

# Lineáris kódok

## Definíció.

Legyen  $S = \mathbb{F}_q$ . Ekkor  $S^n$  az  $\mathbb{F}_q$  test feletti vektortér.  $K$  *lineáris kód*, ha  $K$  az  $S^n$   $k$ -dimenziós altere.  $[n, k]_q$  vagy  $[n, k, d]_q$ .

## Jelölések:

$\underline{u} \in \mathbb{F}_q^n$  esetén  $\underline{u}$  oszlopvektor,  $\underline{u}^T$  sorvektor.  $W_q^{(n, k)}$  az  $n$  dimenziós tér  $k$ -dimenziós altere.

## 3. tétel.

Legyen  $K$   $[n, k, d]$  kód ( $k \geq 1$ ). Ekkor  $d(K) = w(K)$

## Bizonyítás.

◆ Legyen  $d = d(K)$ ,  $w = w(K)$ . Ekkor  $\exists \underline{u}, \underline{v} \in K$ , melyre  $d(\underline{u}, \underline{v}) = d$ .

A kód lineáris, így a két vektor különbsége is kódszó:

$$\underline{u} - \underline{v} = \underline{u}_1 \in K.$$

$w(\underline{u}_1) = d$ , így van  $d$  súlyú vektor  $K$ -ban, ezért  $w \leq d$ .

◆  $w = w(K)$  miatt  $\exists \underline{u} \in K$ :  $w(\underline{u}) = w$ ,  $d(\underline{u}, 0) = w$ , ezért  $d \leq w$ .

$\Rightarrow d = w$   
2007. május 31.



## Definíció.

$\underline{a}, \underline{b} \in \mathbf{F}_q^n$  skalár (belső) szorzata  $(\underline{a}, \underline{b}) = \underline{a}^T \underline{b} = \sum_{i=1}^n a_i \cdot b_i$

$\underline{a}$  és  $\underline{b}$  ortogonálisak, ha  $(\underline{a}, \underline{b})=0$ .

$\underline{a}$  önortogonális, ha  $(\underline{a}, \underline{a})=0$ .

$W_q^{(n,k)}$  ortogonális altere  $\mathbf{F}_q^n$  mindazon vektorainak a halmaza,  
melyek  $W_q^{(n,k)}$  minden vektorára merőlegesek:  $W_q^{(n,k)\perp}$

## 4. tétel.

◆  $W_q^{(n,k)\perp}$  az  $\mathbf{F}_q^n$   $(n-k)$ -dimenziós altere.

◆  $\left(W_q^{(n,k)\perp}\right)^\perp = W_q^{(n,k)}$

## Definíció.

Legyen  $W_q^{(n,k)}$   $[n,k]$  kód ( $n > k$ ). A kód *generátormátrixa* a

$W_q^{(n,k)}$  egy bázisának elemeiből, mint sorvektorokból álló  $G$  mátrix.

A kód (*paritás-ellenőrző mátrixa* a  $W_q^{(n,k)\perp}$  egy bázisának elemeiből, mint sorvektorokból álló  $H$  mátrix.

## Megjegyzés.

Egy kódnak általában több generátormátrixa és több paritásellenőrző mátrixa is lehet.

## 5. tétel.

Legyen az  $F_q$  fölötti  $[n,k]$  kód generátormátrixa  $G$ , ellenőrző mátrixa  $H$ .

1. Ekkor  $G$  ( $k \times n$ )-es,  $k$  rangú,  $H$  ( $(n-k) \times n$ )-es,  $n-k$  rangú  $F_q$  fölötti mátrix.
2.  $H \cdot G^T = 0$ .
3.  $\underline{v} \in \mathbf{F}_q^n$  akkor és csak akkor kódszó, ha  $H \cdot \underline{v} = 0$ .

## Bizonyítás.

1.  $G$  ( $k \times n$ )-es,  $k$  rangú,  $H$  ( $(n-k) \times n$ )-es,  $n-k$  rangú mátrix: Következménye a definíciónak.
2.  $H \cdot G^T = 0$ :

A szorzás során  $H$  egy-egy sorának a skalárszorzatát képezzük  $G$  egy-egy sorával. Minden skalárszorzat eredménye 0, mert  $H$  sorvektorai merőlegesek  $G$  minden egyes sorvektorára. A  $H \cdot G^T$  szorzat egy csupa 0-ból álló  $(n-k) \times k$  méretű mátrix.

3. Legyen  $\underline{v} \in \mathbf{F}_q^n$  kódszó. Ekkor merőleges H minden sorára, tehát  $H \cdot \underline{v}$  eredménye  $(n-k)$  elemű nullvektor.

Fordítva: Ha  $\underline{v} \in \mathbf{F}_q^n$  nem kódszó, akkor nem merőleges H minden sorára, s így a  $H \cdot \underline{v}$  szorzat eredménye sem nullvektor.



## Kódolás lineáris kóddal:

Legyen  $K$   $[n,k]_q$  kód. A kódszavak az  $n$  dimenziós tér  $k$  dimenziós alterének szavai, és az alter bármely bázisa alkalmas generátormátrix képzésére.

Közleményszavakhoz kódszavakat rendelünk:

egy rögzített  $G$  generátormátrixszal dolgozunk. A közleményszavak  $k$  hosszú vektorok, az  $\mathbf{F}_q^k$  elemei.

$\underline{u} \in \mathbf{F}_q^k$  egy lehetséges közleményszó és  $\underline{u}^T \cdot G = \underline{v}^T$ .

$\underline{v} \in \mathbf{F}_q^n$  vektor az  $\underline{u}$  kódja.

## A kódolás sémája:

közleményszavak  $\rightarrow$  kódszavak

$$\mathbf{F}_q^k \rightarrow \mathbf{F}_q^n$$

$$\underline{u} \in \mathbf{F}_q^k \quad \underline{u}^T \cdot G = \underline{v}^T \quad \underline{v} \in \mathbf{F}_q^n$$

$$\underline{u} \rightarrow \underline{v}$$

## 8. példa.

- ◆ Az 6. példa kétszeres ismétlés kódja lineáris kód, generátormátrixa  $G=(I_k \ I_k)$ . ( $I_k$   $k \times k$  méretű egységmátrix)
- ◆ A háromszoros ismétlés kódja szintén lineáris, generátormátrixa  $G=(I_k \ I_k \ I_k)$ .
- ◆ Hasonlóan lineáris a paritásellenőrző kód is, generátormátrixa  $G=(I_k \ I)$ . ( $I$  csupa 1-esből álló oszlopvektor.)

## 9. példa.

Az alábbi kódok esetében állapítsuk meg a minimális távolságot, a hibajelző, illetve hibajavító képességet, valamint azt, hogy melyik lineáris, a lineárisoknak pedig adjuk meg a generátormátrixát.

- a. Legyen  $k=3$ ,  $n=4$ , és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$(\alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_1, \alpha_2, \alpha_3, \alpha_1 + \alpha_2 + \alpha_3 + 1)$$

---

$d=2$ , mert ha az üzenetben egy jelet megváltoztatunk, a kódszóban két jel változik.

$d-1=1$  hibajelző és  $\left\lfloor \frac{d-1}{2} \right\rfloor = 0$  hibajavító.

A kód nem lineáris, mert például a  $\underline{0}$  vektor nem kódszó.



b. Legyen  $k=3$ ,  $n=5$ , és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$(\alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_1, \alpha_2, \alpha_3, \alpha_1, \alpha_2 + \alpha_3)$$

---

$d=2$ , mert ha az üzenetben egy jelet megváltoztatunk, a kódszóban két jelel változik.

→  $d-1=1$  hibajelző

$$\left\lfloor \frac{d-1}{2} \right\rfloor = 0 \text{ hibajavító.}$$

A kód lineáris

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

c.  $k=3$ ,  $n=5$ , és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$(\alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_1, \alpha_2, \alpha_3, \alpha_1, \max(\alpha_2, \alpha_3))$$

---

$d=1$ , mert van egymástól 1 távolságra lévő két kódszó.

Például  $(1\ 0\ 1\ 1\ 1)$  és  $(1\ 1\ 1\ 1\ 1)$ .

A kód  $d-1=0$  hibajelző és 0 hibajavító.

A kód nem lineáris, mert van két olyan kódszó, amelyek összege nem kódszó, s így az összeadás (valamint a kivonás is) kivezet a kódszavak halmazából.

Például  $\underline{u}_1^T = (1\ 1\ 0\ 1\ 1)$  és  $\underline{u}_2^T = (1\ 0\ 1\ 1\ 1)$  kódszavak, de  $\underline{u}_1^T + \underline{u}_2^T = (0\ 1\ 1\ 0\ 0)$  nem kódszó.

## 6. tétel.

Ha egy  $[n,k]$  kód generátormátrixa  $G = \begin{pmatrix} I_k & P \\ \hline & \end{pmatrix}$   
 $k \times n$                        $k \times (n-k)$

alakú, akkor a  $H = \begin{pmatrix} -P^T & I_{n-k} \\ \hline & \end{pmatrix}$  mátrix a kód ellenőrző mátrixa.  
 $(n-k) \times n$                        $(n-k) \times k$

(P tetszőleges mátrix .)

### Bizonyítás.

Elég belátnunk azt, hogy  $H \cdot G^T = 0$ . Blokkonkénti szorzással a következőt kapjuk:

$$\begin{pmatrix} -P^T & I_{n-k} \end{pmatrix} \cdot \begin{pmatrix} I_k \\ P^T \end{pmatrix} = -P^T + P^T = 0$$



### Megjegyzés.

Hasonlóan igaz az is, hogy ha egy  $[n,k]$  kód ellenőrző mátrixa  $H = \begin{pmatrix} I_{n-k} & R \\ \hline & \end{pmatrix}$  alakú, ahol R tetszőleges  $((n-k) \times k)$  méretű mátrix, akkor a  $G = \begin{pmatrix} -R^T & I_k \\ \hline & \end{pmatrix}$  mátrix megfelel generátormátrixnak. A kételemű test fölött  $-P$  helyett  $P$  is írható, mert  $F_2$ -ben  $1 = -1$ .

## 10. példa.

Adjuk meg a 9. példában szereplő lineáris kód ellenőrző mátrixát a

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

generátormátrix felhasználásával.

Az előző tételt alkalmazzuk.

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

## 7. tétel.

Egy  $[n,k,d]$  kód  $H$  ellenőrző mátrixában van  $d$  lineárisan összefüggő oszlop, de bármely  $d$ -nél kevesebb oszlop lineárisan független.

### Bizonyítás.

- ◆ Egy  $[n,k,d]$  kód  $H$  ellenőrző mátrixában van  $d$  lineárisan összefüggő oszlop: a következő módon lehet ilyet találni:  
 $d=d(K)=w(K)$  miatt  $\exists \underline{u} \in K: w(\underline{u})=d$ .  
 $\underline{u}$  –ban  $d$  helyen nem nulla érték áll, a többi helyen nulla.  
 $H \cdot \underline{u} = 0$ :  $H$  oszlopainak vesszük a lineáris kombinációit, és  $\underline{u}$  elemei az együtthatók.

A lineáris kombinációban pontosan  $d$  számú együttható különbözik nullától. A megfelelő  $d$  oszlop  $H$ -ban lineárisan összefüggő.

- ◆ H-ban bármely  $d$ -nél kevesebb oszlop lineárisan független:  
Legyen  $0 < d_1 < d$  és tegyük fel, hogy H-ban van  $d_1$  összefüggő oszlop. Így van H oszlopainak olyan lineáris kombinációja, amelyben ez a  $d_1$  oszlop nem mind nullával szorzódik, a többi együttható azonban mind nulla, s az eredmény a nullvektor.

Az együtthatókból készítsünk egy  $\underline{u}_1$  vektort.

Egyrészt  $H \cdot \underline{u}_1 = 0$ , emiatt  $\underline{u}_1$  kódvektor.

Másrészt  $w(\underline{u}_1) = d_1$ , így a kód súlya és ezzel együtt a távolsága kisebb lenne  $d$ -nél, ami ellentmondás. ↗

Beláttuk, hogy minden  $d$ -nél kevesebb oszlop lineárisan független H-ban.



## 11. példa.

Adjuk meg a 10. példában szereplő lineáris kód

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

ellenőrző mátrixának segítségével a kód távolságát és hibajelző, valamint hibajavító képességét.

---

Az ellenőrző mátrixban van két összefüggő oszlop (a 2. és a 3.), bármely oszlop önmagában lineárisan független (nem szerepel köztük a nullvektor),  
Így  $d=2$ , 1-hibajelző és 0-hibajavító a kód.

(Más megfontolással a 7.b példában ugyanezt kaptuk.)

## 8. tétel. (Singleton korlát)

$[n,k,d]$  kódban  $d \leq n-k+1$ .

### Bizonyítás.

$H$  rangja  $n-k$ , emiatt  $H$ -ban a független oszlopok száma  $\leq n-k$ .

Előző tétel szerint  $H$ -ban bármelyik  $d-1$  oszlop lineárisan független. Így

$$d-1 \leq n-k$$

$$d \leq n-k+1$$



### Definíció.

Az  $[n,k,d]$  kód *maximális távolságú*, ha  $d=n-k+1$ .

Jelölése: MDS kód. (S: szeparábilis).



## 13. példa.

Egy bináris kód generátormátrixa  $G$ . Adjuk meg a kód paritásellenőrző mátrixát és a távolságát.

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

Bázistranszformáció a sorvektorokon: ugyanannak az altérnek másik bázisát kapjuk, ugyanaz a mátrix lehet az ellenőrző mátrix. Az 1. sort adjuk a 2.-hoz.

$$G_1 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \quad \begin{matrix} 4-1-3-2 \text{ permutáció} \\ \\ \\ \end{matrix} \quad G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$
$$H_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

2-3-1-4 permutáció

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

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

A kód távolsága  $d=2$ , mert  $H$ -ban van két összefüggő oszlop (3. 7. ), de mindegyik oszlop önmagában független.