1. 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.

1.1. 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).

1.2. 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.

1.3. 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 egy a eleme **balról reguláris**, ha az $\mathcal{A}$ 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.

1.4. 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).

1.5. 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.

□

1.6. 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.

□

1.7. 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.

□

1.8. 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 $a^k = a^l$.

1.9. 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

1.10. 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 $a^{k+t} = a^{l+t}$.

1.11. 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.

1.12. 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.

1.13. 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.

□

1.14. 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.

1.15. 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

1.16. 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 $\bar{e} = \overline{r'a + m'} = \overline{r'}\bar{a} + \overline{m'} = \overline{r'}\bar{a} + \bar{0} = \overline{r'}\bar{a}$, és így $\mathcal{R}/\mathcal{M}$-ben $\overline{r'}$ 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.

Egy gyűrű bármely ideálja egyben bal oldali ideálja is 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 akkor 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.

1.17. 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.

□

1.18. 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.

1.19. 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

1.20. 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 $\mathcal{I}$ az $\mathcal{I}_\gamma$-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 $\bigcup_{\substack{\Delta\subseteq\Gamma \\ |\Delta|\in\mathbb{N}}} \sum_{\gamma\in\Delta} \mathcal{I}_\gamma \subseteq \mathcal{I}$-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 $\mathcal{I}_\gamma$ összegében, hiszen $ru^{(i)} = \sum_{\gamma\in\Delta_i} ra_\gamma^{(i)} \in \sum_{\gamma\in\Delta} I_\gamma$.

□

Ha $\mathcal{I}_1$ és $\mathcal{I}_2$ két ideál, $a_1^{(1)} \in \mathcal{I}_1$, $a_2^{(1)} \in \mathcal{I}_1$, $a_1^{(2)} \in \mathcal{I}_2$, $a_2^{(2)} \in \mathcal{I}_2$, 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 $\mathcal{I}_1$-beli, míg a másik különbség az $\mathcal{I}_2$ 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).

1.21. 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.

1.22. 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 $\sum_{a\in A}(a) = \bigcap_{b\in B}(b)$.

□

1.23. 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.

1.24. 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.

1.25. Tétel

Ha $\mathcal{I}$ és minden $\gamma \in \Gamma$-ra $\mathcal{J}_\gamma$ az $\mathcal{R}$ gyűrű ideálja, továbbá 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 művelettartó, ezért $\varphi\big(\sum_{\gamma\in\Delta} j_\gamma\big) = \sum_{\gamma\in\Delta}\varphi\big(j_\gamma\big)$, ennélfogva

$$\varphi\left(\sum_{\gamma\in\Gamma}\mathcal{J}_\gamma\right) = \varphi\big(\big\{\textstyle\sum_{\gamma\in\Delta} j_\gamma \,\big|\Delta \subseteq \Gamma \wedge |\Delta| \in \mathbb{N}\big\}\big) = \big\{\varphi\big(\textstyle\sum_{\gamma\in\Delta} j_\gamma\big)\big|\Delta \subseteq \Gamma \wedge |\Delta| \in \mathbb{N}\big\}$$
$$= \big\{\textstyle\sum_{\gamma\in\Delta}\varphi\big(j_\gamma\big) \,\big|\Delta \subseteq \Gamma \wedge |\Delta| \in \mathbb{N}\big\} = \sum_{\gamma\in\Gamma}\varphi\big(\mathcal{J}_\gamma\big),$$

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 $f\big(\bigcap_{\gamma\in\Gamma} A_\gamma\big) \subseteq \bigcap_{\gamma\in\Gamma} f\big(A_\gamma\big)$, $f^{-1}(\bigcap_{\delta\in\Delta} B_\delta) = \bigcap_{\delta\in\Delta} f^{-1}(B_\delta)$, 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 $\varphi\big(\bigcap_{\gamma\in\Gamma}\mathcal{J}_\gamma\big) = \bigcap_{\gamma\in\Gamma}\varphi\big(\mathcal{J}_\gamma\big)$.

□

1.26. 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.

1.27. 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.

1.28. 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 $\left(\bar{b}\right)$ 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 $\bar{u} = \bar{\varepsilon}$.

□

1.29. 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.

1.30. 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.

□

1.31. 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

1.32. 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.

1.33. 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.

1.34. 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. $\sum_{i\in K}\left(\frac{\overline{a}}{a_i}\right) = \bigcap_{i\in L}(\overline{a}_i) = (\prod_{i\in L}\overline{a}_i) = (\overline{b})$;
2. $\bigcap_{\delta\in\Delta}\sum_{i\in U_\delta}\left(\frac{\overline{a}}{a_i}\right) = (\overline{0})$;
3. $\bar{u} \in (\overline{b})$ egy- és csak egyféleképpen írható $\left(\frac{\overline{a}}{a_i}\right)$-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 $\sum_{i\in K}\left(\frac{\bar{a}}{a_i}\right) = \left(\bar{d}_K\right) = \left(\overline{\prod_{\iota\in L} a_\iota}\right) = \left(\prod_{i\in L}\bar{a}_i\right) = \bigcap_{i\in L}(\bar{a}_i)$;
2. $\bigcap_{\delta\in\Delta}\sum_{i\in U_\delta}\left(\frac{\bar{a}}{a_i}\right) = \bigcap_{\delta\in\Delta}\bigcap_{i\in\mathbb{N}_m\setminus U_\delta}(\bar{a}_i) = \left(\overline{\prod_{\delta\in\Delta}\prod_{\iota\in\mathbb{N}_m\setminus U_\delta} a_\iota}\right) = \left(\overline{\prod_{\iota\in\bigcup_{\delta\in\Delta}\mathbb{N}_m\setminus U_\delta} a_\iota}\right) = \left(\overline{\prod_{\iota\in\overline{\bigcap_{\delta\in\Delta} U_\delta}} a_\iota}\right) = \left(\overline{\prod_{\iota\in\bar{\emptyset}} a_\iota}\right) = \left(\overline{\prod_{\iota\in\mathbb{N}_m} a_\iota}\right) = (\bar{a}) = (\bar{0})$;
3. az előző pont alapján minden $i \in \mathbb{N}_m$-re $\left(\frac{\bar{a}}{a_i}\right) \cap \sum_{j\in K\setminus i}\left(\frac{\bar{a}}{a_i}\right) = (\bar{0})$.

□

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.

1.35. 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

1.36. 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 $\overline{\varepsilon^{(\imath)}}\cdot\overline{\varepsilon^{(\jmath)}}$ az $\mathcal{R}_{(a)}$ nulleleme;
2. $\sum_{i=0}^{m-1}\overline{\varepsilon^{(\imath)}} = \bar{e}$;
3. minimális ideálban a generáló idempotensen kívül csak a nullelem idempotens;

Δ

Bizonyítás:

1. $\overline{\varepsilon^{(\imath)}}\cdot\overline{\varepsilon^{(\jmath)}}$ 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 $\sum_{i=0}^{m-1}\overline{\varepsilon^{(\imath)}} = \bar{e}$.
3. Legyen ε idempotens az $\overline{\varepsilon^{(\imath)}}$-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.

1.37. 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 $\overline{w} = \bar{v}\bar{\varepsilon}$ mint az $\mathcal{M}$ ideál egy elemének többszöröse maga is eleme M-nek, és $\bar{\varepsilon} = \bar{\varepsilon}^2 = \bar{u}\bar{v}\bar{\varepsilon} = \bar{u}\overline{w}$, 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.

1.38. 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 egy nem triviális ideál szerinti maradékosztály-gyűrű – egymást kizáró módon – vagy 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.

1.39. 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 1.30. Tételnek és 1.31. Megjegyzésnek.

□

1.40. 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 $\mathbf{G} = \begin{pmatrix} \boldsymbol{\varepsilon}_{\overrightarrow{0}} \\ \vdots \\ \boldsymbol{\varepsilon}_{\overrightarrow{i}} \\ \vdots \\ \boldsymbol{\varepsilon}_{\overrightarrow{k-1}} \end{pmatrix}$ mátrix sorai a kód egy generátorrendszere, ahol $\boldsymbol{\varepsilon}$ az ε polinomhoz tartozó kódszó, és $k > i \in \mathbb{N}$-re $\boldsymbol{\varepsilon}_{\overrightarrow{i}}$ 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 $\boldsymbol{\varepsilon}_{\overrightarrow{i}}$ is kódszó (ahol $\boldsymbol{\varepsilon}_{\overrightarrow{0}} = \boldsymbol{\varepsilon}$), 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 $a = 0$.

□

1.41. 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.

□

1.42. 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.

1.43. 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.

2. Maradékkód

Az alább definiálandó kódhoz szükségünk lesz a következő eredményre.

2.1. 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 $\frac{p-1}{t}$.

2.2. 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 17. oldalon kapott eredmény szerint $\left(C^{(r)}\right)_e = (C_e)^{(r)}$ és $\left(C^{(r)}\right)_o = (C_o)^{(r)}$.

2.3. Tétel

A 2.2. 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.

2.4. 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 1.43. 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.

2.5. 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 19. 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.

2.6. 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 $\text{modulo } n$ 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.

2.7. 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 $\text{modulo } n$, ha vagy mindkettő maradék, vagy mindkettő nemmaradék. $-s = (-1) \cdot s$, és $s \in NQ$, így $-s$ maradék, ha a -1 is nemmaradék $\text{modulo } n$, 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.

2.8. 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 $\text{modulo } p$ 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 $(e + E)^2 = e + E^2$.

□

2.9. 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.

2.10. 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 $\theta^2 = \varepsilon p e$.

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

$$\theta^q = \left(\sum_{i=0}^{p-1} \chi(i)\alpha^i\right)^q = \sum_{i=0}^{p-1} \left(\chi(i)\alpha^i\right)^q$$
$$= \sum_{i=0}^{p-1} \left(\chi(i)\right)^q \left(\alpha^i\right)^q = \sum_{i=0}^{p-1} \chi(qi)\alpha^{qi} = \sum_{i=0}^{p-1} \chi(i)\alpha^i = \theta,$$

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.

2.11. 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 $\bar{\mathbf{G}}$ 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 $\bar{\mathbf{G}}$-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.

2.12. 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.

2.13. 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.

2.14. 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.

2.15. 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 **u** képét $\mathcal{GP}(\mathbf{u})$-val jelöljük.

Δ

2.16. 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

2.17. Tétel

A 2.15. Definíció szerinti **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.

□

2.18. 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.

2.19. 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

2.20. 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 $R_0+R_\infty=\psi(R_0)$, 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 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 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.

2.21. 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 2.6. Tétellel rögtön kapjuk az alábbi eredményt.

2.22. 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

3. A Golay-kód

Elsőként egy, látszólag a kódolástól távol eső kérdéssel foglalkozunk.

3.1. 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.

3.2. 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.

3.3. 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 $i = 1$.

3.4. 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 $b\binom{k}{t} = \lambda\binom{v}{t}$.

3.5. 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, $b\binom{k}{t} = \sum_{|U|=t,\, U\subseteq X} \lambda(U) \leq \lambda\binom{v}{t} = b\binom{k}{t}$. 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 2.22. 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.

3.6. 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. $\mathbf{u}$-ban még $w'-p$ olyan hely van, ahol 0-tól különböző elem van, és $\mathbf{v}$ 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 $\mathbf{v}$-ben bármi állhat, kivéve a 0-t, és az s-számú helyen is szinte bármi lehet $\mathbf{v}$-ben a 0-t és azt az egyetlen karaktert leszámítva, amely $\mathbf{u}$-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 $A_{12} = 24$.

3.7. 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 3.2. 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 $216=16\cdot 13+8\le (n+1)(n-2)+8=8(2m+1)\le 24$, 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.

3.8. Tétel

Ha egy bináris, (n, M, d)-paraméterű C kódban $n=23$, $M\ge 2^{12}$ és $d\ge 7$, akkor a kód ekvivalens a bináris Golay-kóddal, míg egy, a $\mathbf{0}$-t tartalmazó, $(24, M\ge 2^{12}, d\ge 8)_2$-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 3.5. 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.

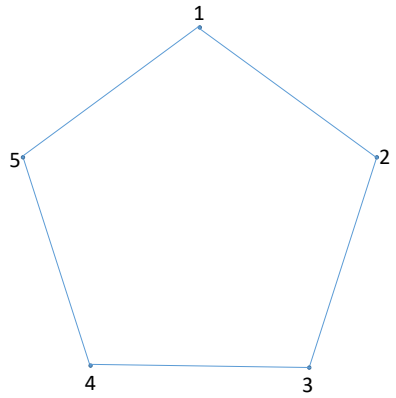
Ha $i\neq j$, akkor $E_{p_i}\neq E_{p_j}$, tehát a két gráf is különböző, mert láttuk, hogy a két gráfnak két közös éle van, de ha a két gráf azonos lenne, akkor legfeljebb csak egy másodfokú csúcs lenne.

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 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

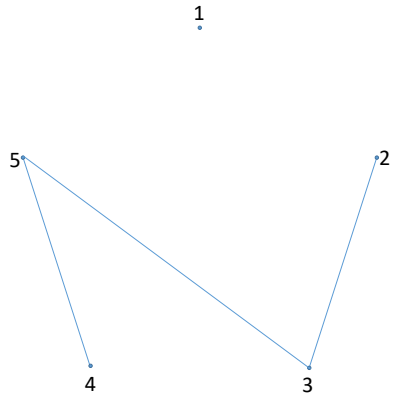
[1] Az egyértelműség bizonyításánál az Interneten a http://www.cs.elte.hu/~csiki/golay.pdf címen található, Csikvári Péter által írt Golay-kód és Witt-design című munkára támaszkodunk.

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.

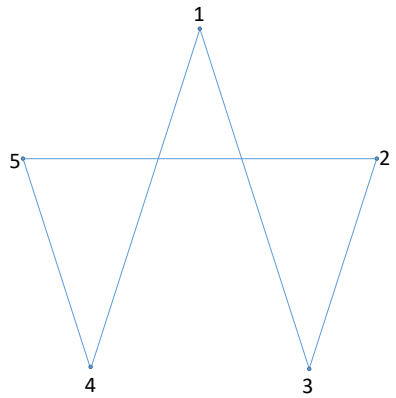


1. ábra

Legyen az egyik gráf olyan, ahol a kör pontjai az indexek sorrendjében követik egymást, amint az 1. 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 2. 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.



2. ábra



3. 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 3. 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.

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

$$\mathbf{G} = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&1&1&0&0\\
1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&0&1&1&0\\
1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&0&1&1&1&0\\
1&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&0&0&1&1&0&0&1\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1\\
1&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&1&0&1&1&0&1\\
1&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&1&0&1&0&0&1&1\\
1&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&0&1&0&1&1\\
1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&0&0&0&0&1&1&1
\end{pmatrix}$$

□

Korábban már találkoztunk az Hadamard-mátrixokkal és a belőlük közvetlenül származtatott kódokkal. Most majd a Golay-kódokhoz fogjuk ezeket a mátrixokat alkalmazni.

Az alábbiakban $n \in \mathbb{N}$-re $\mathbf{I}_n$ az n-méretű egységmátrix, és ^{T} a transzponálás jele.

3.9. 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.

3.10. 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.

□

3.11. 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 $p_{i,j} = \big(\mathbf{P}_q\big)_{i,j} = \nu\big(a_i - a_j\big)$, a q-**adrendű Paley-mátrix**.

Δ

3.12. 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:

$$p_{i,j}^T = p_{j,i} = \nu\big(a_j - a_i\big) = \nu\Big(-e\big(a_i - a_j\big)\Big) = \nu(-e)\nu\big(a_i - a_j\big) = (-1)^{\frac{q-1}{2}} p_{i,j},$$

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.

$$\big(\mathbf{P}_q\mathbf{P}_q^T\big)_{i,k} = \sum_{j=0}^{q-1} p_{i,j}p_{j,k}^T = \sum_{j=0}^{q-1} p_{i,j}p_{k,j} = \sum_{j=0}^{q-1} \nu\big(a_i - a_j\big)\nu\big(a_k - a_j\big) = \sum_{j=0}^{q-1} \nu\Big(\big(a_i - a_j\big)\big(a_k - a_j\big)\Big)$$
$$= \sum_{j=0}^{q-1} \nu\Big(\big(a_i - a_j\big)\big(\big(a_i - a_j\big) + \big(a_k - a_i\big)\big)\Big) = \sum_{c\in\mathbb{F}_q} \nu\big(c(c+h)\big) = -1 + \delta_{h,0}q,$$

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.

3.13. Tétel

Legyen q egy $4k+3$ alakú prímszám páratlan kitevős hatványa és $\mathbf{P}_q$ a q-adrendű Paley-mátrix. Ekkor a

$$\mathbf{H}_{q+1} = \begin{pmatrix} 1 & \mathbf{1}_q^T \\ \mathbf{1}_q & -(\mathbf{P}_q + \mathbf{I}_q) \end{pmatrix}$$

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:

$$\mathbf{H}_{q+1}\mathbf{H}_{q+1}^T = \begin{pmatrix} 1 + \mathbf{1}_q^T\,\mathbf{1}_q & \mathbf{1}_q^T - \mathbf{1}_q^T(\mathbf{P}_q^T + \mathbf{I}_q) \\ \mathbf{1}_q - (\mathbf{P}_q + \mathbf{I}_q)\,\mathbf{1}_q & \mathbf{1}_q\mathbf{1}_q^T + (\mathbf{P}_q + \mathbf{I}_q)(\mathbf{P}_q^T + \mathbf{I}_q) \end{pmatrix}$$
$$= \begin{pmatrix} q+1 & \mathbf{0}_q^T \\ \mathbf{0}_q & (q+1)\mathbf{I}_q \end{pmatrix} = (q+1)\mathbf{I}_{q+1},$$

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.

□

3.14. 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.

3.15. Definíció

Ha **A** egy $p \times q$ és **B** egy $r \times s$ méretű mátrix, akkor az **A** és **B** **A** $\otimes$ **B**-vel jelölt **Kronecker-szorzat**a az a $pr \times qs$-méretű **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

$$\sum_j (a_{i,j}\mathbf{B})(c_{j,k}\mathbf{D}) = \mathbf{BD}\sum_j a_{i,j}c_{j,k} = (\mathbf{AC})_{i,k}\,\mathbf{BD},$$

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:

$$(\mathbf{A}\otimes\mathbf{B})^{\boldsymbol{T}} = \begin{pmatrix} a_{0,0}\mathbf{B} & \cdots & a_{0,j}\mathbf{B} & \cdots & a_{0,q-1}\mathbf{B} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i,0}\mathbf{B} & \vdots & a_{i,j}\mathbf{B} & \vdots & a_{i,q-1}\mathbf{B} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{p-1,0}\mathbf{B} & \cdots & a_{p-1,j}\mathbf{B} & \cdots & a_{p-1,q-1}\mathbf{B} \end{pmatrix}^{\boldsymbol{T}} = \begin{pmatrix} a_{0,0}\mathbf{B}^T & \cdots & a_{i,0}\mathbf{B}^T & \cdots & a_{p-1,0}\mathbf{B}^T \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{0,j}\mathbf{B}^T & \vdots & a_{i,j}\mathbf{B}^T & \vdots & a_{p-1,j}\mathbf{B}^T \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{0,q-1}\mathbf{B}^T & \cdots & a_{i,q-1}\mathbf{B}^T & \cdots & a_{p-1,q-1}\mathbf{B}^T \end{pmatrix}$$

$$= \begin{pmatrix} a_{0,0}^T\mathbf{B}^T & \cdots & a_{0,i}^T\mathbf{B}^T & \cdots & a_{0,p-1}^T\mathbf{B}^T \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{j,0}^T\mathbf{B}^T & \vdots & a_{j,i}^T\mathbf{B}^T & \vdots & a_{j,p-1}^T\mathbf{B}^T \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{q-1,0}^T\mathbf{B}^T & \cdots & a_{q-1,i}^T\mathbf{B}^T & \cdots & a_{q-1,p-1}^T\mathbf{B}^T \end{pmatrix} = \mathbf{A}^T\otimes\mathbf{B}^T.$$

3.16. 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

$$(\mathbf{H}_m\otimes\mathbf{H}_n)(\mathbf{H}_m\otimes\mathbf{H}_n)^T = \mathbf{H}_m\mathbf{H}_m^T\otimes\mathbf{H}_n\mathbf{H}_n^T = (m\mathbf{I}_m)\otimes(n\mathbf{I}_n) = (mn)\mathbf{I}_{mn},$$

és ez igazolja, hogy a Kronecker-szorzat is Hadamard-mátrix, amelynek 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.

3.17. 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 $\mathbf{H} = (-\mathbf{A}_{q+1}^T, \mathbf{I}_{q+1}) = (\mathbf{A}_{q+1}, \mathbf{I}_{q+1}) = \mathbf{G}$.

3.18. 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: $\mathbf{c} = (\mathbf{c}_b, \mathbf{c}_j)$, ahol mindkét rész 12-bites. $\mathbf{c}_b$-t is $\mathbf{I}_{12}$-ből kaphatjuk nemtriviális kombinációval, $\mathbf{c}_j$-t is, ezért $w(\mathbf{c}_b) \neq 0 \neq w(\mathbf{c}_j)$. 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 $w(\mathbf{c}_j) \neq 1$, tehát $w(\mathbf{c}_b) \geq 2$ és $w(\mathbf{c}_j) \geq 2$. De $w(\mathbf{c}) = 4$ a feltételezés szerint, így csak $w(\mathbf{c}_b) = 2 = w(\mathbf{c}_j)$ 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 $\mathbf{G}$ az alábbi mátrix:

$$\mathbf{G} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&1&1&0&1&1&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&1&1&0&1&1&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&1&0&1&1&0&1&1&1\\
0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0&1&0&1&1&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&0&0&0&1&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&1&0&1
\end{pmatrix}$$

A 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.

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.

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.

Az előbbi esetek láthatóak táblázatos formában, 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
$5 \leq u$	$5 \leq v$	az egyik részben pontosan 1 hiba, a másikban legfeljebb 2, és $\mathbf{u}^{(i)}$-vel korrigálhatunk
és egy $\mathbf{u}^{(i)}$-vel pontosan az egyikre 1 és 3 közé esik (a határok is jók), míg a másiknál legalább 5		
minden más esetben		3-nál több hiba

4. 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 $k = \sum_{i=0}^{m-1} k_i q^i$. 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 $p = p^{(0)} + x_m p^{(1)}$ 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.

4.1. 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.

4.2. 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.

4.3. 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 4.2. és 4.3. Tétel alapján meg tudjuk határozni a Reed-Muller kódok generátor- és ellenőrző mátrixát és paramétereit. Ezt írja le a következő tétel.

4.4. 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.

4.5. 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 $P^{(i-1)}=0$.

5. 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 idempotensének meghatározásához felhasználható Perron tétele[2], bár az eredetihez képest kicsit általánosabban adjuk 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 $|(a + NQ) \cap NQ| = \big|z\big((a + NQ) \cap NQ\big)\big| = |(b + Q) \cap Q|$. 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.

5.1. Tétel

Legyen q egy páratlan prím pozitív egész kitevős hatványa, $Q = \big\{r \in \mathbb{F}_q^* \big| \exists\big(s \in \mathbb{F}_q\big)\colon s^2 = r\big\}$ 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

$$\begin{aligned} a^2 \qquad\qquad + (p-1)bc \qquad\qquad &= a \\ 2ab \quad + \frac{1}{4}(p-3)b^2 + \frac{1}{2}(p-3)bc + \frac{1}{4}(p+1)c^2 &= b \\ 2ac + \frac{1}{4}(p+1)b^2 + \frac{1}{2}(p-3)bc + \frac{1}{4}(p-3)c^2 &= c. \end{aligned}$$

Hasonlóan tudjuk meghatározni az egyenleteket a $p = 4k+1$ esetre, és az eredmény

$$\begin{aligned} a^2 \quad + \frac{1}{2}(p-1)b^2 \quad + \frac{1}{2}(p-1)c^2 &= a \\ 2ab \quad + \frac{1}{4}(p-5)b^2 + \frac{1}{2}(p-1)bc + \frac{1}{4}(p-1)c^2 &= b \\ 2ac + \frac{1}{4}(p-1)b^2 + \frac{1}{2}(p-1)bc + \frac{1}{4}(p-5)c^2 &= c. \end{aligned}$$

(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.