(\mathbf{a}) = \sum_{\mathbf{a}\in 2^S}\widehat{P^{(\mathbf{b})}}(\mathbf{a}) = \sum_{\mathbf{a}\in 2^S}\left(c_S\mathbf{a}^S + \sum_{T\subsetneq S} v_T^{(S)}\mathbf{a}^T\right)$$
$$= \sum_{\mathbf{a}\in 2^S} c_S\mathbf{a}^S + \sum_{T\subsetneq S}\sum_{\mathbf{a}\in 2^S} v_T^{(S)}\mathbf{a}^T = c_S,$$

ugyanis $\mathbf{a}\in 2^S$-nél $\mathbf{a}^S = \prod_{i\in S} a_i$ akkor és csak akkor 1, amikor minden i-re $a_i = 1$, míg $T\subsetneq S$ következtében $2\left|2^{S\setminus T}\right| = 2^{|S\setminus T|}$, így $\mathbf{a}^T$-nek páros sokszor azonos az értéke, ennélfogva minden $T\subsetneq S$ esetén $\sum_{\mathbf{a}\in 2^S} v_T^{(S)}\mathbf{a}^T = 0$.

Az előbbi eredmény szerint c_S nem függ a $\mathbf{b}$ választásától, az értéke mindig ugyanaz. Ezt használjuk ki a dekódolásnál. Mivel minimális távolságú dekódolásnál hibát javítani csak legalább 3-távolságú kódnál lehet, és $\mathcal{RM}(r,m)$ távolsága 2^{m-r}, ezért $m-r\ge 2$. Legyen $f\colon \mathbb{F}_2^m\to\mathbb{F}_2$ egy m-változós Boole-függvény, amely az $\mathcal{RM}(r,m)$ kód egy kódszavától $2^{m-r-1} = \frac{d}{2}$-nél kevesebb helyen tér el, és legyen P az ezen kódszót meghatározó polinom. $\mathbf{b}$-t összesen $\left|2^{\mathbb{N}_m\setminus S}\right| = 2^{|\mathbb{N}_m\setminus S|} = 2^{m-r}$-féleképpen választhatjuk. Ugyanakkor f és a P-hez tartozó függvény legfeljebb $2^{m-r-1}-1$ helyen különbözik, tehát legalább $2^{m-r-1}+1 > 2^{m-r-1}-1$ helyen a két függvény megegyezik. Innen már adódik egy r-elemű S halmazhoz c_S meghatározása, ez ugyanis a különböző $\mathbf{b}$ helyeken kiszámolt $f(\mathbf{a})$ értékek többségi értéke, és így $c_S = 0$, ha $\left|\left\{\mathbf{b}\in\mathbb{F}_2^{m-r}\middle|\sum_{\substack{\mathbf{a}\in\mathbb{F}_2^m\\ \mathbf{a}|\bar{S}=\mathbf{b}}} f^{(r)}(\mathbf{a}) = 0\right\}\right| \ge \left|\left\{\mathbf{b}\in\mathbb{F}_2^{m-r}\middle|\sum_{\substack{\mathbf{a}\in\mathbb{F}_2^m\\ \mathbf{a}|\bar{S}=\mathbf{b}}} f^{(r)}(\mathbf{a}) = 1\right\}\right|$, egyébként $c_S = 1$.

A dekódolásnál az $r\ge i\in\mathbb{N}$ indexekre egy $P^{(i)}$ polinomsorozatot állítunk elő, ahol $P^{(r)} = 0$ és $P^{(i-1)} = P^{(i)} + \sum_{\substack{S\subseteq\mathbb{N}_m\\ |S|=i}} c_S\mathbf{x}^S$. Az eljárásban $f^{(r)} = f$, $f^{(i-1)} = f^{(i)} - \widehat{\sum_{\substack{S\subseteq\mathbb{N}_m\\ |S|=\imath}} c_S\mathbf{x}^S}$, és c_S értékét az előbbi módon határozzuk meg. Igazolni kell, hogy $P^{(0)} = P$.

A kód linearitása miatt elegendő megmutatni, hogy ha $w(f) < 2^{m-r-1}$, akkor $P^{(0)} = 0$. Ez az eredmény indukcióval könnyen adódik. $\left|\left\{\mathbf{b}\in\mathbb{F}_2^{m-r}\middle|\sum_{\substack{\mathbf{a}\in\mathbb{F}_2^m\\ \mathbf{a}|\bar{S}=\mathbf{b}}} f^{(r)}(\mathbf{a}) = 1\right\}\right| \le w(f) < 2^{m-r-1}$, ezért minden r-edfokú tag együtthatója 0 lesz, és így $\sum_{\substack{S\subseteq\mathbb{N}_m\\ |S|=r}} c_S\mathbf{x}^S$ a nullpolinom. De ha $\sum_{\substack{S\subseteq\mathbb{N}_m\\ |S|=r}} c_S\mathbf{x}^S = 0$, akkor $P^{(r-1)} = P^{(r)} + \sum_{\substack{S\subseteq\mathbb{N}_m\\ |S|=r}} c_S\mathbf{x}^S = P^{(r)} = 0$ és $f^{(r-1)} = f^{(r)} - \widehat{\sum_{\substack{S\subseteq\mathbb{N}_m\\ |S|=r}} c_S\mathbf{x}^S} = f^{(r)} = f$. Ha most valamely $r\ge i\in\mathbb{N}^+$-nál igaz, hogy $f^{(i)} = f$ és $P^{(i)} = 0$, akkor minden olyan $U\subseteq\mathbb{N}_m$ esetén, amelynél $i\le|U|\le r$, $c_U = 0$, így az $f^{(i-1)}$-hez legközelebbi kódszó polinomja már $\sum_{\substack{U\subseteq\mathbb{N}_m\\ |U|\le i-1}} c_U\mathbf{x}^U$ alakú. Ebben a lépésben a $\mathbf{b}$ választási lehetőségeinek a száma $2^{m-i+1} > 2^{m-i}\ge 2^{m-r}$, és $f^{(i-1)}$ súlya ugyanaz, mint f súlya, amiből következik, hogy $\sum_{\substack{S\subseteq\mathbb{N}_m\\ |S|=i-1}} c_S\mathbf{x}^S$ is a nullpolinom, és $P^{(i-1)} = 0$.

19. Függelék

Ebben a fejezetben olyan kérdésekkel foglalkozunk, amelyeket az előző részekben nem használtunk fel, de amelyek alkalmazásával a vizsgált kódok más módon tárgyalhatóak.

A kód idempotensét Perron tételével[2] is meghatározhatjuk, amelyet az eredetihez képest kicsit általánosabban adunk meg. Legyen q páratlan prímhatvány, Q az $\mathbb{F}_q$-beli négyzetelemek összessége, míg NQ a test azon elemeinek halmaza, amelyek nem négyzetei a test valamely elemének. A nullelemnek is van négyzetgyöke a testben, és a kvadratikus elemek 0-val bővített halmazát Q_0-val fogjuk jelölni. Nyilván $\{\{0\}, Q, NQ\}$ elemei páronként diszjunktak, és az uniójuk $\mathbb{F}_q$, így $|NQ| = q - |Q_0|$.

Legyen a a test egy tetszőleges, a 0-tól különböző eleme, és nézzük meg, hogy az $a + Q_0$ illetve az $a + NQ$ halmazban hány olyan elem van, amely maga is eleme Q_0-nak, vagyis $|(a + Q_0) \cap Q_0|$ és $|(a + NQ) \cap Q_0|$ értékét akarjuk meghatározni. Ez nyilván azt is meghatározza, hogy mekkora az $(a + Q_0) \cap NQ$ valamint az $(a + NQ) \cap NQ$ halmaz számossága, hiszen hasonlóan az előzőhöz, most $|(a + Q_0) \cap NQ| = |Q_0| - |(a + Q_0) \cap Q_0|$ és $|(a + NQ) \cap NQ| = |NQ| - |(a + NQ) \cap Q_0|$

Legyen $r \in Q_0$, ekkor $r = s^2$ egy $s \in \mathbb{F}_q$ elemmel. $a + r$ akkor és csak akkor eleme Q_0-nak, ha $a + r = t^2$, ahol t ismét a q-elemű test eleme, vagyis pontosan akkor, ha $a + s^2 = t^2$. Innen kapjuk, hogy $-a = s^2 - t^2 = (s + t)(s - t)$. $a \neq 0$-ból következik, hogy $s^2 - t^2 \neq 0$, tehát $s \neq \pm t$, vagyis sem $s + t$, sem $s - t$ nem nulla. Ekkor $s - t = -\frac{a}{s+t}$, $s = t - \frac{a}{s+t}$, majd $2s = (s + t) - \frac{a}{s+t} = u - \frac{a}{u}$ a test egy nullától különböző u elemével. q páratlan, ennélfogva $2e \neq 0$, oszthatunk vele, majd az így kapott elemnek a négyzetét véve oda jutunk, hogy $r = (4e)^{-1}\left(u - \frac{a}{u}\right)^2$, vagyis $a + r$ akkor és csak akkor a test egy elemének négyzete, ha $r = (4e)^{-1}\left(u - \frac{a}{u}\right)^2$ a test egy alkalmas, nem nulla u elemével. Az eredményünk azt jelenti, hogy az $a + r$ elemek között annyi lesz Q_0-beli, ahány különböző értéke van az $u \mapsto \left(u - \frac{a}{u}\right)^2$ leképezésnek, miközben u végigfut a test nem nulla elemeinek összességén. Ha $u \sim v$ az a reláció $\mathbb{F}_q^*$-ban, hogy $\left(u - \frac{a}{u}\right)^2 = \left(v - \frac{a}{v}\right)^2$, akkor ez ekvivalencia-reláció, azaz $\mathbb{F}_q^*$ egy osztályozása, egy osztály elemeihez azonos Q_0-beli elem tartozik, míg különböző osztályok Q_0 más és más elemével találkoznak. A feladatunk már csak annyi, hogy meghatározzuk az osztályok számát. Nézzük meg, mikor lesz $u \in \mathbb{F}_q$, $v \in \mathbb{F}_q$-val $\left(u - \frac{a}{u}\right)^2 = \left(v - \frac{a}{v}\right)^2$, vagy, kihasználva, hogy testben két különböző elem négyzete akkor és csak akkor azonos, ha egymás ellentettjei, mikor lesz $u - \frac{a}{u} = \pm\left(v - \frac{a}{v}\right)$. Átrendezés után kapjuk, hogy $u \mp v = \frac{a}{u} \mp \frac{a}{v} = \frac{\mp a(u-v)}{uv}$, azaz $uv(u \mp v) = \mp a(u \mp v)$. Ez az egyenlőség pontosan akkor teljesül, ha vagy $v = \pm u$, vagy $v = \mp\frac{a}{u}$.

Mivel a test páratlan elemszámú, azaz a karakterisztikája nem 2, ezért $u \neq -u$ és $\frac{a}{u} \neq -\frac{a}{u}$, ami azt jelenti, hogy ha $u \neq \pm\frac{a}{u}$, akkor egy osztály négy különböző elemet tartalmaz. Maradt az az eset, amikor $u = \frac{a}{u}$ vagy $u = -\frac{a}{u}$. Mivel egyszerre a két egyenlőség nem teljesülhet, ezért, ha adott a esetén van ilyen u, akkor az ilyen u-t tartalmazó osztálynak két eleme van, u és $-u$. $u = \pm\frac{a}{u}$ másként írva $u^2 = \pm a$, vagyis kételemű osztály akkor és csak akkor van, ha a és $-a$ legalább egyike Q eleme.

Abban az esetben, ha $q = 4k - 1$, akkor $-e$ nem négyzetelem, így a és $-a$ közül az egyik és csak az egyik eleme Q-nak, ez esetben tehát pontosan egy olyan osztály van, amely két elemet tartalmaz. A nullától különböző elemek száma most $4k - 2$, az előbbi osztály két elemét elhagyva $4k - 4$ elem marad, így a négyelemű osztályok száma $k - 1$, és ehhez jön még az egyetlen kételemű osztály, vagyis az osztályok száma, és így $(a + Q_0) \cap Q_0$ számossága most k. Mivel $|Q_0| = \frac{(4k-1)-1}{2} + 1 = 2k$, ezért a másik halmaznak, $(a + Q_0) \cap NQ$-nak is ugyanennyi eleme van.

[2] O. Perron: Bemerkungen über die Verteilung der quadratischen Reste, Mathematische Zeitschrift 56 (1952), pp. 122-130

$q = 4k + 1$ esetén vagy mind a, mind $-a$ kvadratikus elem, vagy egyikük sem az. Az előbbi esetben két darab kételemű osztály van, a másik esetben pedig nincs ilyen osztály. Most $|Q_0| = 2k + 1$, az első esetben az osztályok száma $\frac{((4k+1)-1)-2\cdot 2}{4} + 2 = k + 1$, tehát $|(a + Q_0) \cap Q_0| = k + 1$, és ennek megfelelően $|(a + Q_0) \cap NQ| = k$, míg a második esetben $|(a + Q_0) \cap Q_0| = \frac{(4k+1)-1}{4} = k$ illetve $|(a + Q_0) \cap NQ| = k + 1$.

A nem kvadratikus elemek halmazának eltolása már könnyen tárgyalható az előző eredményekkel. A feladat az NQ egy-egy rögzített eltoltja Q_0 és NQ közötti megoszlásának meghatározása, vagyis hogy hány elem kerül az egyik illetve a másik halmazba. Mivel a két halmaz idegen, és különböző elem eltoltja különböző, ezért $|NQ| = |(a + NQ) \cap NQ| + |(a + NQ) \cap Q_0|$, amiből egyszerű átrendezéssel $|(a + NQ) \cap Q_0| = |NQ| - |(a + NQ) \cap NQ|$, elegendő tehát például $|(a + NQ) \cap NQ|$ meghatározása. Ha z egy $\mathcal{K}$ test tetszőleges, nem nulla eleme, és $A \subseteq K$, akkor $|A| = |zA|$. Legyen most $\mathcal{K} = \mathbb{F}_q$, $z \in NQ$ tetszőleges, de rögzített elem, $b = za$, és $n \in NQ$. Ekkor $zn \in Q$, és $a + n \in NQ$ akkor és csak akkor, ha $b + zn = za + zn = z(a + n) \in Q$. Az eredményünk más formában azt jelenti, hogy $|(a + NQ) \cap NQ| = |z((a + NQ) \cap NQ)| = |(b + Q) \cap Q|$. A négyzetek eltolásából ismerjük már $|(b + Q_0) \cap Q_0|$ értékét. $Q_0 = \{0\} \cup Q$-ból $b + Q_0 = \{b\} \cup (b + Q)$, majd

$$\begin{aligned}(b + Q_0) \cap Q_0 &= \big(\{b\} \cup (b + Q)\big) \cap (\{0\} \cup Q) \\ &= (\{b\} \cap Q) \cup \big(\{0\} \cap (b + Q)\big) \cup \big((b + Q) \cap Q\big).\end{aligned}$$

$(\{b\} \cap Q)$-nak legfeljebb csak $b \neq 0$ az eleme, $\{0\} \cap (b + Q)$-nak pedig, ha nem üres, az egyetlen eleme a 0. $0 \notin Q$, amiből következik, hogy $0 \notin b + Q$, és így $(b + Q) \cap Q$-nak sem 0, sem b nem eleme, ami azt jelenti, hogy a három halmaz, $(\{b\} \cap Q)$, $\{0\} \cap (b + Q)$ és $(b + Q) \cap Q$ páronként diszjunkt. Ezen eredményünk alapján

$$|(a + NQ) \cap NQ| = |(b + Q) \cap Q| = |(b + Q_0) \cap Q_0| - (|\{b\} \cap Q| + |\{0\} \cap (b + Q)|),$$

ahol tehát $\{b\} \cap Q \subseteq \{b\}$ és $\{0\} \cap (b + Q) \subseteq \{0\}$. $\{b\} \cap Q = \{b\}$ akkor és csak akkor, ha $b \in Q$, vagyis b kvadratikus, míg $\{0\} \cap (b + Q) = \{0\}$-hez szükséges és elegendő, hogy egy $r \in Q$-val $b + r = 0$ legyen, azaz $-b$ legyen kvadratikus. Ismét három esetet kell szétválasztani:

- ha $n = 4k - 1$, akkor az előbbi két lehetőség közül pontosan az egyik teljesül, így ez esetben $|(a + NQ) \cap NQ| = |(b + Q_0) \cap Q_0| - 1 = k - 1$, és $|(a + NQ) \cap Q_0| = (2k - 1) - (k - 1) = k$;
- amennyiben $n = 4k + 1$ és a nem kvadratikus elem, akkor $b \in Q$ és $-b \in Q$, vagyis most $|(a + NQ) \cap NQ| = |(b + Q_0) \cap Q_0| - 2 = (k + 1) - 2 = k - 1$, és a másik halmazban lévő elemek száma $2k - (k - 1) = k + 1$;
- végül $4k + 1$-alakú n és kvadratikus a esetén mind b, mind $-b$ nem kvadratikus, így a korábbi eredményt nem kell korrigálni, $|(a + NQ) \cap NQ| = |(b + Q_0) \cap Q_0| = k$, és ebből következően ilyen n és a esetén $|(a + NQ) \cap Q_0| = 2k - k = k$.

Ezzel igazoltuk az alábbi Perron-tételt.

19.1. Tétel

Legyen q egy páratlan prím pozitív egész kitevős hatványa, $Q = \{r \in \mathbb{F}_q^* | \exists(s \in \mathbb{F}_q): s^2 = r\}$ az $\mathbb{F}_q$ kvadratikus elemeinek halmaza, $Q_0 = Q \cup \{0\}$ a test négyzetelemeinek összessége, végül NQ a nem kvadratikus elemek halmaza, és legyen a az $\mathbb{F}_q^*$ egy tetszőleges, rögzített eleme. Ekkor

1. $q = 4k - 1$ esetén $|Q| = 2k - 1 = |NQ|$, $|Q_0| = 2k$, és ekkor

   - $|(a + Q_0) \cap Q_0| = k = |(a + Q_0) \cap NQ|$;
   - $|(a + NQ) \cap Q_0| = k$, $|(a + NQ) \cap NQ| = k - 1$;

2. ha $q = 4k + 1$, akkor $|Q| = 2k = |NQ|$, $|Q_0| = 2k + 1$, és

   a) $a \in Q$-nál

   - $|(a + Q_0) \cap Q_0| = k + 1$, $|(a + Q_0) \cap NQ| = k$;
   - $|(a + NQ) \cap Q_0| = k = |(a + NQ) \cap NQ|$;

   b) $a \in NQ$ esetén

   - $|(a + Q_0) \cap Q_0| = k$, $|(a + Q_0) \cap NQ| = k + 1$;
   - $|(a + NQ) \cap Q_0| = k + 1$, $|(a + NQ) \cap NQ| = k - 1$.

Δ

Perron a tételt páratlan prím-modulusú kongruenciák kvadratikus maradékairól és nemmaradékairól bizonyította, de ez lényegében véve prímszám-elemű testet jelent, és az általános eset sem különbözik tőle.

Nézzük Perron tételével páratlan q esetében az idempotenst. $f = a + b\sum_{r\in Q} x^r + c\sum_{s\in NQ} x^s$ $\mathbb{F}_q$-beli a, b és c együtthatókkal. Ha $b = c$, akkor $f = a + b\sum_{i=1}^{p-1} x^i = (a - b) + b\sum_{i=0}^{p-1} x^i$. Ekkor tetszőleges $p > l \in \mathbb{N}^+$-nál és $\mathbb{F}_q$ fölötti α primitív p-edik egységgyöknél $\hat{f}(\alpha^l) = a - b$, ami vagy egyáltalán nem 0, vagy mind maradék-kitevővel, mind nemmaradék kitevővel 0, így ez a polinom nem lehet idempotense a kódnak. Ebből következik, hogy b nem lehet egyenlő c-vel.

Ha f idempotens, teljesülnie kell, hogy $f^2 \bmod (x^p - e) = f$. Elvégezve a négyzetre emelést

$$f^2 = a^2 + b^2 \sum_{r'\in Q}\sum_{r"\in Q} x^{r'+r"} + c^2 \sum_{s'\in NQ}\sum_{r"\in NQ} x^{s'+s"} + 2ab\sum_{r\in Q} x^r + 2ac\sum_{s\in NQ} x^s + 2bc\sum_{r'\in Q}\sum_{s"\in NQ} x^{r'+s'}.$$

Az azonos kitevőhöz tartozó tagokat összevonva lesznek x^0-, x^r- és x^s-alakú tagok. $f^2 \sim f$ csak úgy teljesülhet, ha az azonos típusú minden kitevő ugyanazzal az együtthatóval lép fel a négyzetben. Határozzuk meg ezeket az együtthatókat.

x^0-t kapunk egyrészt a^2-ben, nyilván egyszer, aztán $r' + r"$-ből, ha $-r'$ kvadratikus maradék, ez esetben minden Q-beli elem eggyel járul hozzá az együtthatóhoz. Ugyanez a helyzet $s' + s"$-nél. Végül $r' + s'$ akkor ad x^0-nak megfelelő tagot, ha $-r'$ kvadratikus nemmaradék. Mindezek alapján külön kell nézni a $p = 4k - 1$ és a $p = 4k + 1$ esetet.

Elsőként legyen $p = 4k - 1$. Ekkor kvadratikus maradék ellentettje nemmaradék és fordítva, így x^0-hoz csak $r' + s'$ járul hozzá, minden r' eggyel, összességében véve tehát a négyzetben az x^0-nak megfelelő tag együtthatója $a^2 + 2bc|Q| = a^2 + (p - 1)bc$, ez kell, hogy a-val legyen egyenlő.

Következnek az r-kitevős tagok. Mindenegyes rögzített $r \in Q$-ra $r' + r" \equiv r\ (p)$ ekvivalens az $r" \equiv r - r'\ (p)$ kongruenciával, vagyis $\sum_{r'\in Q}\sum_{r"\in Q} x^{r'+r"}$-ben annyi esetben lesz x^r, ahány kvadratikus maradék van az $r - r' = r + (-r')$ összegek között. Most $-r'$ kvadratikus nemmaradék, így a kérdéses szám az $r + NQ$ halmazban lévő maradékok száma. Mivel $0 = r + (-r)$, ezért ez a szám eggyel kisebb, mint $|(r + NQ) \cap Q_0|$, ami Perron tétele szerint $k - 1$, vagy más alakban írva $\frac{1}{4}(p - 3)$. Ugyanígy $s' + s" \equiv r\ (p)$-t $|(r + Q) \cap NQ| = |(r + Q_0) \cap NQ| = k$ esetben kapunk, ahol $r + Q$ helyett azért írhattunk $r + Q_0$-t, mert $r = r + 0 \notin NQ$. $k = \frac{1}{4}(p + 1)$, valamennyi x^r-hez ennyi tagot kapunk az $x^{s'+s"}$-alakú tagok között. Végül az $r' + s' \equiv r\ (p)$ megoldásainak számát kell megadnunk. Átalakítva $s' \equiv r + (-r')\ (p)$, és $r + NQ$-ban a nemmaradékok száma $k - 1 = \frac{1}{4}(p - 3)$. Mindent összeszámolva azt látjuk, hogy az x^r-alakú tagok együtthatója nem függ r-től, és egy-egy ilyen tag együtthatója, amely b-vel kell, hogy megegyezzen, $2ab + \frac{1}{4}(p - 3)b^2 + \frac{1}{4}(p + 1)c^2 + \frac{1}{2}(p - 3)bc$.

Utolsóként a nemmaradékokhoz mint kitevőkhöz tartozó tagokat kell megvizsgálni. Adott s-hez egyrészt kapunk egy tagot $\sum_{s\in NQ} x^s$-ből. $r'+r'' \equiv s\ (p)$ ből $r'' \equiv s+(-r') = s+s'\ (p)$, és ilyen maradék összesen $|(s+NQ)\cap Q| = |(s+NQ)\cap Q_0| = k = \frac{1}{4}(p+1)$ van, mert ismét az a helyzet, hogy $s'+s'' \equiv 0\ (p)$ nem lehetséges. $s'+s'' \equiv s\ (p)$ $|(s+Q)\cap NQ| = |(s+Q_0)\cap NQ| - 1 = k-1$ alkalommal adódik, ahol figyelembe kellett venni, hogy $s+0=s$ nemmaradék. s egy maradék és egy nemmaradék összegeként, vagyis $r'+s' \equiv s\ (p)$ formában $|(s+NQ)\cap NQ| = k-1$-szer keletkezik, amivel megkaptuk, hogy c-nek $2ac+\frac{1}{4}(p+1)b^2+\frac{1}{4}(p-3)c^2+\frac{1}{2}(p-3)bc$-vel kell megegyeznie.

Összefoglalva, ha $p=4k-1$, akkor $f=a+b\sum_{r\in Q}x^r+c\sum_{s\in NQ}x^s$ négyzetében az egyes kitevőkhöz tartozó tagok együtthatója csak attól függ, hogy a kitevő 0, maradék vagy nemmaradék, és $f^2\sim f$, ha

$$\begin{aligned} a^2 \quad\quad\quad\quad + \ (p-1)bc \quad\quad\quad\quad &= a \\ 2ab \quad + \frac{1}{4}(p-3)b^2 + \frac{1}{2}(p-3)bc + \frac{1}{4}(p+1)c^2 &= b \\ 2ac + \frac{1}{4}(p+1)b^2 + \frac{1}{2}(p-3)bc + \frac{1}{4}(p-3)c^2 &= c. \end{aligned}$$

Hasonlóan tudjuk meghatározni az egyenleteket a $p=4k+1$ esetre, és az eredmény

$$\begin{aligned} a^2 \quad + \frac{1}{2}(p-1)b^2 \quad\quad\quad + \frac{1}{2}(p-1)c^2 &= a \\ 2ab \quad + \frac{1}{4}(p-5)b^2 + \frac{1}{2}(p-1)bc + \frac{1}{4}(p-1)c^2 &= b \\ 2ac + \frac{1}{4}(p-1)b^2 + \frac{1}{2}(p-1)bc + \frac{1}{4}(p-5)c^2 &= c. \end{aligned}$$

(Megfigyelhetjük, hogy mindkét esetben mindhárom egyenletben az együtthatók összege éppen p). A második egyenletből kivonva a harmadikat, az eredmény

$$(2a-e)(b-c)-(b^2-c^2)=0,$$

függetlenül p alakjától. Mivel $b\neq c$, ezért $b-c$-vel való egyszerűsítés után $2a-e=b+c$.

Ha a második egyenletrendszernél a második és harmadik egyenletet összeadjuk, akkor összevonás és némi átalakítás után ez

$$\begin{aligned} 0 &= (2a-e)(b+c)+\frac{p-3}{2}(b^2+c^2)+(p-1)bc \\ &= (b+c)^2+\frac{p-3}{2}(b^2+c^2)+(p-1)bc \\ &= \frac{p-1}{2}(b^2+c^2)+(p+1)bc. \end{aligned}$$

Ha ezt kivonjuk az első egyenletből, akkor abból $a^2-(p+1)bc=a$-t kapunk. p-t a két esetnek megfelelően $p=4k+\varepsilon$ alakban írva, az első egyenletek egységes alakra hozhatóak:

$$\big((-\varepsilon p)-1\big)bc = a-a^2.$$

Az első egyenletrendszer utolsó két egyenletének összege $(2a-e)(b+c)+\frac{p-1}{2}(b+c)^2-2bc=0$, és $b+c$ helyére $2a-e$-t írva és kissé átalakítva, átrendezéssel ez $\frac{p+1}{2}(2a-e)^2=2bc$. A második egyenletrendszernél kapott $\frac{p-1}{2}(b^2+c^2)+(p+1)bc=0$ egyenletet hasonlóan átalakítva, a kapott egyenlet $\frac{-p+1}{2}(2a-e)^2=2bc$, és láthatóan az összegek is egységesíthetőek a

$$\frac{(-\varepsilon p)+1}{2}(2a-e)^2 = 2bc$$

formában, vagyis most már a két esetet egységesen tudjuk kezelni.

A legutóbbi egyenletet $\frac{(-\varepsilon p)-1}{2}e$-vel szorozva a jobb oldalon $\big((-\varepsilon p)-1\big)bc$ lesz, ami az első egyenlet alapján $a-a^2$, így most $\frac{(-\varepsilon p)^2-1}{4}(2a-e)^2 = a-a^2$. Négyzetre emelés és összevonás után ebből a kifejezésből az $a^2 - a + \frac{(-\varepsilon p)^2-1}{4(-\varepsilon p)^2}e = 0$ másodfokú egyenletet kapjuk ($(-\varepsilon p)^2 = p^2$, de most meghagytuk az adott alakot, hogy jobban látszódjon p típusa). q páratlan, tehát a test karakterisztikája nem 2, alkalmazható a másodfokú egyenlet megoldó képlete, amiből $a_{1,2} = \frac{e}{2e} \pm \frac{e}{2(-\varepsilon p)e}$.

Az eddigiekből $b+c = 2a-e = \pm\frac{e}{(-\varepsilon p)e}$ és $bc = \frac{((-\varepsilon p)+1)e}{4e}(2a-e)^2 = \frac{((-\varepsilon p)+1)e}{4(-\varepsilon p)^2 e}$. Ekkor b és c gyöke az $x^2 \mp \frac{e}{(-\varepsilon p)e}x + \frac{((-\varepsilon p)+1)e}{4(-\varepsilon p)^2 e}$ másodfokú polinomnak. Az $a = \frac{e}{2e} + \frac{e}{2(-\varepsilon p)e}$-hez tartozó két gyök $x_{1,2} = \frac{e}{2(-\varepsilon p)e} \pm \frac{e}{2\sqrt{\varepsilon p e}}$, míg $a = \frac{e}{2e} - \frac{e}{2(-\varepsilon p)e}$ esetén $x_{1,2} = -\frac{e}{2(-\varepsilon p)e} \pm \frac{e}{2\sqrt{\varepsilon p e}}$. Korábban azt kaptuk, hogy $\theta^2 = \varepsilon p e$, így $\frac{e}{\varepsilon p e} = \frac{e}{\theta^2}$, tehát az első esethez tartozó gyökök $-\frac{\varepsilon e}{2pe} \pm \frac{e}{2\theta}$, a másodiknál pedig $\frac{\varepsilon e}{2pe} \pm \frac{e}{2\theta}$. Mindkét esetben az egyik gyök b, a másik c. Végeredményként, ε-tól függetlenül, négy lehetséges idempotenst kaptunk:

$$f_1 = \left(\frac{e}{2e}+\frac{e}{2pe}\right) + \left(\frac{e}{2pe}+\frac{e}{2\theta e}\right)\sum_{r\in Q} x^r + \left(\frac{e}{2pe}-\frac{e}{2\theta e}\right)\sum_{s\in NQ} x^s$$

$$f_2 = \left(\frac{e}{2e}+\frac{e}{2pe}\right) + \left(\frac{e}{2pe}-\frac{e}{2\theta e}\right)\sum_{r\in Q} x^r + \left(\frac{e}{2pe}+\frac{e}{2\theta e}\right)\sum_{s\in NQ} x^s$$

$$f_3 = \left(\frac{e}{2e}-\frac{e}{2pe}\right) - \left(\frac{e}{2pe}-\frac{e}{2\theta e}\right)\sum_{r\in Q} x^r - \left(\frac{e}{2pe}+\frac{e}{2\theta e}\right)\sum_{s\in NQ} x^s$$

$$f_4 = \left(\frac{e}{2e}-\frac{e}{2pe}\right) - \left(\frac{e}{2pe}+\frac{e}{2\theta e}\right)\sum_{r\in Q} x^r - \left(\frac{e}{2pe}-\frac{e}{2\theta e}\right)\sum_{s\in NQ} x^s.$$

Éppen négy idempotensre van szükségünk, nevezetesen a C, a $\bar{C}$, a $C^{(1)}$ és a $\overline{C^{(1)}}$ kód E, $\bar{E}$, $E^{(1)}$ és $\overline{E^{(1)}}$ idempotensére. Azt kell megnézni, hogy az előbbi polinomok milyen értéket adnak a test fölötti primitív p-edik gyök különböző hatványainál. Az utolsó két egyenletnek gyöke e, míg az első kettő értéke e-ben e, így az első két egyenlet lehet a növelt kódok, a második kettő pedig a törléses kódok idempotense. A polinomok az előbbi sorrendben

$$f_1 = \frac{e}{2e} + \frac{e}{2pe}\sum_{i=0}^{p-1} x^i + \frac{e}{2\theta e}\sum_{i=1}^{p-1}\chi(i)x^i$$

$$f_2 = \frac{e}{2e} + \frac{e}{2pe}\sum_{i=0}^{p-1} x^i - \frac{e}{2\theta e}\sum_{i=1}^{p-1}\chi(i)x^i$$

$$f_3 = \frac{e}{2e} - \frac{e}{2pe}\sum_{i=0}^{p-1} x^i + \frac{e}{2\theta e}\sum_{i=1}^{p-1}\chi(i)x^i$$

$$f_4 = \frac{e}{2e} - \frac{e}{2pe}\sum_{i=0}^{p-1} x^i + \frac{e}{2\theta e}\sum_{i=1}^{p-1}\chi(i)x^i$$

alakban is írhatóak. Ha α tetszőleges primitív p-edik gyök, akkor $\sum_{i=0}^{p-1} \alpha^i = 0$ és $\sum_{i=1}^{p-1} \chi(i)\alpha^i = \theta$, így a helyettesítési értékek $\widehat{f_1}(\alpha) = e = \widehat{f_3}(\alpha)$, $\widehat{f_2}(\alpha) = 0 = \widehat{f_4}(\alpha)$, míg egy $s \in NQ$-ra $\chi(s^{-1}i) = -\chi(i)$, tehát $\sum_{i=1}^{p-1} \chi(i)(\alpha^s)^i = -\theta$, és így $\widehat{f_1}(\alpha^s) = 0 = \widehat{f_3}(\alpha^s)$, $\widehat{f_2}(\alpha^s) = e = \widehat{f_4}(\alpha^s)$. Ezek az eredmények azt jelentik, hogy az előbbi α választással $f_2 = E$, $f_4 = \bar{E}, f_1 = E^{(1)}$ és $f_3 = \overline{E^{(1)}}$, megkaptuk a négy kód idempotensét.

20. Példa dekódolásra

1. Konstruáljunk egy ternáris (azaz a háromelemű test feletti) BCH-kódot az $n = 13$, $\tau = 1$, $\delta = 5$ paraméterekkel. Legyen α egy $\mathbb{Z}_3$ fölötti primitív 13. egységgyök, ekkor $\alpha^{13} = 1$, azaz α gyöke a $\mathbb{Z}_3$ fölötti $x^{13} - 1$ polinomnak, de $13 > k \in \mathbb{N}^+$ esetén nem gyöke egyetlen $x^k - 1 \in \mathbb{Z}_3[x]$ polinomnak sem. Ha a legszűkebb test, amely tartalmazza α-t, $\mathbb{F}_q$, akkor mindenesetre $\mathbb{F}_q$ a $\mathbb{Z}_3$ bővítése, tehát $q = 3^m$ valamilyen pozitív egész m-mel. $\mathbb{F}_q$ minden nullától különböző η elemére teljesül az $\eta^{q-1} = 1$ összefüggés, ennélfogva $\alpha^{q-1} = 1$. De a legkisebb kitevő, amellyel α megfelelő hatványa 1, éppen n, ezért $n|q-1$, ami másként $q \equiv 1\ (n)$, és q a legkisebb ilyen tulajdonságú pozitív egész. Az előzőek szerint a $3^u \equiv 1\ (13)$ kongruencia legkisebb pozitív megoldása lesz m. $3^1 = 3$ és $3^2 = 9$ önmagát, azaz nem 1-et ad maradékul a 13-mal való osztáskor, de $3^3 = 27 = 2 \cdot 13 + 1$, ezért $m = 3$ és $q = 27$. $\mathbb{F}_{27}$ megszerkesztéséhez keresni kell egy $\mathbb{Z}_3$ fölött irreducibilis harmadfokú főpolinomot. Tetszőleges harmadfokú főpolinom $x^3 + ax^2 + bx + c$ alakú, és ha ez $\mathbb{Z}_3$ fölötti, akkor az együtthatói a 3-elemű test elemei, amelyeket most egyszerűen 0, 1 és -1 (vagy ez utóbbi esetben 2) jelöl. Egy harmadfokú polinom pontosan akkor felbonthatatlan egy test felett, ha nincs gyöke ebben a testben. Ez azt jelenti, hogy $c \neq 0$, $1 + a + b + c \neq 0$ és $-1 + a - b + c \neq 0$, így a megoldandó egyenletek a következők: $c = r$, $1 + a + b + c = s$ és $-1 + a - b + c = t$, ahol r, s és t egymástól függetlenül 1 vagy -1. Ezekből a feltételekből $c = r$, $a = -r - s - t$, $b = -1 - s + t$, és a nyolc polinom

i	r	s	t	a	b	c	$m^{(i)}$			
1	1	1	1	0	−1	1	x^3		$-x$	$+1$
2	−1	1	1	−1	−1	−1	x^3	$-x^2$	$-x$	-1
3	1	−1	1	−1	1	1	x^3	$-x^2$	$+x$	$+1$
4	−1	−1	1	1	1	−1	x^3	$+x^2$	$+x$	-1
5	1	1	−1	−1	0	1	x^3	$-x^2$		$+1$
6	−1	1	−1	1	0	−1	x^3	$+x^2$		-1
7	1	−1	−1	1	−1	1	x^3	$+x^2$	$-x$	$+1$
8	−1	−1	−1	0	−1	−1	x^3		$-x$	-1

Válasszuk a 7. polinomot, és legyen ennek gyöke $\mathbb{F}_{27}$-ben u, ekkor $u^3 = -u^2 + u - 1$, és a test valamennyi eleme felírható $a + bu + cu^2$ alakban $\mathbb{Z}_3$-beli a, b és c-vel. Másrészről $\mathbb{F}_{27}$-ben minden nem nulla elem multiplikatív rendje osztója $27 - 1 = 26$-nak, így csak 1, 2, 13 és 26 lehet, és csupán az egységelem rendje 1, valamint -1 rendje 2. $\mathbb{Z}_3$ minden bővítésében $(a + b)^3 = a + b$, így

$$u^4 = uu^3 = u(-u^2 + u - 1) = -u^3 + u^2 - u$$
$$= u^2 - u + 1 + u^2 - u = 2u^2 - 2u + 1 = -u^2 + u + 1$$

$$u^9 = (u^3)^3 = (-u^2 + u - 1)^3 = -u^6 + u^3 - 1 = -u^2u^4 + u^3 - 1$$
$$= -u^2(-u^2 + u + 1) + u^3 - 1 = u^4 - u^2 - 1 = -u^2 + u + 1 - u^2 - 1 = u^2 + u$$

$$u^{13} = u^9 \cdot u^4 = (u^2 + u)(-u^2 + u + 1) = -u^4 + 2u^2 + u$$
$$= u^2 - u - 1 + 2u^2 + u = -1 \neq 1,$$

vagyis u rendje 26, u a test egy primitív eleme. Ekkor a test valamennyi nem nulla eleme megkapható u hatványaként. A hatványokkal könnyű a szorzás, ám közvetlenül nem alkalmas az összeadás elvégzésére. Vegyük azonban észre, hogy bármely testben $u^k + u^j = u^j\left(u^{k-j} + e\right)$, ahol e a test egységeleme, így ismerve $u^{k-j} + e = u^t$-t, $u^k + u^j = u^j \cdot u^t = u^{j+t} = u^{(j+t) \bmod (q-1)}$-et ($q$ a test elemszáma), már az összeadás is könnyű. Egyre kell ügyelni, nevezetesen ha $u^{k-j} = -e$, vagyis jelen esetben ha $k - j = \pm 13$, ugyanis ekkor $u^{k-j} + e = 0$, és a 0 nem írható fel mint u hatványa. Írjuk 0-t u^* alakban, akkor a test bármely eleme u^t alakú, ahol most $26 > t \in \mathbb{N}$ vagy $t = *$, és minden ilyen t-re

$u^t + 1 = u^v$, ahol ismét $26 > v \in \mathbb{N}$ vagy $v = *$. v az adott testelem **Zech-logaritmusa**, míg t-ről tudjuk, hogy az u^t **diszkrét logaritmusa** (mindkettő u-ra mint alapra vonatkoztatva). Ha a test valamelyik a elemének logaritmusát $d(a)$, Zech-logaritmusát $z(a)$ jelöli, akkor

$$d(a \cdot b) = \big(d(a) + d(b)\big) \bmod (q-1)$$

$$d(a+b) = \Big(d(a) + z\Big(\big(d(b) - d(a)\big) \bmod\ (q-1)\Big)\Big) \bmod (q-1),$$

ahol $d(a) = *$ esetén $a = 0$, tehát $a \cdot b = 0$ és $a + b = b$, így ebben az esetben $d(a \cdot b) = d(0) = *$ és $d(a+b) = d(b)$. A testbeli műveletek elvégzéséhez ismerni kell egy adott elem logaritmusát (ez a **log-tábla**), adott kitevőhöz tartozó elemet (**antilog-tábla**), valamint a kitevőhöz tartozó eleme Zech-logaritmusát. $\mathbb{F}_{27}$ esetén az u bővítőelemre mint alapra vonatkozó értékek az 7. táblázaton láthatóak.

$\underline{a}$	$\underline{d(a)}$	$\underline{d(a)}$	$\underline{z(a)}$	$\underline{a}$
0	$*$	$*$	0	0
1	0	0	13	1
2	13	1	8	u
u	1	2	6	u^2
$u+1$	8	3	24	$2u^2+u+2$
$u+2$	10	4	3	$2u^2+u+1$
$2u$	14	5	19	$2u^2+1$
$2u+1$	23	6	18	u^2+1
$2u+2$	21	7	22	$2u^2+2u+2$
u^2	2	8	10	$u+1$
u^2+1	6	9	20	u^2+u
u^2+2	18	10	1	$u+2$
u^2+u	9	11	16	u^2+2u
u^2+u+1	20	12	9	u^2+u+2
u^2+u+2	12	13	$*$	2
u^2+2u	11	14	23	$2u$
u^2+2u+1	16	15	5	$2u^2$
u^2+2u+2	17	16	17	u^2+2u+1
$2u^2$	15	17	11	u^2+2u+2
$2u^2+1$	5	18	2	u^2+2
$2u^2+2$	19	19	15	$2u^2+2$
$2u^2+u$	24	20	12	u^2+u+1
$2u^2+u+1$	4	21	14	$2u+2$
$2u^2+u+2$	3	22	25	$2u^2+2u$
$2u^2+2u$	22	23	21	$2u+1$
$2u^2+2u+1$	25	24	4	$2u^2+u$
$2u^2+2u+2$	7	25	7	$2u^2+2u+1$

7. táblázat

$\mathbb{F}_{27}$-ben u minden pozitív páros kitevős hatványa 13-rendű elem, ezért ezek mindegyike primitív 13. egységgyök, válasszuk α-nak u^2-et. Kis számolással $x^{13} - 1 = (x-1)m^{(2)}m^{(4)}m^{(6)}m^{(8)}$, továbbá

$$\hat{m}^{(8)}(\alpha) = \hat{m}^{(8)}(\alpha^3) = \hat{m}^{(8)}(\alpha^9) = 0 \quad \hat{m}^{(4)}(\alpha^2) = \hat{m}^{(4)}(\alpha^6) = \hat{m}^{(4)}(\alpha^5) = 0$$
$$\hat{m}^{(2)}(\alpha^4) = \hat{m}^{(2)}(\alpha^{12}) = \hat{m}^{(2)}(\alpha^{10}) = 0 \quad \hat{m}^{(6)}(\alpha^7) = \hat{m}^{(6)}(\alpha^8) = \hat{m}^{(6)}(\alpha^{11}) = 0.$$

Ha egy BCH-kódban adott α, τ és δ, akkor g az $\alpha^{\tau}, \alpha^{\tau+1}, \dots, \alpha^{\tau+\delta-2}$ minimálpolinomjainak szorzata, minden ilyen polinomot csupán egyszer szerepeltetve a szorzatban, azaz a mi esetünkben

$$g = m^{(8)}m^{(4)}m^{(2)} = x^9 - x^8 + x^7 - x^6 + x^4 + x^3 - 1,$$

hiszen most $\tau = 1$ és $\delta = 5$, ezért α, α^2, α^3 és α^4 minimálpolinomját, $m^{(8)}$-at, $m^{(4)}$-et, $m^{(8)}$-at és $m^{(2)}$-t kell tekinteni, de α-hoz és α^3-höz egyaránt $m^{(8)}$ tartozik, így az csak egyszer szerepel a szorzatban. Mivel g foka 9, ezért a kód dimenziója $k = 13 - 9 = 4$ lesz. Még azt is látjuk, hogy g gyökei $m^{(2)}$, $m^{(4)}$ és $m^{(8)}$ gyökei, tehát α, α^2, α^3, α^4, α^5, α^6, α^9, α^{10}, α^{12}, és ezek közül az első 6 egymás utáni kitevőhöz tartozik, tehát a kód azonos egy olyan BCH-kóddal, amelyre $\delta = 7$, ezért a kód minimális távolsága $d \geq 7$, így egy $[13{,}4{,}d]_3$ ciklikus kódot kapunk, ahol d legalább 7. g meghatározza h-t is, ugyanis $x^{13} - 1 = g \cdot h$, tehát $h = (x-1)m^{(6)} = x^4 + x^3 + 1$.

A generátor- és ellenőrző polinom ismeretében meg tudjuk adni a kód generátor- és ellenőrző mátrixát. $\mathbf{G}_1$ egy 4×13-as mátrix, amelynek i-edik sorában $3 \geq i \in \mathbb{N}$-re $x^i g$ együtthatói állnak, bal szélen a polinom konstans tagjával, míg $\mathbf{H}_1$ egy 9×13-as mátrix, és ennek i-edik sora az $x^{8-i}h$ polinom együtthatóit tartalmazza a 12-edfokú tag együtthatójával kezdve. A két mátrix a következő:

$$\mathbf{H}_1 = \begin{pmatrix} 0&0&0&0&0&0&0&0&1&1&0&0&1 \\ 0&0&0&0&0&0&0&1&1&0&0&1&0 \\ 0&0&0&0&0&0&1&1&0&0&1&0&0 \\ 0&0&0&0&0&1&1&0&0&1&0&0&0 \\ 0&0&0&0&1&1&0&0&1&0&0&0&0 \\ 0&0&0&1&1&0&0&1&0&0&0&0&0 \\ 0&0&1&1&0&0&1&0&0&0&0&0&0 \\ 0&1&1&0&0&1&0&0&0&0&0&0&0 \\ 1&1&0&0&1&0&0&0&0&0&0&0&0 \end{pmatrix}$$

$$\mathbf{G}_1 = \begin{pmatrix} 2&0&0&1&1&0&2&1&2&1&0&0&0 \\ 0&2&0&0&1&1&0&2&1&2&1&0&0 \\ 0&0&2&0&0&1&1&0&2&1&2&1&0 \\ 0&0&0&2&0&0&1&1&0&2&1&2&1 \end{pmatrix}$$

$\mathbf{G}_1$ nem szisztematikus kódot generál. Szisztematikus kód generátormátrixához úgy jutunk, ha figyelembe vesszük, hogy $x^{9+i} = t \cdot g + r$-ből $x^{9+i} - r = t \cdot g$ eleme a kódnak, és mivel r vagy azonosan nulla, vagy a fokszáma kisebb, mint 9, ezért a bal oldali polinomban $3 \geq i \in \mathbb{N}$ esetén a négy legmagasabbfokú tag együtthatója közül pontosan egy, az i-edik lesz 1, a többi nulla, ezért ezek a polinomok lineárisan függetlenek, így generátormátrixot adnak, és ebben a mátrixban a jobb szélső négy oszlop egységmátrix:

$$\begin{aligned} x^9 &= \quad 1 \quad \cdot g + (x^8 - x^7 + x^6 - x^4 - x^3 + 1) \\ x^{10} &= (x \ + 1) \cdot g + (x^6 - x^5 + x^4 - x^3 + x \ + 1) \\ x^{11} &= (x^2 + x \ ) \cdot g + (x^7 - x^6 + x^5 - x^4 + x^2 + x) \\ x^{12} &= (x^3 + x^2) \cdot g + (x^8 - x^7 + x^6 - x^5 + x^3 + x^2) \end{aligned}$$

$$\mathbf{H}_2 = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&1&1&0&0 \\ 0&1&0&0&0&0&0&0&0&0&1&1&0 \\ 0&0&1&0&0&0&0&0&0&0&0&1&1 \\ 0&0&0&1&0&0&0&0&0&2&2&0&1 \\ 0&0&0&0&1&0&0&0&0&2&1&2&0 \\ 0&0&0&0&0&1&0&0&0&0&2&1&2 \\ 0&0&0&0&0&0&1&0&0&1&1&2&1 \\ 0&0&0&0&0&0&0&1&0&2&0&1&2 \\ 0&0&0&0&0&0&0&0&1&1&0&0&1 \end{pmatrix},$$

$$\mathbf{G}_2 = \begin{pmatrix} 2&0&0&1&1&0&2&1&2&1&0&0&0 \\ 2&2&0&1&2&1&2&0&0&0&1&0&0 \\ 0&2&2&0&1&2&1&2&0&0&0&1&0 \\ 0&0&2&2&0&1&2&1&2&0&0&0&1 \end{pmatrix}.$$

$\mathbf{H}$ konstrukciójánál felhasználtuk, hogy ha $\mathbf{G} = (\mathbf{P}\ \mathbf{I})$, akkor $\mathbf{H} = (\mathbf{I}\ -\mathbf{P}^T)$ alakú. A generátormátrix ismeretében megadható a teljes kód: ha $\mathbf{G}$ négy sora $\mathbf{g}_0^T$, $\mathbf{g}_1^T$, $\mathbf{g}_2^T$ és $\mathbf{g}_3^T$, akkor a kódszavak a $\sum_{i=0}^{3} a_i \mathbf{g}_i^T$ lineáris kombinációk, ahol az a_i-k értéke egymástól függetlenül 0, 1 és $-1 = 2$ lehet. A kódszavak száma $3^4 = 81$. Mivel a kód ciklikus, ezért egy kódszó és eltoltjai közül elegendő megadni egyet. Tegyük fel, hogy egy kódszó j lépés után az eredetivel egyenlő. Ez azt jelenti, hogy bármely j-hosszúságú szakasza (ciklikusan értve) a szakasz kezdőpontjától j távolságra ismétlődik, vagyis a kódszó periodikus az j periódussal. De 13 lépés után a kódszó visszaérkezik a kiinduló állapotba, így a 13 biztosan periódusa a kódnak, ezért a minimális periódus osztója 13-nak, vagyis csak 1 és 13 lehet. 1-periódusú kódszó valamennyi eleme azonos, ilyen három lehet: minden jegy 0, 1 vagy 2. A nullvektor eleme a kódnak, és ha a csupa 1-ből vagy a csak 2-ből álló vektor eleme a kódnak, akkor a linearitásból kifolyólag a másik is. Mivel $81 = 6 \cdot 13 + 3$, ezért a kód tartalmazza mindhárom konstans-vektort, valamint hat páronként idegen halmazt, amelyek egy-egy vektorukkal reprezentálhatóak. Elegendő ezek közül hármat megadni: ha egy vektor eleme a kódnak, akkor a -1-szerese is, és ezek nem lehetnek azonos osztályban, ugyanis ha c és $-c$ egymás eltoltja, mondjuk $-c$-t megkapjuk c-ből s lépéssel, akkor $2s$ lépéssel az eredetire kell jutnunk, ami a páratlan hossz miatt lehetetlen. Ezek alapján a teljes kódot megadhatjuk:

$$\begin{matrix} 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 2\,0\,0\,1\,1\,0\,2\,1\,2\,1\,0\,0\,0 \\ 1\,2\,0\,2\,0\,1\,1\,1\,2\,1\,1\,0\,0 \\ 1\,2\,2\,2\,0\,2\,2\,1\,1\,2\,0\,1\,0 \\ 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \end{matrix}$$

és ezek eltoltjai valamint az ilyenek ellentettjei. Ebből látjuk, hogy a kód távolsága pontosan 7: a fenti nem nulla vektorok súlya 7, 9, 10 és 13, és az eltolt valamint az ellentett súlya ugyanakkora.

Szükség lesz még az α-hatványokkal megadott $\mathbf{H}$ mátrixra. Egyrészről ez tartalmazza a kód valamennyi egymás utáni gyökének hatványát, a jelen esetben tehát az α, α^2, α^3, α^4, α^5 és α^6 elemek hatványait, ugyanis az n, τ, δ-paraméterű BCH-kód paritásellenőrző mátrixában $H_{i,j} = \left(\alpha^{\tau+i}\right)^j$, ahol $\delta - 1 > i \in \mathbb{N}$ és $n > j \in \mathbb{N}$, vagyis $H_{i,j} = \left(\alpha^{1+i}\right)^j$ a $6 > i \in \mathbb{N}$, $13 > j \in \mathbb{N}$ indexekre:

$$\mathbf{H}_3 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^2 & \alpha^5 & \alpha^8 & \alpha^{11} & \alpha & \alpha^4 & \alpha^7 & \alpha^{10} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^3 & \alpha^7 & \alpha^{11} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha & \alpha^5 & \alpha^9 \\ 1 & \alpha^5 & \alpha^{10} & \alpha^2 & \alpha^7 & \alpha^{12} & \alpha^4 & \alpha^9 & \alpha & \alpha^6 & \alpha^{11} & \alpha^3 & \alpha^8 \\ 1 & \alpha^6 & \alpha^{12} & \alpha^5 & \alpha^{11} & \alpha^4 & \alpha^{10} & \alpha^3 & \alpha^9 & \alpha^2 & \alpha^8 & \alpha & \alpha^7 \end{pmatrix},$$

más esetekben viszont a generátorpolinom irreducibilis tényezőinek csupán egy-egy gyökének hatványai alkotnak egy sort, például α, α^2 és α^4:

$$\mathbf{H}_4 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^3 & \alpha^7 & \alpha^{11} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha & \alpha^5 & \alpha^9 \end{pmatrix}.$$

α hatványait egyértelműen megadhatjuk a báziselemek együtthatóiból álló oszlopvektorral, és így egy $\mathbb{Z}_3$ fölötti mátrixot kapunk:

$$\mathbf{H}_5 = \begin{pmatrix} 1&0&1&1&1&2&2&0&1&2&1&0&0 \\ 0&0&1&0&1&1&1&2&2&0&1&2&1 \\ 0&1&2&1&0&0&1&0&1&1&1&2&2 \\ 1&1&1&2&1&1&0&0&1&2&0&2&0 \\ 0&1&1&1&2&1&1&0&0&1&2&0&2 \\ 0&2&0&1&1&1&2&1&1&0&0&1&2 \\ 1&1&1&0&1&0&0&1&2&1&0&2&2 \\ 0&1&2&1&0&2&2&1&1&1&0&1&0 \\ 0&0&1&2&1&0&2&2&1&1&1&0&1 \end{pmatrix}.$$

A sorokkal végzett manipulációkkal ebből a mátrixból kapjuk a

$$\mathbf{H}_6 = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&1&1&0&0 \\ 0&1&0&0&0&0&0&0&0&0&1&1&0 \\ 0&0&1&0&0&0&0&0&0&0&0&1&1 \\ 0&0&0&1&0&0&0&0&0&2&2&0&1 \\ 0&0&0&0&1&0&0&0&0&2&1&2&0 \\ 0&0&0&0&0&1&0&0&0&0&2&1&2 \\ 0&0&0&0&0&0&1&0&0&1&1&2&1 \\ 0&0&0&0&0&0&0&1&0&2&0&1&2 \\ 0&0&0&0&0&0&0&0&1&1&0&0&1 \end{pmatrix}$$

mátrixot, és ez egybeesik $\mathbf{H}_2$-vel, így a $\mathbf{H}_6$-ból kapott generátormátrix éppen $\mathbf{G}_2$ lesz.

2. Az előbbiekben megalkotott kód távolsága 7, ezért legfeljebb három hibát ki tud javítani, viszont ennél több hibát általában nem. Vegyünk egy kódszót, $\mathbf{c}^T = 1122102021110$-t, és legyen két hibavektor, $\boldsymbol{\varepsilon}_1^T = 0001000001020$ és $\boldsymbol{\varepsilon}_2^T = 0001121000000$. Ekkor $\mathbf{v}_1^T = 1120102022100$ lesz az egyik esetben a vett szó, és a másik esetben $\mathbf{v}_1^T = 1120220021110$.

Háromféle módon végezzük a dekódolást.

a) **Hibacsapdadekódolás**:

A lényege: ha a legfeljebb három hiba teljes egészében a szó paritásrészébe esik, akkor a szindróma súlya nem haladja meg a hármat, míg az ellenkező esetben (feltéve, hogy valóban nincs több mint három hiba) ez a súly meghaladja a hármat. Ha viszont a hiba a paritásrészre korlátozódik, akkor a hibavektor paritásrésze azonos a szindrómával, így azt levonva a vett szó paritásrészéből, rendelkezésünkre áll a hibátlan üzenet. Ha a kód ciklikus, akkor egy kódszó eltoltja is kódszó, ezért a vett szót cilikusan léptetve az új szó szindrómája a hiba ciklikus eltoltjának a szindrómája lesz. Ciklikus kód esetén a szindrómát megkapjuk, ha a vett szót osztjuk a generátorpolinommal, és vesszük a maradékot, míg az eltolt szindrómája a szindróma eltoltjának maradéka.

Nézzük az első szót.

0. lépés

$$\begin{array}{l} (x^{10}-x^9-x^8 \quad -x^6 \quad +x^4-x^2+x+1) : (x^9-x^8+x^7-x^6+x^4+x^3-1) = x \\ \quad\; x^8+x^7-x^6-x^5 \quad -x^2-x+1 \end{array}$$

a maradék súlya 7. A továbbiakban elléptetve a maradékot balra (azaz megszorozva *x*-szel), osztunk g-vel mindaddig, amíg a súly kisebb lesz 4-nél, vagy visszajutunk a kiinduló helyzetbe.

1. lépés

$$\begin{array}{l}(x^9+x^8-x^7-x^6 \quad -x^3-x^2+x): (x^9-x^8+x^7-x^6+x^4+x^3-1)=1\\ \quad -x^8+x^7 \quad -x^4+x^3-x^2+x+1\end{array}$$

2. lépés

$$\begin{array}{l}(-x^9+x^8 \quad -x^5+x^4-x^3+x^2+x): (x^9-x^8+x^7-x^6+x^4+x^3-1)=-1\\ \quad x^7-x^6-x^5-x^4 \quad +x^2+x+1\end{array}$$

3. lépés

$$(x^8-x^7-x^6-x^5+x^3+x^2-x): (x^9-x^8+x^7-x^6+x^4+x^3-1)=0$$

4. lépés

$$\begin{array}{l}(x^9-x^8-x^7-x^6+x^4+x^3-x^2): (x^9-x^8+x^7-x^6+x^4+x^3-1)=1\\ \quad x^7 \quad -x^2+1\end{array}$$

a súly 3, tehát a vett szót négy hellyel ciklikusan jobbra léptetve a hiba az alsó 9 jegyen található, és maga a számított hibavektor a fordított sorrendben írt maradék visszaléptetésével nyerhető (vegyük figyelembe, hogy a polinomokban a jegyek sorrendje fordított most, ezért mondtuk, hogy a vektort jobbra léptettük). Toljuk tehát el az 1020000100000 vektort 4 hellyel ciklikusan balra. Ekkor a kapott vektor 0001000001020 lesz, és ez megegyezik a tényleges hibával.

Vegyük a második szót.

0. lépés

$$\begin{array}{l}(x^{11}+x^{10}+x^9-x^8 \quad -x^5-x^4 \quad -x^2+x+1): (x^9-x^8+x^7-x^6+x^4+x^3-1)\\ \quad -x^{10} \quad -x^6+x^5-x^4 \quad +x+1 \quad =x^2-x-1\\ \quad -x^9+x^8-x^7-x^6-x^5 \quad +1\\ \quad x^6-x^5+x^4+x^3\end{array}$$

1. lépés

$$(x^7-x^6+x^5+x^4): (x^9-x^8+x^7-x^6+x^4+x^3-1)=0$$

2. lépés

$$(x^8-x^7+x^6+x^5): (x^9-x^8+x^7-x^6+x^4+x^3-1)=0$$

3. lépés

$$\begin{array}{l}(x^9-x^8+x^7+x^6): (x^9-x^8+x^7-x^6+x^4+x^3-1)=1\\ \quad -x^6-x^4-x^3+1\end{array}$$

4. lépés

$$(-x^7-x^5-x^4+x): (x^9-x^8+x^7-x^6+x^4+x^3-1)=0$$

5. lépés

$$(-x^8-x^6-x^5+x^2): (x^9-x^8+x^7-x^6+x^4+x^3-1)=0$$

6. lépés

$$\begin{array}{l}(-x^9 \quad -x^7-x^6 \quad +x^3):(x^9-x^8+x^7-x^6+x^4+x^3-1)=-1\\ \quad -x^8 \quad +x^6+x^4-x^3-1\end{array}$$

7. lépés

$$\begin{array}{l}(-x^9 \quad +x^7 \quad +x^5-x^4 \quad -x):(x^9-x^8+x^7-x^6+x^4+x^3-1)=-1\\ \quad -x^8-x^7-x^6+x^5 \quad +x^3-x-1\end{array}$$

8. lépés

$$\begin{array}{l}(-x^9-x^8-x^7+x^6+x^4 \quad -x^2-x):(x^9-x^8+x^7-x^6+x^4+x^3-1)=-1\\ \quad x^8 \quad -x^4+x^3-x^2-x-1\end{array}$$

9. lépés

$$\begin{array}{l}(x^9 \quad -x^5+x^4-x^3-x^2-x):(x^9-x^8+x^7-x^6+x^4+x^3-1)=1\\ \quad x^8-x^7+x^6-x^5 \quad +x^3-x^2-x+1\end{array}$$

10. lépés

$$\begin{array}{l}(x^9-x^8+x^7-x^6+x^4-x^3-x^2+x):(x^9-x^8+x^7-x^6+x^4+x^3-1)=1\\ \quad +x^3-x^2+x+1\end{array}$$

11. lépés

$$(x^4-x^3+x^2+x):(x^9-x^8+x^7-x^6+x^4+x^3-1)=0$$

12. lépés

$$(x^5-x^4+x^3+x^2):(x^9-x^8+x^7-x^6+x^4+x^3-1)=0$$

és a következő léptetés után már az eredeti vektorra jutunk. Mivel egyetlen léptetéssel sem kaptunk olyan szindrómát, amelynek a súlya kisebb lenne 4-nél, ezért nem tudjuk a hibákat a paritásrészre lokalizálni. Ez általában nem azt jelenti, hogy a megengedettnél több hiba lépett fel, mert a kódok jelentős részénél a paritásrész hossza kicsi a teljes hosszhoz képest. Ám a jelenlegi kódnál nem ez a helyzet. Ha valóban legfeljebb három hiba van, akkor biztosan van két olyan hibahely, amelyek között ciklikusan legalább négy hibátlan hely van, vagyis a csomó hossza legfeljebb 9, és $n-k=13-4=9$, tehát most az, hogy egyetlen léptetéssel sem kapunk 4-nél kisebb súlyú hibát, valóban azt jelenti, hogy az átvitel során fellépett hibák száma háromnál több, amit a kód nem tud javítani.

b) **Dekódolás rekurzív sorozattal**:

Ha **H** i-edik sorát szorozzuk **v**-vel, akkor a **v** vektor Fourier-transzformáltjának $\tau+i$-edik komponensét kapjuk (most a kód valamennyi, sorban egymás utáni gyökét tartalmazó paritásellenőrző mátrixszal kell számolni). A kapott k komponenst egy homogén lineáris rekurzív sorozat első k elemének tekintve kereshetjük a megfelelő minimálpolinomot. Ennek menete az alábbi: a kiinduló polinom $m=1$, ennek foka $L=0$, és a segédpolinom értéke $m^{(p)}=0$, továbbá $j=0$. Az egymás után következő j értékekkel kiszámítjuk a $d=\sum_{i=0}^{L} m_i S_{i-L+j}$ összeget. Ha $d\neq 0$, akkor $\tilde{m}=m$, és m új értéke $m=x^{L_1-L}m-dd_p^{-1}x^{L_1-j+p-L_p}m^{(p)}$, ahol $L_1=\max\{L, j+1-L\}$, és amennyiben $L_1>L$, akkor még $L_p=L$, $L=L_1$, $p=j$, $d_p=d$ és $m^{(p)}=\tilde{m}$. Az eljárást addig folytatjuk, amíg j el nem éri a sorozat

utolsó elemének indexét. Kis számolással ellenőrizhető, hogy a keretezett részben megadott algoritmus az előbbi eljárásnak felel meg.

Visszatranszformálva a sorozatot, majd ciklikusan τ hellyel jobbra tolva a hibavektort kapjuk, feltéve, hogy nem lépett fel a megengedettnél több hiba, ellenkező esetben a kapott vektor nem feltétlenül az eredeti hibavektor, sőt esetleg nem is minden komponense van $\mathbb{Z}_3$-ban (bizonyos szempontból ez a jobbik eset, hiszen ekkor tudjuk, hogy a hibák száma meghaladja a lehetőségeket).

Fourier
$m^{(p)} = 0$
$L = 0$
$m = 1 \quad \left(m = \sum_{i=0}^{L} m_i x^i \,;\; m_L = 1\right)$
$j = 0$
ciklus amíg $j < \delta - 1$
  $d = \sum_{i=0}^{L} m_i S_{i-L+j}$
  $j = j + 1$
  ha $d \neq 0$
    $L_1 = 2l - j$
    ha $L_1 \geq 0$
      $m = m + dx^{L_1} m^{(p)}$
    különben
      $\widetilde{m} = m$
      $m = x^{-L_1} m + d m^{(p)}$
      $L = j - L$
      $m^{(p)} = -d^{-1}\widetilde{m}$
    elágazás vége
  elágazás vége
ciklus vége
ciklus amíg $j < n$
  $s_j = -\sum_{i=0}^{L-1} m_i S_{i-L+j}$
  $j = j + 1$
ciklus vége
Fourier vége.

Nézzük az első vektort.

$$S = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^2 & \alpha^5 & \alpha^8 & \alpha^{11} & \alpha & \alpha^4 & \alpha^7 & \alpha^{10} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^3 & \alpha^7 & \alpha^{11} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha & \alpha^5 & \alpha^9 \\ 1 & \alpha^5 & \alpha^{10} & \alpha^2 & \alpha^7 & \alpha^{12} & \alpha^4 & \alpha^9 & \alpha & \alpha^6 & \alpha^{11} & \alpha^3 & \alpha^8 \\ 1 & \alpha^6 & \alpha^{12} & \alpha^5 & \alpha^{11} & \alpha^4 & \alpha^{10} & \alpha^3 & \alpha^9 & \alpha^2 & \alpha^8 & \alpha & \alpha^7 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 2 \\ 0 \\ 1 \\ 0 \\ 2 \\ 0 \\ 2 \\ 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} u \\ u^{21} \\ u^3 \\ u^{10} \\ u^7 \\ u^{11} \end{pmatrix}.$$

Megmutatjuk például a második elem kiszámítását. Ennek értéke

$$\begin{aligned} S_1 &= 1+\alpha^2+2\alpha^4+\alpha^8+2\alpha^{12}+2\alpha^3+2\alpha^5+\alpha^7 \\ &= 1+u^4+u^{21}+u^{16}+u^{11}+u^{19}+u^{23}+u^{14}. \end{aligned}$$

u^4 logaritmusa $d(u^4)=4$, és az 7. táblázat szerint ennek az elemnek a Zech-logaritmusa $z(u^4)=3$, ami azt jelenti, hogy $1+u^4=u^3$. $1+u^4+u^{21}=(1+u^4)+u^{21}=u^3+u^{21}=u^3(1+u^{18})$, és az előzőhöz hasonlóan $z(u^{18})=2$, így $u^3(1+u^{18})=u^3\cdot u^2=u^5$, vagyis $1+u^4+u^{21}=u^5$. A számítást hasonlóan folytatva megkapjuk S_1-et:

$$\begin{aligned} S_1 &= 1+\alpha^2+2\alpha^4+\alpha^8+2\alpha^{12}+2\alpha^3+2\alpha^5+\alpha^7 \\ &= 1+u^4+u^{21}+u^{16}+u^{11}+u^{19}+u^{23}+u^{14} \\ &= (1+u^4)+(u^{21}+u^{16}+u^{11}+u^{19}+u^{23}+u^{14}) \\ &= u^3+u^{21}+u^{16}+u^{11}+u^{19}+u^{23}+u^{14} \\ &= u^3(1+u^{18})+(u^{16}+u^{11}+u^{19}+u^{23}+u^{14}) \\ &= u^5+u^{16}+u^{11}+u^{19}+u^{23}+u^{14} \\ &= u^5(1+u^{11})+(u^{11}+u^{19}+u^{23}+u^{14}) \\ &= u^{21}+u^{11}+u^{19}+u^{23}+u^{14} \\ &= u^{21}(1+u^3)+(u^{19}+u^{23}+u^{14}) \\ &= u^{12}+u^{19}+u^{23}+u^{14} \\ &= u^{12}(1+u^7)+(u^{23}+u^{14}) \\ &= u^8+u^{23}+u^{14} \\ &= u^8(1+u^{15})+u^{14} \\ &= u^{13}+u^{14} \\ &= u^{13}(1+u)=u^{21}, \end{aligned}$$

ahol figyelembe vettük, hogy $\alpha^{13}=1$, $\alpha=u^2$ és $-1=u^{13}$.

A következő sorozatot kaptuk:

$$\begin{aligned} E_1=V_1=S_0=u \qquad & E_2=V_2=S_1=u^{21} \\ E_3=V_3=S_2=u^3 \qquad & E_4=V_4=S_3=u^{10} \\ E_5=V_5=S_4=u^7 \qquad & E_6=V_6=S_5=u^{11}. \end{aligned}$$

Most alkalmazzuk a megadott algoritmust.

$m^{(p)}=0$
$L=0, m=1$
$j=0$
  $d=\sum_{i=0}^{0} m_i S_{i-0+0}=m_0\cdot S_0=1\cdot u=u$
  $j=j+1=1$
  $d\neq 0 \Rightarrow L_1=2L-j=-1$
  $L_1<0 \Rightarrow$
    $\tilde{m}=m=1$
    $m=x^{-L_1}m+dm^{(p)}=x^1\cdot 1+u\cdot 0=x$
    $L=j-L=1$
    $m^{(p)}=-d^{-1}\tilde{m}=-u^{-1}\cdot 1=u^{12}$.

A további lépésekben hasonlóan eljárva, a részletek mellőzése nélkül az alábbi eredményeket kapjuk:

$j=1$: $d=\sum_{i=0}^{1} m_i S_{i-1+1}=0\cdot u+1\cdot u^{21}=u^{21}\neq 0$
$m=x+u^{21}u^{12}=x+u^7$

$j=2$: $d=\sum_{i=0}^{1} m_i S_{i-1+2}=u^7u^{21}+1\cdot u^3=u^2+u^3=u^{10}\neq 0$
$m=x(x+u^7)+u^{10}u^{12}=x^2+u^7x+u^{22}$

$L = 2, m^{(p)} = u^3x + u^{10}$

$j = 3$: $d = \sum_{i=0}^{2} m_i S_{i-2+3} = u^{22}u^{21} + u^7u^3 + 1 \cdot u^{10} = u^9 \neq 0$
$m = (x^2 + u^7x + u^{22}) + u^9(u^3x + u^{10}) = x^2 + x + u^{17}$

$j = 4$: $d = \sum_{i=0}^{2} m_i S_{i-2+4} = u^{17}u^3 + 1 \cdot u^{10} + 1 \cdot u^7 = u^{10} \neq 0$
$m = x(x^2 + x + u^{17}) + u^{10}(u^3x + u^{10}) = x^3 + x^2 + u^{16}x + u^{20}$
$L = 3, m^{(p)} = u^3x^2 + u^3x + u^{20}$

$j = 5$: $d = \sum_{i=0}^{3} m_i S_{i-3+5} = u^{20}u^3 + u^{16}u^{10} + 1 \cdot u^7 + 1 \cdot u^{11} = 1 \neq 0$
$m = (x^3 + x^2 + u^{16}x + u^{20}) + 1 \cdot (u^3x^2 + u^3x + u^{20}) = x^3 + u^{24}x^2 + u^7,$

tehát a sorozat minimálpolinomja $m = x^3 + u^{24}x^2 + u^7$. Ezzel a polinommal a sorozat további elemei

$$\begin{aligned}
E_7 &= S_6 = -\textstyle\sum_{i=0}^{2} m_i S_{i-3+6} = -(u^7u^7 + u^{24}u^6) = u^{18}\\
E_8 &= S_7 = -\textstyle\sum_{i=0}^{2} m_i S_{i-3+7} = -(u^7u^{10} + u^{24}u^{11}) = u^6\\
E_9 &= S_8 = -\textstyle\sum_{i=0}^{2} m_i S_{i-3+8} = -(u^7u^{11} + u^{24}u^{18}) = u^9\\
E_{10} &= S_9 = -\textstyle\sum_{i=0}^{2} m_i S_{i-3+9} = -(u^7u^6 + u^{24}u^9) = u^{12}\\
E_{11} &= S_{10} = -\textstyle\sum_{i=0}^{2} m_i S_{i-3+10} = -(u^7u^{18} + u^{24}u^{12}) = u^2\\
E_{12} &= S_{11} = -\textstyle\sum_{i=0}^{2} m_i S_{i-3+11} = -(u^7u^9 + u^{24}u^2) = u^4\\
E_0 &= S_{12} = -\textstyle\sum_{i=0}^{2} m_i S_{i-3+12} = -(u^7u^{12} + u^{24}u^4) = u^0 (= 1),
\end{aligned}$$

vagyis a hibavektor Fourier-transzformáltja $u^0u^1u^{21}u^3u^{10}u^7u^{11}u^6u^{18}u^9u^{12}u^2u^4$.

Az inverz transzformáció $n = 13$ esetén $\varepsilon_i = (13 \cdot 1)^{-1} \sum_{j=0}^{12} (\alpha^{-i})^j E_j$, és $(13 \cdot 1)^{-1} = 1$ $\mathbb{F}_{27}$-ben. A számítás az előbbihez hasonló, és eredményként az $\boldsymbol{\varepsilon}'^T = 0001000001020$ vektort kapjuk, ami éppen az eredeti hibavektor.

A másik vektorral hasonlóan végezzük a számítást:

a szindróma: $u^3u^{13}u^9u^4u^{13}u^{13}$

a minimálpolinom: $x^3 + u^{11}x^2 + u^{22}x + u^2$

a teljes sorozat (egy hellyel való ciklikus jobbraléptetés után):

$0u^3u^{13}u^9u^4u^{13}u^{13}u^30u^3u^{12}u^{16}u^{20}$

a visszatranszformált sorozat: $2u^5u^{20}u^5u^5u^{20}u^4uu^{15}00u^{14}1$

és szemmel látható, hogy ez utóbbi nem $\mathbb{Z}_3$ fölötti.

c) **Dekódolás euklideszi algoritmussal**:

Megint összefoglaljuk a módszer lényegét. Ha egy alternáns kód ellenőrző mátrixának r sora van, akkor kiszámítva a szindrómát, és ebből képezve az S polinomot, euklideszi algoritmust végzünk az x^r és S polinommal addig, amíg a maradék fokszáma kisebb nem lesz r felénél. Közben az $U = 0, V = 1$ kezdőértékekkel minden lépés után kiszámítjuk a $W = U - t \cdot V$ polinomot, ahol t az éppen végrehajtott osztás hányadosa, és U új értéke az eddigi V, V új értéke pedig W lesz. Amikor a maradék fokszáma megfelelő, akkor $\hat{V}(0)$ inverzével szorozva V-t és a maradékot kapjuk a hibahely- és hibaérték-polinomot, σ-t és ω-t. σ gyökei megadják a hibahelyeket. Ha a gyök c, és c inverze a **H**-mátrix j-edik oszlopát generálja, akkor j egy hibás pozíció. Magát az ezen helyen fellépő hibát úgy kapjuk, hogy σ-t elosztjuk

$1 - c^{-1}x$-szel, a kapott polinomba behelyettesítjük c-t, ezt megszorozzuk az adott oszlopban szorzóként szereplő tényezővel, és az így kapott értékkel osztjuk az $\widehat{\omega}(c)$ értékét.

Először az első vektort vizsgáljuk:

A szindrómát meghatároztuk, $S = u^{11}x^5 + u^7x^4 + u^{10}x^3 + u^3x^2 + u^{21}x + u$, továbbá $r = 6$.

$$\begin{array}{l} x^6 : (u^{11}x^5 + u^7\ x^4 + u^{10}x^3 + u^3\ x^2 + u^{21}x + u) \ = u^{15}x + u^{24} = t \\ \quad u^9\ x^5 + u^{12}x^4 + u^5\ x^3 + u^{23}x^2 + u^3\ x \\ \qquad\quad u^4\ x^4 + u^{22}x^3 + u^8\ x^2 + u\ \ x + u^{12} \end{array}$$

$$r_1 = u^4x^4 + u^{22}x^3 + u^8x^2 + ux + u^{12}, \quad \deg(r_1) = 4 \geq 3$$

$$U = 1$$
$$V = 0 - 1 \cdot q = u^2x + u^{11}.$$

Mivel a maradék fokszáma 4, és ez nem kisebb r felénél, háromnál, ezért folytatjuk az algoritmust.

$$\begin{array}{l} (u^{11}x^5 + u^7x^4 + u^{10}x^3 + u^3x^2 + u^{21}x + u) \ : (u^4x^4 + u^{22}x^3 + u^8x^2 + ux + u^{12}) = u^7x + u^{23} \\ \quad u\ x^4 + u^{12}x^3 + u^5x^2 + u^{11}x + u \\ \qquad u^{24}x^3 \qquad\quad + u^{24}x + u^{15} \end{array}$$

$$r_2 = u^{24}x^3 + u^{24}x + u^{15}, \qquad \deg(r_2) = 3 \geq 3$$

$$U = \quad u^2x + u^{11}$$
$$V = u^{22}x^2 + u\ \ x + u^{14}$$

$$\begin{array}{l} (u^4x^4 + u^{22}x^3 + u^8x^2 + u\ \ x + u^{12}) : (u^{24}x^3 + u^{24}x + u^{15}) = u^6x + u^{24} \\ \quad + u^{22}x^3 + u^2x^2 + u^{23}x + u^{12} \\ \qquad\quad u^2x^2 + u^6\ x + u^9 \end{array}$$

$$r_3 = u^2x^2 + u^6x + u^9, \qquad \deg(r_3) = 2 < 3$$

$$U = \quad u^{22}x^2 + u\ \ x + u^{14}$$
$$V = u^{15}x^3 \qquad + u^6x + u^8$$

Most a maradék fokszáma $2 < 3$, így az osztást befejezzük. $\hat{V}(0) = u^8$, ennek inverzével, u^{18}-nal megszorozva V-t és az utolsó maradékot kapjuk, hogy

$$\sigma = u^7x^3 \qquad + u^{24}x + 1$$
$$\omega = \quad u^{20}x^2 + u^{24}x + u$$

Meghatározzuk σ gyökeit. Mivel a konstans tag nem nulla, ezért a 0 nem lehet gyöke a polinomnak (szerencsére). További helyettesítéssel kapjuk, hogy

$$\hat{\sigma}(1\ \ ) = u^7\ \ + u^{24} + 1 = u^2 \neq 0 \qquad \hat{\sigma}(u\ \ ) = u^{10} + u^{25} + 1 = u^5\ \ \neq 0$$
$$\hat{\sigma}(u^2) = u^{13} + 1\ \ + 1 = 1\ \ \neq 0 \qquad \hat{\sigma}(u^3) = u^{16} + u\ \ + 1 = u^{18} \neq 0$$
$$\hat{\sigma}(u^4) = u^{19} + u^2\ \ + 1 = u^* = 0.$$

u^4 inverze u^{22}, ez α^{11}, ami a paritásellenőrző mátrix 11. oszlopát generálja, így a 11. pozíció hibás. Határozzuk meg a hiba értékét ebben a pozícióban.

$$
\begin{array}{l}
(u^7x^3 \quad\quad + u^{24}x + 1) : (u^9x + 1) = u^{24}x^2 + u^2x + 1 = \sigma^{(0)} \\
\quad\quad u^{11}x^2 + u^{24}x + 1 \\
\quad\quad\quad\quad + u^9\ x + 1 \\
\quad\quad\quad\quad\quad\quad\ \ 0
\end{array}
$$

$$\hat{\sigma}^{(0)}(u^4) = u^{24}\,u^8 + u^2\ \ u^4\ \ + 1 = u^{15} \neq 0$$
$$\widehat{\omega}\quad(u^4) = u^{20}\,u^8 + u^{24}\,u^4\ \ + u = u^{24}.$$

A 11. oszlopban a szorzó α^{11}, ezért $\widehat{\omega}(u^4) = u^{24}$-t $u^{22} \cdot \hat{\sigma}^{(0)}(u^4) = u^{11}$-nel kell osztani, és az eredmény $u^{13} = -1$.

A következő gyököket közvetlenül megkapjuk $\sigma^{(0)}$-ból. Ez egy másodfokú polinom, és ha egy test karakterisztikája különbözik kettőtől, akkor alkalmazható az ismert megoldóképlet. Ezzel

$$x_{1,2} = \frac{-u^2 \pm \sqrt{u^4 - u^{24}}}{-u^{24}} = \frac{u^{15} \pm u^{13}}{u^{11}},$$

ahonnan a két gyök $x_1 = u^8$, $x_2 = u^{20}$, és az előző gyököt is figyelembe véve

$$\sigma = (1 - u^{22}x)(1 - u^{18}x)(1 - u^6x) = (u^9x + 1)(u^5x + 1)(u^{19}x + 1).$$

Az első gyök inverze α^9, a hiba helye tehát a 9. pozíció.

$$\sigma^{(1)} = (u^9x + 1)(u^{19}x + 1) = u^2x^2 + u^{10}x + 1,$$

ennek értéke az x_1 helyen $u^2\,u^{16} + u^{10}\,u^8 + 1 = u^{19}$,

$$\widehat{\omega}(u^8) = u^{20}\,u^{16}\ + u^{24}\,u^8 + u = u^{11}.$$

Az oszlop szorzója $\alpha^9 = u^{18}$, így a hiba értéke $u^{11}(u^{18}\,u^{19}\,)^{-1} = 1$.

Hasonlóan járunk el x_2 esetén. u^{20} inverze $u^6 = \alpha^3$, a hiba helye a 3. pozíció;

$$\sigma^{(2)} = (u^9x + 1)(u^5x + 1) = u^{14}x^2 + u^8x + 1,$$

$$\hat{\sigma}^{(2)}(u^{20}) = u^{14}\,u^{20}\ + u^8\ \ u^{20}\ + 1 = u^5$$
$$\widehat{\omega}\quad(u^{20}) = u^{20}\,u^{14}\ + u^{24}\,u^{20}\ + u = u^{11}.$$

$u^{11}(u^6\,u^5\,)^{-1} = 1$, azaz három hiba van, és a számított hibavektor $\boldsymbol{\varepsilon}'^T = 0001000001020$, a dekódolás ismét helyes eredményre vezetett.

Nézzük a másik hibát. Most $S = u^{13}x^5 + u^{13}x^4 + u^4x^3 + u^9x^2 + u^{13}x + u^3$ lesz a szindróma. Ha elvégezzük az algoritmust, akkor

$$
\begin{array}{ll}
\sigma = & u^2x^3 + u^{22}x^2 + u^{11}x + 1 \\
\omega = u^2x^4 & \quad\quad + u^{21}x + u^3
\end{array}
$$

lesz a két polinom. Behelyettesítve $\mathbb{F}_{27}$ elemeit azt tapasztaljuk, hogy ennek a polinomnak nincs gyöke, vagyis a hibát nem tudjuk korrigálni (de már az gyanús, hogy ω fokszáma nagyobb σ fokszámánál).

Érdemes megfigyelni, hogy a rekurzív sorozatok esetén kapott minimálpolinom, valamint az euklideszi algoritmus során nyert σpolinom éppen egymás reciproka, így az egyik gyökei pontosan a másik gyökeinek inverzei. Ez persze világos, ha meggondoljuk, hogy a rekurzív sorozattal való dekódoláshoz mi volt a sorozatot generáló lineáris összefüggésben az együtthatók definíciója. Amennyiben a kód bináris, akkor a hiba értéke pontosan 1, vagyis ilyen esetben elegendő a hibahelypolinom meghatározása,

így ilyenkor a rekurzív sorozatokkal történő dekódolásnál a sorozat további elemeinek generálása és visszatranszformálás helyett elegendő a minimálpolinom gyökeinek meghatározása.

Tárgymutató

A,Á

B

C

Cs

D

E,É

G

H

I,Í

K

Irodalomjegyzék

Berlekamp, E. R.
Algebraic Coding Theory
McGraw Hill, 1968.

Csiszár, I., Fritz, J.
Információelmélet
Tankönyvkiadó, 1986.

Gonda, J.
Véges testek
http://www.inf.elte.hu/karunkrol/digitkonyv/Jegyzetek2011/GondaJanos-VegesTestek15.pdf, 2011.

Györfi, L., Győri, S., Vajda, I.
Információ- és kódelmélet
Typotex Kiadó, 2000.

Györfi, L., Vajda, I.
A hibajavító kódolás és a nyilvános kulcsú rejtjelezés elemei
Műegyetemi Kiadó, 1990.

Huffman, W. C., Pless, V.
Fundamentals of Error-Correcting Codes
Cambridge University Press, 2003.

Linder, T., Lugosi, G.
Bevezetés az információelméletbe
Műegyetemi Kiadó, 1993.

van Lint, J. H.
Introduction to Coding Theory
Springer Verlag, 1982.

Lucky, R. W., Salz, J., Weldon, E. J.
Adatátvitel
Műszaki Könyvkiadó, 1973.

MacWilliams, F. J., Sloane, M. J. A.
The Theory of Error-Correcting Codes
North-Holland, 1977.

Reza, F. M.
Információelmélet
Műszaki Könyvkiadó, 1963.

Roman, S.
Coding and Information Theory
Springer Verlag, 1992.

Shannon, C. E.
A mathematical theory of communication
Bell System Technical Journal, 1948.

Shannon, C. E., Weaver, W.
A kommunikáció matematikai elmélete
Országos Műszaki Információs Központ és Könyvtár, Budapest, 1986.

Tsfasman, M. A., Vlăduţ, S. G.
Algebraic-Geometric Codes
Kluwer Academic Publishers, 1991.

Vajda, I.
Hibajavító kódolás és műszaki alkalmazásai
BME Mérnöki Továbbképző Intézete, 1982.