

# Hamming-kód

## Definíció.

Az 1-hibajavító, perfekt lineáris kódot *Hamming-kódnak* nevezzük.

$F_2$  fölötti vektorokkal foglalkozunk.

## Hamming-kód készítése:

$r$  egész szám (ellenőrző jegyek száma)

$n=2^r-1$  a kódszavak hossza

$k=2^r-1-r$  a közleményszavak hossza

A  $H$  ( $r \times n$ )-es mátrix  $j$ -edik oszlopában a  $j$  2-es számrendszerbeli alakjának jegyei szerepelnek. \*

## 14. Példa:

$r=3$   $n=7$   $k=4$  a  $[7,4]$  kód ellenőrző mátrixa:

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

## 9. tétel:

Az előbbi szabállyal megadott kód Hamming-kód.

### Bizonyítás:

- A fenti \* szabállyal megadott H mátrixban van három összefüggő oszlop, de bármely kettő lineárisan független. Így a kód minimális távolsága  $d=3$ .

1-hiba javító a kód.

- A Hamming-korlát teljesülése

Mivel 1-hibajavító

$$|K| \cdot \left( \binom{n}{0} + \binom{n}{1} \right) \leq 2^n$$

A kódszavak hossza  $n=k+r$ :

$k=2^r-1-r$	$r$
-------------	-----

$$|K| = 2^{2^r-1-r}$$

Ezt behelyettesítve a Hamming-korlátba:

$$|K| \cdot \left( \binom{2^r-1}{0} + \binom{2^r-1}{1} \right) = 2^{2^r-1-r} (1 + 2^r - 1) = 2^{2^r-1} = 2^n$$

Beláttuk, hogy perfekt a kód:  
a kódszavak körüli 1 sugarú gömbökben minden  
lehetséges  $2^r-1$  jegyű szó pontosan egyszer fordul elő.

A \* szabállyal Hamming kódot adtunk meg.



## Példa.

Adjuk meg a 14. példabeli [7, 4] Hamming-kód H ellenőrző mátrixának ismeretében a kód (egyik) generátormátrixát.

---

Megfelelő S permutációs mátrixsal a kódunk H ellenőrző mátrixa

$HS=(I_{n-k}, P)$  alakra hozható.

$$P = -P \pmod{2}.$$

A  $G=(P^T, I_k) \cdot S^T$  mátrix a H-nak megfelelő generátormátrix:

$$H \cdot G^T = H \cdot S \cdot \begin{pmatrix} P \\ I_k \end{pmatrix} = (I_{n-k}, P) \cdot \begin{pmatrix} P \\ I_k \end{pmatrix} = P + P = 0$$

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

az oszlopok (3,4)

transzpozíciójával

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

A  $H_1$ -nek megfelelő  $G_1$  mátrix ( $P^T, I_k$ ) alakú:

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ebből a transzpozíciót újra alkalmazva megkapjuk a keresett  $G$  mátrixot.

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

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

Ha ezt a generátormátrixot alkalmazzuk a kódolásnál, mi lesz a (0 1 1 1) üzenet kódja?

A (0 1 1 1) vektort jobbról szorozzuk G-vel.

Az eredmény: (0 0 0 1 1 1 1)

## Hibajavítás Hamming-kóddal:

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

A [7,4] Hamming-kód esetén  $b^T=(0001111)$  kódszó.

$$H \cdot b = \underline{0} = (0 \ 0 \ 0)^T.$$

Tegyük fel, hogy az átvitel során egy hiba történt, mégpedig a 3. helyen.

Az  $e^T=(0010000)$  a hibavektor, a  $(b+e)^T=(0011111)$  vektor érkezik meg a csatornán.

$$H \cdot (b+e) = (110)^T$$

Ez a vektor a H mátrix 3. oszlopa, alulról olvasva éppen a 3 bináris alakja, rámutat arra, hogy a 3. pozícióban van a hiba.

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

Tegyük fel, hogy az átvitel során egy hiba történt, mégpedig a 7. helyen.

$e=(0000001)$  a hibavektor,

$$H \cdot (b+e) = H \cdot (0 \ 0 \ 0 \ 1 \ 1 \ 1)^T = (1 \ 1 \ 1)^T$$

Ez a 7 bináris értéke, ami azt mutatja, hogy a 7. jegy hibás.

Ezzel a módszerrel mindig megkapjuk a hiba helyét, feltéve, hogy legfeljebb 1 hiba történt.



Egynél több hiba esetén a kód nem működik helyesen.

Időnként nem ismeri fel a hibát, vagy rosszul javítja.

Ha olyan hiba lép fel, mely maga is kódszó, akkor  $H \cdot (b+e) = 0$  olyan mintha nem történt volna hiba.

Ha a hiba két 1-est tartalmaz (kéthiba), akkor a kód egyhibának tekinti.

## 16. példa.

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

[7,4] Hamming-kódnál feltételezve, hogy egynél több hiba nem lépett fel az átvitelnél, mi volt a továbbított kódvektor, ha

1.  $a^T = (0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0)$
2.  $b^T = (0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0)$  érkezett.

---

1.  $H \cdot a = (0 \ 1 \ 1)^T.$

A 6. hely hibás,  $(0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0)^T$  volt a küldött szó.

2.  $H \cdot b = (0 \ 0 \ 0)^T.$

A kapott szó hibátlan.

# BCH-kód

A Hamming-kód a kódelmélet hajnalán, az 1940-es évek végére született meg.

Több mint 10 évvel később történt a hasonló hatékonyságú 2-hibajavító kódok kifejlesztése.

## **BCH-kódok:**

R. C. Bose, D. K. Chaudhuri és A. Hocquenghem.

A véges testek nagy szerepe.

A kételemű test ( $\mathbb{F}_2 = \mathbb{T}$ ) feletti  $[n, k]$  kódokkal foglalkozunk.

$k$  a kód dimenziója,

$n$  a hossza,

$r = n - k$  az ellenőrző jegyek száma

$t$ -hibajavító kódot keresünk.

Legyen  $n = k + r$  rögzített, minél kisebb  $r$  értékkel minél nagyobb  $k$  értéket igyekszünk biztosítani.

Más szavakkal  $\mathbb{T}^n$ -ben keresünk minél nagyobb  $K$  alteret, amelynek elemei (a kódszavak) legalább  $2t + 1$  távolságra vannak egymástól.

Megfelelő méretű  $H$  ellenőrző mátrixot készítünk.  $H$ -nak minél kevesebb sora legyen.

Először olyan  $Q$  ( $m \times n$ -es) mátrixot készítünk, amelynek bármely  $2t$  oszlopa lineárisan független és lehetőleg kevés sora van.

Másként:  $Q$  bármely legfeljebb  $t$  oszlopának összege legyen különböző egymástól és ne legyen nulla vektor.

Ez a  $Q$  egy  $t$ -hibajavító kódot definiál, így  $Q$  a kód *kvázi-paritásellenőrző mátrixa*.

Ha  $Q$  sorai nem függetlenek, bizonyos sorokat –amelyek függnék a többitől - elhagyhatunk, hogy a maradék sorok függetlenek legyenek.

(Ez nem változtat a mátrix hibajavítással kapcsolatos tulajdonságain.)

## 2-hibajavító BCH-kód.

$t=2$ . Legyen  $q \geq 3$  és  $n=2^q-1$ .

Hamming-korlátból adódik, hogy  $r \geq 2q-1$ . A 2-hibajavító BCH kódnál  $r \leq 2q$ .  
(Belátható, hogy  $r = 2q$  teljesül.)

Azonos  $n$  mellett a Hamming-kódhoz képest a 2-hibajavító BCH kódnál kétszer annyi ellenőrző jegyre van szükség.

### Q kvázi-paritásellenőrző mátrix definiálása:

Q legyen  $(2q \times n)$  méretű.

Első  $q$  sora legyen ugyanaz, mint a Hamming-kódnál, vagyis az oszlopok éppen  $T^q$  nemnulla elemei.

Most tekintsük  $T^q$ -t  $2^q$  elemű testként. Ennek a testnek, és a  $T^q$  vektortérnek az additív szerkezete megegyezik, ezért a testet is jelölhetjük  $T^q$ -val. Legyen  $\alpha$  a  $(T^{q*}, \cdot)$  egyik generátoreleme.

$(T^{q*} = T^q - \{0\})$ .  $T^{q*}$  elemei tehát  $\alpha^i$  ( $0 \leq i \leq 2^q - 2$ ). Q felső felében ezek az elemek állnak. A Q alsó felében levő oszlopok a Q felső felében levő elemek köbei.

$$Q = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^j & \dots \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3j} & \dots \end{pmatrix}$$

Megmutatható, hogy a  $Q$  mátrix bármely legfeljebb 2 oszlopának összege más és más nemnulla vektor, így  $Q$  2-hibajavító BCH-kód kvázi-paritásellenőrző mátrixa.

$Q$  rangja éppen  $2q$ , s így  $Q$  a kód paritásellenőrző mátrixa.

### **Definíció.**

$t=2$  esetén legyen  $q \geq 3$ ,  $n=2^q-1$ ,  $k=2^q-2q-1$ .

$T^q$ -t  $2^q$ -elemű testnek tekintjük.  $\alpha$  a  $(T^q, \cdot)$  generátoreleme.  $T^q$  elemei  $\alpha^i$  ( $0 \leq i \leq 2^q-2$ ). Legyen  $Q$  a fenti mátrix.

Belátható, hogy ez a  $Q$  mátrix egy 2-hibajavító lineáris kódot definiál. Ezt a kódot *2-hibajavító BCH-kódnak* nevezzük.

## 17. példa. 2-hibajavító BCH-kód készítése.

Legyen  $q=4$ . A  $2^4=16$  elemű testben keressük a nemnulla elemek multiplikatív csoportjának egyik generáló elemét.

Az  $f=x^4+x+1$  polinom gyökei megfelelnek. Legyen  $\alpha$  az  $f$  gyöke.

A  $T^4$  vektortér egy bázisa  $1, \alpha, \alpha^2, \alpha^3$ , ezek lesznek most az egységvektorok. A többi hatvány koordinátáit a minimálpolinomból adódó  $\alpha^4 = \alpha + 1$  ismételt alkalmazásával kaphatjuk meg.

Az alábbi  $(8 \times 15)$ -ös paritásellenőrző mátrixhoz jutunk.

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

## **t-hibajavító BCH-kód.**

Legyen most  $n=2^q-1$ ,  $r \leq tq$ .

A kód  $Q$  kvázi-paritásellenőrző mátrixa  $t$  darab  $q \times n$  méretű blokkból áll.

A felső blokk oszlopai  $T^q$  nemnulla elemei.

Az  $i$ -edik blokk oszlopai a felső blokkbeli vektoroknak (mint a  $T^q$  test elemeinek)  $2^{i-1}$ -edik hatványai,  $i=2, 3, \dots, t$  (harmadik, ötödik, hetedik, stb. hatványok).

Ha  $Q$  sorai összefüggők, akkor kiválasztunk közülük egy maximális független rendszert, ezek alkotják kódunk  $H$  paritásellenőrző mátrixát.



## Definíció.

Legyen  $q$  rögzített pozitív egész, amelyre  $2^q - 1 > qt$ ,  $n = 2^q - 1$ .

$T^q$ -t  $2^q$ -elemű testnek tekintjük.  $\alpha$  a  $(T^q, \cdot)$  generátoreleme.

Legyen  $Q$  az a  $(tq \times n)$  méretű mátrix, amelynek a  $j+1$ -edik oszlopában egymás alatt rendre az alábbi  $t$  darab  $T^q$ -beli vektor áll:  $\alpha^j, \alpha^{3j}, \alpha^{5j}, \dots, \alpha^{(2t-1)j}$ .

$$Q = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^j & \dots \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3j} & \dots \\ 1 & \alpha^5 & \alpha^{10} & \dots & \alpha^{5j} & \dots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots \\ 1 & \alpha^{2t-1} & \alpha^{4t-2} & \dots & \alpha^{(2t-1)j} & \dots \end{pmatrix}$$

Belátható, hogy a  $Q$  ( $tq \times n$ ) méretű mátrix soraiból kiválasztva egy maximális összefüggő rendszert, a kapott  $H$  paritásellenőrző mátrix  $t$ -hibajavító lineáris kódot határoz meg. Az ellenőrző jegyek száma  $r \leq tq$ .

Ezt a kódot *t*-hibajavító BCH-kódnak nevezzük.

## Polinomkódok.

Legyen  $T=\mathbb{F}_2$ , és  $T_m[x]$  a  $T$  feletti legfeljebb  $m-1$ -edfokú polinomok vektortere a szokásos műveletekkel.

Ekkor az  $\alpha_0 \alpha_1 \dots \alpha_{m-1} \mapsto \alpha_0 + \alpha_1 x + \dots + \alpha_{m-1} x^{m-1}$

megfeleltetés izomorfizmus  $T^m$  és  $T_m[x]$  között.

Azonosítsuk a  $T^k$  és  $T^n$  vektortereket a belőlük a fenti izomorfizmussal létesített  $T_k[x]$ , illetve  $T_n[x]$  vektorterekkel.

## Definíció.

Legyen  $g \neq 0$  egy rögzített  $s$ -edfokú polinom  $T$  felett.

Legyen az  $A: T_k[x] \rightarrow T_n[x]$  leképezés a  $g$  polinommal történő szorzás, azaz  $A$  minden legfeljebb  $k-1$ -edfokú  $f$  polinomhoz a  $gf$  polinomot rendeli hozzá:  $Af=gf$ .

Az így definiált lineáris kódot *polinomkódnak*, a  $g$  polinomot pedig a kód *generáló polinomjának* nevezzük.

Ha  $\deg g < s$ , akkor minden kódszó végén  $s - \deg g$  darab nulla áll, ami semmire sem használható.

Csak a  $\deg g = s$  eset érdekes. Ekkor a kódszavak éppen  $g$  többszörösei (polinomszorosai).

## A Hamming-kód polinomkód.

Paritásellenőrző mátrixnak tekinthető az  $r$  sorból és  $n=2^r-1$  oszlopból álló  $H=(1 \ \alpha \ \alpha^2 \ \dots \ \alpha^{n-1})$  mátrix.

Legyen az

$$\underline{u} = \gamma_0 \gamma_1 \dots \gamma_{n-1} \in T^n$$

vektornak megfelelő polinom:

$$U = \gamma_0 + \gamma_1 x + \dots + \gamma_{n-1} x^{n-1} \in T_n[x]$$

Az  $\underline{u}$  vektor pontosan akkor kódszó, ha  $H\underline{u}=\underline{0}$ , azaz

$$\sum_{j=0}^{n-1} \gamma_j \alpha^j = 0$$

Az  $U$  polinomnak gyöke a  $\alpha$ , vagyis  $\underline{u}$  pontosan akkor kódszó, ha az  $\mathbb{F}_2$  feletti  $m_\alpha$  minimálpolinom osztója  $U$ -nak. Emiatt a Hamming-kód olyan polinomkód, amelynek a generáló polinomja  $g = m_\alpha$

## A BCH-kódok is polinomkódok

Tekintsük a 2-hibajavító BCH-kódot.

Az előzőekhez hasonlóan adódik, hogy  $\underline{u}$  pontosan akkor kódszó, ha  $m_\alpha$  és  $m_{\alpha^3}$  is osztója az  $U$  polinomnak, s így a generálópolinom  $\alpha$  és  $\alpha^3$  minimálpolinomjának a legkisebb közös többszöröse:

$$g = [m_\alpha, m_{\alpha^3}]$$

Hasonlóan kapjuk tetszőleges  $t$  esetre vonatkozólag:

Jelöljük  $\alpha^j$   $\mathbf{F}_2$  feletti minimálpolinomját  $m_j$ -vel. A  $t$ -hibajavító BCH-kód olyan polinomkód, amelynek a generáló polinomja

$$g_t = [m_1, m_2, \dots, m_{2t-1}]$$

A kódban az ellenőrzőjegyek száma éppen a  $g_t$  generáló polinom foka. Az  $s=2t$  pontosan akkor teljesül, ha  $\alpha, \alpha^3, \dots, \alpha^{2t-1}$  mindegyike  $q$ -adfokú  $\mathbf{F}_2$  felett és semelyik kettőnek sem ugyanaz a minimálpolinomja.

# Irodalomjegyzék

- ◆ G. Birkhoff-T. C. Barteo: *A modern algebra a számítógéptudományban* Műszaki Könyvkiadó, 1974
- ◆ Demetrovics, Denev, Pavlov: *A számítástudomány matematikai alapjai* Tankönyvkiadó, Budapest, 1985
- ◆ Freud Róbert: *Lineáris algebra* ELTE Eötvös Kiadó, Budapest, 1996
- ◆ Gonda János: *Bevezető fejezetek a matematikába III.* ELTE TTK, Bp. 1998
- ◆ Györfi László-Györi Sándor-Vajda István: *Információ és kódelmélet* Typotex Kiadó, 2000
- ◆ Jablonszkij, Lupanov: *Diszkrét matematika a számítástudományban* Műszaki Könyvkiadó, 1980
- ◆ Járai Antal: *Bevezetés a matematikába* Eötvös Kiadó, Budapest, 2005