Diszkrét matematika II.
9. előadás

Fancsali Szabolcs Levente
nudniq@inf.elte.hu

ELTE IK Komputeralgebra Tanszék

Mérai László diái alapján

Hibakorlátozó kódolás

Példa (ISBN (International Standard Book Number) kódolása)

Legyen $d_1, d_2, \ldots, d_n$ decimális számjegyek egy sorozata ($n \leq 10$). Egészítsük ki a sorozatot egy $n+1$-edik számjeggyel, amelynek értéke

$$d_{n+1} = \sum_{j=1}^{n} j \cdot d_j \mod 11,$$

ha az nem 10, különben d_{n+1} legyen X.
Ha valamelyik számjegyet elírjuk, akkor az összefüggés nem teljesülhet: d_{n+1} elírása esetén ez nyilvánvaló, $j \leq n$-re d_j helyett d'_j-t írva pedig az összeg $j(d'_j - d_j)$-vel nőtt, ami nem lehet 11-gyel osztható (Miért?).
Azt is észrevesszük, ha $j < n$ esetén d_j-t és d_{j+1}-et felcseréljük:
az összeg $jd_{j+1} + (j+1)d_j - jd_j - (j+1)d_{j+1} = d_j - d_{j+1}$-gyel nő, ami csak akkor lehet 11-gyel osztható, ha $d_j = d_{j+1}$.

Megjegyzés

2007 óta 13 jegyű.
A személyi számnál is használják.

Hibakorlátozó kódolás

Példa (Paritásbites kód)

Egy n hosszú 0-1 sorozatot egészítsünk ki egy $n+1$-edik bittel, ami legyen 1, ha a sorozatban páratlan sok 1-es van, különben pedig legyen 0. Ha egy bit megváltozik, akkor észleljük a hibát.

Példa (Kétdimenziós paritásellenőrzés)

$$\begin{array}{ccccc|c} b_{0,0} & \cdots & b_{0,j} & \cdots & b_{0,n-1} & b_{0,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ b_{i,0} & \cdots & b_{i,j} & \cdots & b_{i,n-1} & b_{i,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ b_{m-1,0} & \cdots & b_{m-1,j} & \cdots & b_{m-1,n-1} & b_{m-1,n} \\ \hline b_{m,0} & \cdots & b_{m,j} & \cdots & b_{m,n-1} & b_{m,n} \end{array}$$

Oszlopok és sorok végén paritásbit. Ha megváltozik egy bit, akkor a sor és az oszlop végén jelez az ellenőrző bit, ez alapján tudjuk javítani a hibát. Ha két bit változik meg, akkor észleljük a hibát, de nem tudjuk javítani.

Hibakorlátozó kódolás

Definíció

Egy kód t-hibajelző, ha minden olyan esetben jelez, ha az elküldött és megkapott szó legfeljebb t helyen tér el.
Egy kód pontosan t-hibajelző, ha t-hibajelző, de van olyan $t+1$-hiba, amit nem jelez.

Példa

- ISBN - 1-hibajelző
- paritásbites kód - 1-hibajelző
- kétdimenziós paritásellenőrzés - 2-hibajelző

Hiba javításának módjai

ARQ (Automatic Retransmission Request) - újraküldés,
FEC (Forward Error Correction) - javítható, pl.: kétdimenziós paritásell.

Hibakorlátozó kódolás

Definíció

Legyen A véges ábécé, továbbá $u, v \in A^n$. Ekkor u és v Hamming-távolsága alatt az azonos pozícióban lévő különböző betűk számát értjük:

$$d(u, v) = |\{i : 1 \leq i \leq n \wedge u_i \neq v_i\}|.$$

Példa

0	1	1	1	0
1	0	1	0	1
$\neq$	$\neq$	$=$	$\neq$	$\neq$

$d(01110,10101)=4$

A	L	M	A
A	N	N	A
$=$	$\neq$	$\neq$	$=$

$d(ALMA,ANNA)=2$

Hibakorlátozó kódolás

Állítás

A Hamming-távolság rendelkezik a távolság szokásos tulajdonságaival, vagyis tetszőleges u, v, w-re

1) $d(u, v) \geq 0$;
2) $d(u, v) = 0 \iff u = v$;
3) $d(u, v) = d(v, u)$ (szimmetria);
4) $d(u, v) \leq d(u, w) + d(w, v)$ (háromszög-egyenlőtlenség).

Bizonyítás

1), 2) és 3) nyilvánvaló.
4) Ha u és v eltér valamelyik pozicióban, akkor ott u és w, illetve w és v közül legalább az egyik pár különbözik.

Hibakorlátozó kódolás

Definíció

A K kód távolsága ($d(K)$) a különböző kódszópárok távolságainak a minimuma.

Példa (*)

$$\left.\begin{array}{l}(0,0)\mapsto (0,0,0,0,0)\\ (0,1)\mapsto (0,1,1,1,0)\\ (1,0)\mapsto (1,0,1,0,1)\\ (1,1)\mapsto (1,1,0,1,1)\end{array}\right\rceil \begin{array}{l}3\\4\\3\end{array}\Bigg\rceil 3\Bigg\rceil 3\Bigg\rceil 4$$

A kód távolsága 3.

Felmerül a kérdés, hogy vajon mi lehetett a kódszó, ha a (0,1,0,0,0) szót kapjuk.

Hibakorlátozó kódolás

Definíció

Minimális távolságú dekódolás esetén egy adott szóhoz azt a kódszót rendeljük, amelyik hozzá a legközelebb van. Több ilyen szó esetén kiválasztunk ezek közül egyet, és az adott szóhoz mindig azt rendeljük.

Megjegyzés

A dekódolás két részre bontható: a hibajavításnál megpróbáljuk meghatározni, hogy mi volt az elküldött kódszó, majd visszaállítjuk az üzenetet. Mivel az utóbbi egyértelmű, ezért hibajavító kódok dekódolásán legtöbbször csak a hibajavítást értjük.

Definíció

Egy kód t-hibajavító, ha minden olyan esetben helyesen javít, amikor egy elküldött szó legfeljebb t helyen változik meg.
Egy kód pontosan t-hibajavító, ha t-hibajavító, de van olyan $t+1$ hibával érkező szó, amit helytelenül javít, vagy nem javít.

Hibakorlátozó kódolás

Megjegyzés

Ha a kód távolsága d, akkor minimális távolságú dekódolással $t < \frac{d}{2}$ esetén t-hibajavító.

Példa

Az előző példában szereplő kód pontosan 1-hibajavító.
$(0,0,0,0,0) \rightsquigarrow (1,0,0,0,1) \rightarrow (1,0,1,0,1)$

Példa (ismétléses kód)

$a \mapsto (a,a,a) \quad d = 3 \quad 1$-hibajavító,
$a \mapsto (a,a,a,a,a) \quad d = 5 \quad 2$-hibajavító.

Hibakorlátozó kódolás

Tétel (Singleton-korlát)

Ha $K \subset A^n$, $|A| = q$ és $d(K) = d$, akkor $|K| \leq q^{n-d+1}$.

Bizonyítás

Ha minden kódszóból elhagyunk $d-1$ betűt (ugyanazokból a pozíciókból), akkor az így kapott szavak még mindig különbözőek, és $n-d+1$ hosszúak. Az ilyen hosszú szavak száma szerepel az egyenlőtlenség jobb oldalán.

Definíció

Ha egy kódra a Singleton-korlát egyenlőséggel teljesül, akkor azt maximális távolságú szeparábilis kódnak (MDS-kód) nevezzük.

Példa

Az n-szeri ismétlés kódja. Ekkor $d = n$, és $|K| = q$.

Hibakorlátozó kódolás

Tétel (Hamming-korlát)

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

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

Bizonyítás

Mivel a kód t-hibajavító, ezért bármely két kódszóra a tőlük legfeljebb t távolságra lévő szavak halmazai diszjunktak (Miért?). Egy kódszótól pontosan j távolságra lévő szavak száma $\binom{n}{j}(q-1)^j$ (Miért?), így egy kódszótól legfeljebb t távolságra lévő szavak száma $\sum_{j=0}^{t} \binom{n}{j}(q-1)^j$. A jobb oldalon az n hosszú szavak száma szerepel (Miért?).

Hibakorlátozó kódolás

Definíció

Ha egy kódra a Hamming-korlát egyenlőséggel teljesül, akkor azt perfekt kódnak nevezzük.

Példa (nem perfekt kódra)

A (*) kód esetén $|K| = 4$, $n = 5$, $q = 2$ és $t = 1$.
B.O.$= 4\left(\binom{5}{0}(2-1)^0 + \binom{5}{1}(2-1)^1\right) = 4(1+5) = 24$,
J.O.$= 2^5 = 32$.
Nem perfekt kód.

A kód távolságának és hibajelző képességének kapcsolata

Tekintsünk egy kódot, aminek a távolsága d.

Ha egy elküldött kódszó legalább 1, de d-nél kevesebb helyen sérül, akkor az így kapott szó biztosan nem kódszó, mivel két kódszó legalább d helyen különbözik. Tehát legfeljebb $d-1$ hiba esetén a kód jelez.

A kódban van két olyan kódszó, amelyek távolsága d, és ha az egyiket küldik, és ez úgy változik meg, hogy éppen a másik érkezik meg, akkor d hiba történt, de nem vesszük észre. Tehát van olyan d hiba, amit a kód nem tud jelezni.
Ezáltal a kód pontosan $d-1$-hibajelző.

A kód távolságának és hibajavító képességének kapcsolata

Legyen a kód távolsága továbbra is d, és tegyük fel, hogy minimális távolságú dekódolást használunk.

$t < \frac{d}{2}$ hiba esetén biztosan jól javítunk, hiszen a háromszög-egyenlőtlenség miatt az eredetileg elküldött kódszótól különböző bármely kódszó biztosan $\frac{d}{2}$-nél több helyen tér el a vett szótól (Miért?).

Másrészt legyenek u és w olyan kódszavak, amelyek távolsága d, és legyen v az a szó, amit úgy kapunk u-ból, hogy azon d pozícióból, amelyekben eltérnek, $t \geq \frac{d}{2}$ helyre a w megfelelő pozíciójában lévő betűt írjuk.
Ekkor v az u-tól t helyen, míg w-től $d - t \leq \frac{d}{2} \leq t$ helyen különbözik.
Ha a kód t-hibajavító lenne, akkor v-t egyrészt u-ra, másrészt w-re kellene javítania.
Ezáltal a kód pontosan $\lfloor \frac{d-1}{2} \rfloor$-hibajavító.

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):
$(b_1, b_2, \ldots, b_k) \mapsto (b_1, b_2, \ldots, b_k, \sum_{j=1}^{k} b_j)$.
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

$d(u, v) = w(u - v)$ (Miért?), 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.

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

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 $\mathbf{I}_k \in \mathbb{F}_q^{k \times k}$ 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 $\mathbf{H}(\mathbf{G}u) = (\mathbf{H}\mathbf{G})u = \mathbf{0}u = \underline{0}$,
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 $\sum_{j=1}^{l} u_j \cdot \underline{h_{\ell_j}} = \underline{0}$. 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 $\{\underline{e} + \underline{c} : \underline{c}$ kódszó$\}$ halmaz.

Megjegyzés

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

Állítás

Az azonos mellékosztályban lévő szavak pontosan az azonos szindrómájú szavak.

Bizonyítás

Meggondolni...

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 **H** ellenőrző mátrix oszlopainak a különböző nemnulla, 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, nemnulla 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: $101 + 111 = 010 \notin K$.