Diszkrét matematika 2.C szakirány

11. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2016. ősz

Lineáris kódok

Definíció

Legyen $\mathbb{F}$ véges test. Ekkor az $\mathbb{F}$ elemeiből képzett rendezett n-esek a komponensenkénti összeadással, valamint az n-es minden elemének ugyanazzal az $\mathbb{F}$-beli elemmel való szorzásával egy $\mathbb{F}$ feletti n-dimenziós $\mathbb{F}^n$ lineáris teret alkotnak. Ennek a térnek egy tetszőleges altere egy lineáris kód.

Megjegyzés

Itt $\mathbb{F}$ elemei a betűk, és $\mathbb{F}^n$ elemei a szavak, az altér elemei a kódszavak.

Lineáris kódok

Definíció

Legyen $V \neq \emptyset$ és $\mathbb{F}$ test $0 \in \mathbb{F}$ nullelemmel és $1 \in \mathbb{F}$ egységelemmel, továbbá $+ : V \times V \to V$ és $\cdot : \mathbb{F} \times V \to V$.
A V-t lineáris térnek nevezzük az $\mathbb{F}$ fölött, ha teljesülnek a következők:

1. $\forall \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in V : \mathbf{v}_1 + (\mathbf{v}_2 + \mathbf{v}_3) = (\mathbf{v}_1 + \mathbf{v}_2) + \mathbf{v}_3$;
2. $\forall \mathbf{v}_1, \mathbf{v}_2 \in V : \mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_2 + \mathbf{v}_1$;
3. $\exists \mathbf{0} \in V : \forall \mathbf{v} \in V : \mathbf{v} + \mathbf{0} = \mathbf{v}$;
4. $\forall \mathbf{v} \in V : \exists \mathbf{v'} \in V : \mathbf{v} + \mathbf{v'} = \mathbf{0}$;
5. $\forall \lambda \in \mathbb{F}, \mathbf{v}_1, \mathbf{v}_2 \in V : \lambda(\mathbf{v}_1 + \mathbf{v}_2) = \lambda \mathbf{v}_1 + \lambda \mathbf{v}_2$;
6. $\forall \lambda, \mu \in \mathbb{F}, \mathbf{v} \in V : (\lambda + \mu)\mathbf{v} = \lambda \mathbf{v} + \mu \mathbf{v}$;
7. $\forall \lambda, \mu \in \mathbb{F}, \mathbf{v} \in V : \lambda(\mu \mathbf{v}) = (\lambda \mu)\mathbf{v}$;
8. $\forall \mathbf{v} \in V : 1\mathbf{v} = \mathbf{v}$.

Lineáris kódok

$$\begin{aligned}
&\mathbf{a}+(\mathbf{b}+\mathbf{c}) = \\
&= (a_1, a_2, \ldots, a_n) + ((b_1, b_2, \ldots, b_n) + (c_1, c_2, \ldots, c_n)) = \\
&= (a_1, a_2, \ldots, a_n) + (b_1 + c_1, b_2 + c_2, \ldots, b_n + c_n) = \\
&= (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), \ldots, a_n + (b_n + c_n)) = \\
&= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2, \ldots, (a_n + b_n) + c_n) = \\
&= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) + (c_1, c_2, \ldots, c_n) = \\
&= ((a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)) + (c_1, c_2, \ldots, c_n) = \\
&(\mathbf{a}+\mathbf{b})+\mathbf{c}
\end{aligned}$$

$$\begin{aligned}
&\mathbf{a}+\mathbf{b} = \\
&= (a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = \\
&= (b_1 + a_1, b_2 + a_2, \ldots, b_n + a_n) = (b_1, b_2, \ldots, b_n) + (a_1, a_2, \ldots, a_n) = \\
&= \mathbf{b}+\mathbf{a}
\end{aligned}$$

$$\begin{aligned}
&\mathbf{a}+\mathbf{0} = (a_1, a_2, \ldots, a_n) + (0, 0, \ldots, 0) = (a_1 + 0, a_2 + 0, \ldots, a_n + 0) = \\
&= (a_1, a_2, \ldots, a_n) = \mathbf{a}
\end{aligned}$$

$$\begin{aligned}
&(a_1, a_2, \ldots, a_n) + (-a_1, -a_2, \ldots, -a_n) = (a_1 - a_1, a_2 - a_2, \ldots, a_n - a_n) = \\
&= (0, 0, \ldots, 0) = \mathbf{0}
\end{aligned}$$

Lineáris kódok

$$d(\mathbf{a}+\mathbf{b}) = d((a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n)) =$$
$$= d(a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) =$$
$$= (d(a_1 + b_1), d(a_2 + b_2), \dots, d(a_n + b_n)) =$$
$$= (da_1 + db_1, da_2 + db_2, \dots, da_n + db_n) =$$
$$= (da_1, da_2, \dots, da_n) + (db_1, db_2, \dots, db_n) =$$
$$= d(a_1, a_2, \dots, a_n) + d(b_1, b_2, \dots, b_n) = d\mathbf{a} + d\mathbf{b}$$

$$(d+e)\mathbf{a} = (d+e)(a_1, a_2, \dots, a_n) =$$
$$= ((d+e)a_1, (d+e)a_2, \dots, (d+e)a_n) =$$
$$= (da_1 + ea_1, da_2 + ea_2, \dots, da_n + ea_n) =$$
$$= (da_1, da_2, \dots, da_n) + (ea_1, ea_2, \dots, ea_n) =$$
$$= d(a_1, a_2, \dots, a_n) + e(a_1, a_2, \dots, a_n) = d\mathbf{a} + e\mathbf{a}$$

$$d(e\mathbf{a}) = d(e(a_1, a_2, \dots, a_n)) = d(ea_1, ea_2, \dots, ea_n) =$$
$$= (d(ea_1), d(ea_2), \dots, d(ea_n)) = ((de)a_1, (de)a_2, \dots, (de)a_n) =$$
$$= (de)(a_1, a_2, \dots, a_n) = (de)\mathbf{a}$$

$$1\mathbf{a} = 1(a_1, a_2, \dots, a_n) = (1a_1, 1a_2, \dots, 1a_n) = (a_1, a_2, \dots, a_n) = \mathbf{a}$$

Lineáris kódok

Jelölés

$m \in \mathbb{N}$, $d \in \mathbb{F}$ és $\mathbf{a} \in \mathbb{F}^n$ esetén legyen $md = \underbrace{d + d + \ldots + d}_{m \text{ db}}$, illetve $m\mathbf{a} = \underbrace{\mathbf{a} + \mathbf{a} + \ldots + \mathbf{a}}_{m \text{ db}}$.

Lemma

$m \in \mathbb{N}$ és $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ esetén $m\mathbf{a} = (ma_1, ma_2, \ldots, ma_n)$.

Bizonyítás

TI.: $m = 0$, illetve $m = 1$ esetén az állítás nyilvánvaló.
Tfh. $m = k$-ra igaz az összefüggés. Ekkor $m = k + 1$-re:

$$(k+1)\mathbf{a} = \underbrace{\mathbf{a} + \mathbf{a} + \ldots + \mathbf{a}}_{k+1 \text{ db}} = \underbrace{\mathbf{a} + \mathbf{a} + \ldots + \mathbf{a}}_{k \text{ db}} + \mathbf{a} = k\mathbf{a} + \mathbf{a} =$$
$$= (ka_1, ka_2, \ldots, ka_n) + (a_1, a_2, \ldots, a_n) =$$
$$= (ka_1 + a_1, ka_2 + a_2, \ldots, ka_n + a_n) = ((k+1)a_1, (k+1)a_2, \ldots, (k+1)a_n)$$

Lineáris kódok

Megjegyzés

Legyen $p = char(\mathbb{F}) \in \mathbb{N}$. Ekkor bármely $d \in \mathbb{F}$-re $pd = 0$, így minden $\mathbf{a} \in \mathbb{F}^n$ esetén $p\mathbf{a} = (pa_1, pa_2, \ldots, pa_n) = (0, 0, \ldots, 0) = \mathbf{0}$.

Állítás

Legyen $K \subset \mathbb{F}^n$. Ha minden $k_1, k_2 \in K$, $f \in \mathbb{F}$ esetén $k_1 + k_2 \in K$ és $fk_1 \in K$, akkor a kód lineáris.

Bizonyítás

A feltétel biztosítja, hogy $+|_K : K \times K \to K$ és $\cdot|_K : \mathbb{F} \times K \to K$.
Legyen $p = char(\mathbb{F}) \in \mathbb{N}$.

$$\mathbf{0} = p\mathbf{a} = \underbrace{\mathbf{a} + \mathbf{a} + \ldots + \mathbf{a}}_{p \text{ db}} = \mathbf{a} + \underbrace{\mathbf{a} + \mathbf{a} + \ldots + \mathbf{a}}_{p-1 \text{ db}} = \mathbf{a} + (p-1)\mathbf{a}$$

Lineáris kódok

Definíció

Legyen $\mathbb{F}$ véges test. Ekkor az $\mathbb{F}$ elemeiből képzett rendezett n-esek a komponensenkénti összeadással, valamint az n-es minden elemének ugyanazzal az $\mathbb{F}$-beli elemmel való szorzásával egy $\mathbb{F}$ feletti n-dimenziós $\mathbb{F}^n$ lineáris teret alkotnak. Ennek a térnek egy tetszőleges altere egy lineáris kód.

Megjegyzés

Itt $\mathbb{F}$ elemei a betűk, és $\mathbb{F}^n$ elemei a szavak, az altér elemei a kódszavak.

Jelölés

Ha az altér k-dimenziós, a kód távolsága d, a test elemeinek a száma pedig q, akkor $[n, k, d]_q$ kódról beszélünk.
Ha nem lényeges d és q értéke, akkor elhagyjuk őket a jelölésből, és $[n, k]$-t írunk.

Lineáris kódok

Megjegyzés

Egy $[n, k, d]_q$ kód esetén a Singleton-korlát alakja egyszerűsödik:

$$q^k \leq q^{n-d+1} \iff k \leq n - d + 1.$$

Példa

1) A (*) kód egy $[5, 2, 3]_2$ kód:
(0,0)$\mapsto$ (0,0,0,0,0)
(0,1)$\mapsto$ (0,1,1,1,0)
(1,0)$\mapsto$ (1,0,1,0,1)
(1,1)$\mapsto$ (1,1,0,1,1)

Lineáris kódok

Példa folyt.

2) $\mathbb{F}_q$ felett az ismétléses kód:
pl. a háromszori ismétlés kódja: $a \mapsto (a, a, a)$.
Ez egy $[3, 1, 3]_q$ kód.

3) Paritásbites kód (ha páros sok egyesre egészítünk ki):
$(b_1, b_2, \dots, b_k) \mapsto (b_1, b_2, \dots, b_k, \sum_{j=1}^k b_j)$.
Ez egy $[n, n-1, 2]_2$ kód.

Definíció

Az $\mathbb{F}$ ábécé feletti n hosszú $u \in \mathbb{F}^n$ szó súlya alatt a nem-nulla koordinátáinak a számát értjük, és $w(u)$-val jelöljük.
Egy K kód súlya a nem-nulla kódszavak súlyainak a minimuma:

$$w(K) = \min_{u \neq 0} w(u).$$

Lineáris kódok

Megjegyzés

Egy szó súlya megegyezik a 0-tól vett távolságával:
$w(u) = d(u, (0, 0, \ldots, 0))$.

Állítás

Ha K lineáris kód, akkor $d(K) = w(K)$.

Bizonyítás

$d(u, v) = w(u - v)$, és mivel K linearitása miatt $u, v \in K$ esetén $u - v \in K$, ezért a minimumok is megegyeznek (Miért?).

Lineáris kódok

Lineáris kód esetén a kódolás elvégezhető mátrixszorzással.

Definíció

Legyen $G : \mathbb{F}_q^k \to \mathbb{F}_q^n$ egy teljes rangú lineáris leképzés, illetve $\mathbf{G} \in \mathbb{F}_q^{n\times k}$ a hozzá tartozó mátrix. $K = \mathrm{Im}(G)$ esetén $\mathbf{G}$-t a K kód **generátormátrixának** nevezzük.

$$\begin{array}{cc} & \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} \\ \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nk} \end{pmatrix} & \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \end{array}$$

Lineáris kódok

Példa

1) A (*) kód egy generátormátrixa:

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

2) A háromszori ismétlés kódjának egy generátormátrixa:

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

Lineáris kódok

Példa folyt.

3) A paritásbites kód egy generátormátrixa:

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

Lineáris kódok

Definíció

Egy $[n, k, d]_q$ kódnak $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ mátrix az ellenőrző mátrixa, ha $\mathbf{H}v = 0 \iff v$ kódszó.

Megjegyzés

A $\mathbf{G}$ mátrixhoz tartozó kódolásnak $\mathbf{H}$ pontosan akkor ellenőrző mátrixa, ha $\mathrm{Ker}(\mathbf{H}) = \mathrm{Im}(\mathbf{G})$

Példa

1) A (*) kód egy ellenőrző mátrixa:

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

Lineáris kódok

Példa folyt.

2) A háromszori ismétlés kódjának egy ellenőrző mátrixa:

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

3) A paritásbites kód egy ellenőrző mátrixa:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}$$

Lineáris kódok

Definíció

Ha a kódszavak első k betűje megfelel az eredeti kódolandó szónak, akkor szisztematikus kódolásról beszélünk.
Ekkor az első k karakter az üzenetszegmens, az utolsó $n-k$ pedig a paritásszegmens.

Példa

1) A háromszori ismétlés kódja:

$$(\underbrace{a}_{\text{üz.sz.}}, \underbrace{a, a}_{\text{par.sz.}})$$

2) A paritásbites kód:

$$(\underbrace{b_1, b_2, \ldots, b_{n-1}}_{\text{üz.sz.}}, \underbrace{\sum_{j=1}^{n-1} b_j}_{\text{par.sz.}})$$

Lineáris kódok

Megjegyzés

Szisztematikus kódolás esetén könnyen tudunk dekódolni: a paritásszegmens elhagyásával megkapjuk a kódolandó szót.

Megjegyzés

Egy szisztematikus kód generátormátrixa speciális alakú:

$$\mathbf{G} = \begin{pmatrix} \mathbf{I}_k \\ \mathbf{P} \end{pmatrix},$$

ahol $\mathbf{I}_k \in \mathbb{F}_q^{k \times k}$ az egységmátrix, továbbá $\mathbf{P} \in \mathbb{F}_q^{(n-k) \times k}$.

Lineáris kódok

Állítás

Legyen $\mathbf{G} \in \mathbb{F}_q^{n\times k}$ egy szisztematikus kód generátormátrixa:
$\mathbf{G} = \begin{pmatrix} \mathbf{I}_k \\ \mathbf{P} \end{pmatrix}$. Ekkor $\mathbf{H} = \begin{pmatrix} -\mathbf{P} & \mathbf{I}_{n-k} \end{pmatrix}$ ellenőrző mátrixa a kódnak.

Bizonyítás

$$\mathbf{H} \cdot \mathbf{G} = \begin{pmatrix} -\mathbf{P} & \mathbf{I}_{n-k} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{I}_k \\ \mathbf{P} \end{pmatrix} = -\mathbf{P} + \mathbf{P} = \mathbf{0} \in \mathbb{F}_q^{(n-k)\times k}$$

$(\mathbf{H} \cdot \mathbf{G})_{ij} = \sum_{l=1}^{k} (-\mathbf{P})_{il} \cdot (\mathbf{I}_k)_{lj} + \sum_{l=1}^{n-k} (\mathbf{I}_{n-k})_{il} \cdot (\mathbf{P})_{lj} = -p_{ij} + p_{ij} = 0$.
Tehát bármely u kódolandó szóra $\mathbf{H}(\mathbf{G}u) = (\mathbf{HG})u = \mathbf{0}u = \underline{0}$,
vagyis $\mathrm{Im}(\mathbf{G}) \subset \mathrm{Ker}(\mathbf{H})$, amiből $\dim(\mathrm{Im}(\mathbf{G})) \leq \dim(\mathrm{Ker}(\mathbf{H}))$.
$\dim(\mathrm{Im}(\mathbf{G})) = k$ és $\dim(\mathrm{Ker}(\mathbf{H})) \leq k$ miatt viszont
$\dim(\mathrm{Im}(\mathbf{G})) \geq \dim(\mathrm{Ker}(\mathbf{H}))$ is teljesül, így $\mathrm{Im}(\mathbf{G}) = \mathrm{Ker}(\mathbf{H})$.

Példa

Ld. korábban.

Lineáris kódok

A kód távolsága leolvasható az ellenőrző mátrixból.

Állítás

Legyen $\mathbf{H}$ egy $[n, k]$ kód ellenőrző mátrixa. A $\mathbf{H}$-nak pontosan akkor van l darab lineárisan összefüggő oszlopa, ha van olyan kódszó, aminek a súlya legfeljebb l.

Bizonyítás

Legyen $\mathbf{H} = \begin{pmatrix} \underline{h_1} & \underline{h_2} & \cdots & \underline{h_n} \end{pmatrix}$.

$\Longrightarrow$

Ekkor $\sum_{j=1}^{l} u_j \cdot \underline{h_{l_j}} = \underline{0}$. Tekintsük azt a vektort, aminek az l_j-edik koordinátája u_j, a többi pedig 0. Ez egyrészt kódszó lesz (Miért?), másrészt a súlya legfeljebb l.

$\Longleftarrow$

Legyen $\underline{u} = (u_1, u_2, \ldots, u_n)^T$ az a kódszó, aminek a súlya l. Ekkor $\mathbf{H}$-nak az $\underline{u}$ nem-nulla koordinátáinak megfelelő oszlopai lineárisan összefüggőek.

Lineáris kódok

Következmény

A kód távolsága a legkisebb pozitív egész l, amire létezik az ellenőrző mátrixnak l darab lineárisan összefüggő oszlopa.

Példa

A (*) kód esetén:

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

Egyik oszlopvektor sem a nullvektor, így nincs 1 darab lineárisan összefüggő oszlop.
Egyik oszlopvektor sem többszöröse egy másiknak, így nincs 2 darab lineárisan összefüggő oszlop.
Az 1., 3. és 5. oszlopok lineárisan összefüggőek, így a kód távolsága 3.

Lineáris kódok

A $\mathbf{H}$ ellenőrző mátrix segítségével dekódolni is lehet.

Definíció

Adott $\underline{v} \in \mathbb{F}_q^n$ esetén az $\underline{s} = \mathbf{H}\underline{v} \in \mathbb{F}_q^{n-k}$ vektort szindrómának nevezzük.

Megjegyzés

A $\underline{v}$ pontosan akkor kódszó, ha $\underline{s} = \underline{0}$.

Definíció

Legyen $\underline{c}$ a kódszó, $\underline{v}$ a vett szó. Az $\underline{e} = \underline{v} - \underline{c}$ a hibavektor.

Állítás

$\mathbf{H}\underline{v} = \mathbf{H}\underline{e}$.

Bizonyítás

$\mathbf{H}\underline{v} = \mathbf{H}(\underline{c} + \underline{e}) = \mathbf{H}\underline{c} + \mathbf{H}\underline{e} = \underline{0} + \mathbf{H}\underline{e} = \mathbf{H}\underline{e}$

Lineáris kódok

A dekódolás elve: $\underline{v}$-ből kiszámítjuk a $\mathbf{H}\underline{v}$ szindrómát, ami alapján megbecsüljük az $\underline{e}$ hibavektort, majd meghatározzuk $\underline{c}$-t a $\underline{c} = \underline{v} - \underline{e}$ képlet segítségével.

Definíció

Valamely $\underline{e}$ hibavektorhoz tartozó mellékosztály az $\{\underline{e} + \underline{c} : c \text{ kódszó}\}$ halmaz.

Megjegyzés

Az $\underline{e} = \underline{0}$-hoz tartozó mellékosztály a kód.

Állítás

Az azonos mellékosztályban lévő szavak szindrómája megegyezik.

Lineáris kódok

Definíció

Minden $\underline{s}$ szindróma esetén legyen $\underline{e_s}$ az a minimális súlyú szó, melynek $\underline{s}$ a szindrómája. Ez az $\underline{s}$ szindrómához tartozó mellékosztály-vezető, a mellékosztály elemei $\underline{e_s} + \underline{c}$ alakúak, ahol $\underline{c} \in K$ kódszó.

Szindrómadekódolás

Adott $\underline{v}$ esetén tekintsük az $\underline{s} = \mathbf{H}\underline{v}$ szindrómát, és az $\underline{e_s}$ mellékosztály-vezetőt. Dekódoljuk $\underline{v}$-t $\underline{c} = \underline{v} - \underline{e_s}$-nek.

Állítás

Legyen $\underline{c}$ a kódszó, $\underline{v} = \underline{c} + \underline{e}$ a vett szó, ahol $\underline{e}$ a hiba, és $w(\underline{e}) < d/2$, ahol d a kód távolsága. Ekkor a szindrómadekódolás a minimális távolságú dekódolásnak felel meg.

Lineáris kódok

Bizonyítás

Egyrészt a korábbi állítás alapján $\underline{s} = \mathbf{H}\underline{v} = \mathbf{H}\underline{e}$, másrészt $\underline{e_s}$ definíciója miatt $\underline{s} = \mathbf{H}\underline{e_s}$. Ezért $\underline{e}$ és $\underline{e_s}$ ugyanabban a mellékosztályban van, továbbá $w(\underline{e_s}) \leq w(\underline{e})$.
$w(\underline{e} - \underline{e_s}) = d(\underline{e}, \underline{e_s}) \leq d(\underline{e}, \underline{0}) + d(\underline{0}, \underline{e_s}) = w(\underline{e}) + w(\underline{e_s}) < d$.
De $\mathbf{H}(\underline{e} - \underline{e_s}) = \underline{0}$ miatt $\underline{e} - \underline{e_s}$ kódszó (Miért?), így $\underline{e} = \underline{e_s}$.

Példa

Tekintsük a (*) kódot.
$\underline{v} = (1, 1, 0, 1, 1)^T$ esetén $\mathbf{H}\underline{v} = \underline{0}$, így $\underline{v}$ kódszó.
$\underline{v} = (1, 1, 0, 0, 1)^T$ esetén $\mathbf{H}\underline{v} = (0, 1, 0)^T = \underline{s}$.
Mi az $\underline{s}$-hez tartozó mellékosztály-vezető?
A $(0, 0, 0, 1, 0)^T$ súlya 1, és a szindrómája a keresett $(0, 1, 0)^T$, így ez lesz a mellékosztály-vezető.
$\underline{c} = \underline{v} - \underline{e_s} = (1, 1, 0, 0, 1)^T - (0, 0, 0, 1, 0)^T = (1, 1, 0, 1, 1)^T$

Lineáris kódok

Emlékeztető (Hamming-korlát)

Ha $K \subset A^n$, $|A| = q$ és K t-hibajavító, akkor

$$|K| \sum_{j=0}^{t} \binom{n}{j} (q-1)^j \leq q^n.$$

Egyenlőség esetén perfekt kódról beszélünk.

Definíció

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

Emlékeztető

A kód távolsága a legkisebb pozitív egész l, amire létezik az ellenőrző mátrixnak l darab lineárisan összefüggő oszlopa.

Lineáris kódok

Ha egy olyan bináris kódot készítünk, amelyre a $\mathbf{H}$ ellenőrző mátrix oszlopainak a különböző r hosszú vektorokat választjuk, akkor egy 1-hibajavító kódot kapunk (Miért?).
Ekkor a Hamming-korlát alakja:
$2^k(1+n) \leq 2^n$.
Egyenlőség esetén $n = 2^{n-k} - 1$, és pont ennyi $n-k$ hosszú vektor van.

$n = 2^r - 1$ esetén $k = n - \log(n+1)$, így a megfelelő (n, k) párok:

n	3	7	15	31	63	127	$\cdots$
k	1	4	11	26	57	120	$\cdots$

Dekódolás Hamming-kód esetén:
Ha csak 1 hiba van, akkor a hibavektornak csak egy koordinátája 1, a többi 0, így a szindróma az ellenőrző mátrix valamely oszlopa lesz. Ennek az oszlopnak megfelelő koordinátája hibás az üzenetben.

Lineáris kódok

Példa

$n = 7$, $k = 4$

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

és

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

$v = (1, 1, 0, 0, 1, 1, 1)^T$ esetén $\mathbf{H}v = (0, 1, 1)^T = s$, ami a $\mathbf{H}$ 2. oszlopa, így a 2. koordináta romlott el, vagyis a küldött kódszó $c = (1, 0, 0, 0, 1, 1, 1)^T$.

Lineáris kódok

Megjegyzés

A $[7,4]$-es Hamming-kódot egy paritásbittel kiegészítve kapjuk a teletextnél használt kódolást.
A $[15,11]$-es Hamming-kódot egy paritásbittel kiegészítve a műholdas műsorszórásnál (DBS) használják.

Definíció

A $K \subset \mathbb{F}_q^n$ kód ciklikus, ha minden $(u_1, u_2, \ldots, u_{n-1}, u_n) \in K$ esetén $(u_2, u_3, \ldots, u_n, u_1) \in K$.

Példa

$K = \{000, 101, 110, 011, 111\}$ bináris kód ciklikus.

Megjegyzés

Ez nem lineáris kód: $101 + 111 = 010 \notin K$.