Diszkrét matematika 2.

Szoftvertervező szakirány
Kódolás

Juhász Zsófia
jzsofi@gmail.com, jzsofia@compalg.inf.elte.hu
Mérai László diái alapján

Komputeralgebra Tanszék

2019. ősz

A kommunikáció során információt hordozó adatokat viszünk át egy csatornán keresztül az információforrástól, az adótól az információ címzettjéhez, a vevőhöz.

$$\boxed{\text{Adó}} \longrightarrow \boxed{\text{Csatorna}} \longrightarrow \boxed{\text{Vevő}}$$

A kommunikáció vázlatos ábrája

Megjegyzés

Az információ átvitele térben és időben történik. Egyes esetekben az egyik, más esetekben a másik dimenzió a domináns (pl. telefonálás; információ rögzítése adathordozóra, majd későbbi visszaolvasása).

Definíció (információ)

Az információ új ismeret. Shannon nyomán az általa megszüntetett bizonytalansággal mérjük.

Definíció

Tegyük fel, hogy egy információforrás nagy számú, összesen n üzenetet bocsát ki. Az összes ténylegesen előforduló különböző üzenet legyen $a_1, a_2, \ldots, a_k$.

Ha az a_j üzenet m_j-szer fordul elő, akkor azt mondjuk, hogy a gyakorisága m_j, relatív gyakorisága pedig $p_j = \frac{m_j}{n} > 0$.

A $p_1, p_2, \ldots, p_k$ szám k-ast az üzenetek eloszlásának nevezzük ($\sum_{j=1}^{k} p_j = 1$).

Az a_j üzenet egyedi információtartalma $I_j = -\log_r p_j$, ahol r egy 1-nél nagyobb valós szám, ami az információ egységét határozza meg. Ha $r = 2$, akkor az információ egysége a bit.

Az üzenetforrás által kibocsátott üzenetek átlagos információtartalma, vagyis $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$ a forrás entrópiája. Ez csak az üzenetek eloszlásától függ, a tartalmuktól nem.

Egy k tagú eloszlásnak olyan pozitív valós számokból álló $p_1, p_2, \ldots, p_k$ sorozatot nevezünk, amelyre $\sum_{j=1}^{k} p_j = 1$. Ennek az eloszlásnak az entrópiája $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$.

Definíció (konvex és szigorúan konvex függvény)

Legyen $I \subseteq \mathbb{R}$ egy intervallum. Az $f : I \to \mathbb{R}$ függvényt konvexnek nevezzük, ha bármely $x_1, x_2 \in I$ és $0 \leq t \leq 1$ esetén

$$f\left(tx_1 + (1-t)x_2\right) \leq tf(x_1) + (1-t)f(x_2).$$

f szigorúan konvex, ha egyenlőség csak $t = 0$ vagy $t = 1$ esetén lehetséges.

Lemma (Jensen-egyenlőtlenség, NB)

Legyen $p_1, p_2, \ldots, p_k$ egy eloszlás, $f : I \to \mathbb{R}$ pedig egy szigorúan konvex függvény az $I \subseteq \mathbb{R}$ intervallumon. Ekkor $q_1, q_2, \ldots, q_k \in I$ esetén

$$f\left(\sum_{j=1}^{k} p_j q_j\right) \leq \sum_{j=1}^{k} p_j f(q_j),$$

és egyenlőség pontosan akkor áll fenn, ha $q_1 = q_2 = \ldots = q_k$.

Tétel (Felső korlát eloszlás entrópiájára)

Bármilyen eloszláshoz tartozó entrópiára

$$H_r(p_1, p_2, \ldots, p_k) \leq \log_r k,$$

és egyenlőség pontosan akkor teljesül, ha $p_1 = p_2 = \ldots = p_k = \frac{1}{k}$.

Bizonyítás

$r > 1$ esetén a $-\log_r(x)$ függvény szigorúan konvex, ezért használhatjuk a lemmát $q_j = \frac{1}{p_j}$ választással:

$$-H_r(p_1, p_2, \ldots, p_k) = \sum_{j=1}^{k} p_j \log_r p_j =$$

$$= \sum_{j=1}^{k} p_j \left(-\log_r \frac{1}{p_j}\right) \geq -\log_r \left(\sum_{j=1}^{k} p_j \frac{1}{p_j}\right) = -\log_r k.$$

Definíció (kódolás, felbontható kódolás)

A kódolás alatt a legáltalánosabb értelemben az üzenetek halmazának egy másik halmazba való leképezését értjük.
Ha a leképezés injektív, akkor azt mondjuk, hogy a kódolás felbontható, egyértelműen dekódolható, vagy veszteségmentes, egyébként veszteségesnek nevezzük, mert információvesztéssel jár.

Betűnkénti kódolás

A betűnkénti kódolás során az üzenetet meghatározott módon egymáshoz átfedés nélkül csatlakozó részekre bontjuk, egy-egy ilyen részt egy szótár alapján kódolunk, és az így kapott kódokat az eredeti sorrendnek megfelelően egymáshoz láncoljuk.
Az általánosság csorbítása nélkül feltehetjük, hogy a szótár alapján kódolandó elemi üzenetek egy A ábécé (a kódolandó ábécé) betűi, és egy-egy ilyen betű kódja egy másik (az előbbitől nem feltétlenül különböző) B ábécé (kódoló ábécé vagy kódábécé) betűivel felírt szó, vagyis ezen ábécéből vett betűk véges sorozata, a sorozat elemeit egyszerűen egymás mellé írva. Az ábécékről feltesszük, hogy nem-üresek és végesek.

Definíció (A^+ és A^*)

Az A ábécé betűivel felírható összes (legalább egy betűt tartalmazó) szó halmazát A^+ jelöli, míg az egyetlen betűt sem tartalmazó üres szóval (jele: $\emptyset$ vagy λ) kibővített halmazt A^*.

Betűnkénti kódolás

Definíció (betűnkénti kódolás, kód, kódszavak)

A betűnkénti kódolást egy $\varphi : A \to B^*$ leképezés határozza meg, amelyet természetes módon terjesztünk ki egy $\psi : A^* \to B^*$ leképezéssé: $a_1 a_2 \ldots a_n = \alpha \in A^*$ esetén $\psi(\alpha) = \varphi(a_1)\varphi(a_2)\ldots\varphi(a_n)$. $\mathrm{rng}(\psi)$-t kódnak nevezzük, elemei a kódszavak.

Megjegyzés

Ha φ nem injektív, vagy az üres szó benne van az értékkészletében, akkor a kapott ψ kódolás nem injektív (Miért?), tehát nem felbontható, ezért betűnkénti kódolásnál feltesszük, hogy φ injektív, és B^+-ba képez.

Betűnkénti kódolás

Definíció (szó prefixe, szuffixe és infixe)

Tekintsünk egy A ábécét, és legyen $\alpha, \beta, \gamma \in A^*$. Ekkor α prefixe (előtagja), míg γ szuffixe (utótagja) $\alpha\gamma$-nak, β pedig infixe (belső tagja) $\alpha\beta\gamma$-nak.

Definíció (szó triviális perfixei, szuffixei és infixei)

Az üres szó és α prefixe, szuffixe és infixe is α-nak, ezeket α triviális prefixeinek, triviális szuffixeinek és triviális infixeinek nevezzük.

Definíció (szó valódi prefixe, szuffixe és infixe)

α egy prefixét, szuffixét, illetve infixét valódi prefixnek, valódi szuffixnek, illetve valódi infixnek nevezzük, ha nem egyezik meg α-val.

Definíció (prefixmentes halmaz)

Prefixmentes halmaznak nevezzük szavak egy halmazát, ha nincs benne két olyan különböző szó, hogy egyik a másik prefixe.

Betűnkénti kódolás

Definíció (prefix kód, fix hosszúságú kód, vesszős kód)

Tekintsük az injektív $\varphi : A \to B^+$ leképezést, illetve az általa meghatározott ψ betűnkénti kódolást.
Ha $\mathrm{rng}(\varphi)$ prefixmentes halmaz, akkor prefix kódról beszélünk.
Ha $\mathrm{rng}(\varphi)$ elemei azonos hosszúságúak, akkor egyenletes kódról, fix hosszúságú kódról, esetleg blokk-kódról beszélünk.
Vesszős kódról beszélünk, ha van egy olyan $\vartheta \in B^+$ szó (a vessző), amely minden kódszónak szuffixe, de egyetlen kódszó sem áll elő $\alpha\vartheta\beta$ alakban nem üres β szóval.

Állítás (Prefix kód felbontahtósága)

Prefix kód felbontható.

Bizonyítás

Konstruktív: nézzük az eddig beérkezett szimbólumokból összeálló szót. Amint ez kiadja a kódolandó ábécé valamely betűjének a kódját, azonnal dekódolhatunk a megfelelő betűre, mert a folytatásával kapott jelsorozat egyetlen betűnek sem lehet a kódja.

Betűnkénti kódolás

Állítás (Az egyenletes kódok prefix kódok)

Egyenletes kód prefix (így nyilván felbontható is).

Bizonyítás

Mivel a kódszavak hossza azonos, ezért csak úgy lehet egy kódszó prefixe egy másiknak, ha megegyeznek.

Állítás (A vesszős kódok prefix kódok)

Vesszős kód prefix (így nyilván felbontható is).

Bizonyítás

A vessző egyértelműen jelzi egy kódszó végét, hiszen ha folytatva kódszót kapnánk, abban a vessző tiltott módon szerepelne.

Betűnkénti kódolás

Példák

Legyen $A = \{a,b,c\}$, $B = \{0,1\}$, $\varphi : A \to B^+$ pedig az alábbi módon definiált.

	1.	2.	3.	4.	5.	6.
$\varphi(a)$	01	1	01	0	00	01
$\varphi(b)$	1101	01	011	10	10	001
$\varphi(c)$	01	10	11	11	11	0001

1. $\varphi(a) = \varphi(c) \implies \varphi$ nem injektív
2. $\psi(ab) =101= \psi(ca) \implies$ nem felbontható
3. nem prefix, de felbontható
4. prefix
5. egyenletes
6. vesszős

Betűnkénti kódolás

Tétel (McMillan-egyenlőtlenség, NB)

Legyen $A = \{a_1, a_2, \ldots, a_n\}$ és B két ábécé, B elemeinek száma $r \geq 2$, és $\varphi : A \to B^+$ injektív leképezés.
Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $\ell_j = |\varphi(a_j)|$ jelöléssel

$$\sum_{j=1}^{n} \frac{1}{r^{\ell_j}} \leq 1.$$

Tétel (McMillan-egyenlőtlenség „megfordítása”, NB)

Az előző tétel jelöléseit használva, ha $\ell_1, \ell_2, \ldots, \ell_n$ olyan pozitív egész számok, hogy $\sum_{j=1}^{n} r^{-\ell_j} \leq 1$, akkor van az A-nak a B elemeivel való olyan felbontható (sőt prefix) kódolása, hogy az a_j betű kódjának hossza ℓ_j.

Betűnkénti kódolás

Tétel (McMillan-egyenlőtlenség, NB)

Legyen $A = \{a_1, a_2, \ldots, a_n\}$ és B két ábécé, B elemeinek száma $r \geq 2$, és $\varphi : A \to B^+$ injektív leképezés.
Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $\ell_j = |\varphi(a_j)|$ jelöléssel

$$\sum_{j=1}^{n} r^{-\ell_j} \leq 1.$$

Tétel (McMillan-egyenlőtlenség „megfordítása”, NB)

Az előző tétel jelöléseit használva, ha $\ell_1, \ell_2, \ldots, \ell_n$ olyan pozitív egész számok, hogy $\sum_{j=1}^{n} r^{-\ell_j} \leq 1$, akkor van az A-nak a B elemeivel való olyan felbontható (sőt prefix) kódolása, hogy az a_j betű kódjának hossza ℓ_j.

Betűnkénti kódolás

Definíció (átlagos szóhossz, optimális kód)

Legyen $A = \{a_1, a_2, \ldots, a_n\}$ a kódolandó ábécé, $p_1, p_2, \ldots, p_n$ a betűk eloszlása, $\varphi : A \to B^+$ injektív leképezés, továbbá $\ell_j = |\varphi(a_j)|$.
Ekkor $\overline{\ell} = \sum_{j=1}^{n} p_j \ell_j$ a kód átlagos szóhossza.
Ha adott elemszámú ábécével és eloszlással egy felbontható betűnkénti kód átlagos szóhosszúsága minimális, akkor optimális kódnak nevezzük.

Megjegyzés

Az átlagos kódhossz valós szám, és valós számok halmazában nem feltétlenül van minimális elem (ld. $\{\frac{1}{n} | n \in \mathbb{N}\}$), ezért optimális kód létezése nem triviális.

Betűnkénti kódolás

Állítás (Optimális kód létezése)

Adott ábécé és eloszlás esetén létezik optimális kód.

Bizonyítás

Válasszunk egy tetszőleges felbontható kódot (Miért van ilyen?), ennek átlagos szóhosszúsága legyen ℓ*. Mivel* $p_j\ell_j > \ell$ *esetén a kód nem lehet optimális (Miért?), ezért elég azokat a kódokat tekinteni, amelyekre* $\ell_j \leq \frac{\ell}{p_j}$*, ha* $j = 1, 2, \ldots, n$*. Ilyen kód csak véges sok van, így van köztük minimális átlagos hosszúságú.*

Betűnkénti kódolás

Tétel (Shannon tétele zajmentes csatornára)

Legyen $A = \{a_1, a_2, \ldots, a_n\}$ a kódolandó ábécé, $p_1, p_2, \ldots, p_n$ a betűk eloszlása, $\varphi : A \to B^+$ injektív leképezés, B elemeinek a száma $r \geq 2$, továbbá $\ell_j = |\varphi(a_j)|$.
Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $H_r(p_1, p_2, \ldots, p_n) \leq \overline{\ell}$.

Bizonyítás

$$\overline{\ell} - H_r(p_1, p_2, \ldots, p_n) = \sum_{j=1}^{n} p_j \ell_j + \sum_{j=1}^{n} p_j \log_r p_j =$$

$$= \sum_{j=1}^{n} p_j \cdot (-\log_r(r^{-\ell_j})) + \sum_{j=1}^{n} p_j \cdot \left(-\log_r \frac{1}{p_j}\right) = \sum_{j=1}^{n} p_j \cdot \left(-\log_r \frac{r^{-\ell_j}}{p_j}\right) \geq$$

$$\geq -\log_r \left(\sum_{j=1}^{n} r^{-\ell_j}\right) \geq -\log_r 1 = 0$$

Betűnkénti kódolás

Tétel (Shannon kód létezése)

Az előző tétel jelöléseivel, ha $n > 1$, akkor van olyan prefix kód, amire $\overline{\ell} < H_r(p_1, p_2, \ldots, p_n) + 1$.

Bizonyítás

Válasszunk olyan $\ell_1, \ell_2, \ldots, \ell_n$ természetes számokat, amelyekre $r^{-\ell_j} \leq p_j < r^{-\ell_j+1}$, ha $j = 1, 2, \ldots, n$ (Miért tudunk ilyeneket választani?). Ekkor $\sum_{j=1}^{n} r^{-\ell_j} \leq \sum_{j=1}^{n} p_j = 1$, így a McMillan-egyenlőtlenség megfordítása miatt létezik prefix kód az adott ℓ_j hosszakkal. Mivel $\ell_j < 1 - \log_r p_j$ (Miért?), ezért

$$\overline{\ell} = \sum_{j=1}^{n} p_j \ell_j < \sum_{j=1}^{n} p_j (1 - \log_r p_j) = 1 + H_r(p_1, p_2, \ldots, p_n).$$

Optimális kódkonstrukció: Huffman-kód

Legyen $\{a_1, a_2, \ldots, a_n\}$ az üzenetek halmaza, a hozzájuk tartozó eloszlás pedig $\{p_1, p_2, \ldots, p_n\}$, a kódábécé elemszáma r.
Rendezzük relatív gyakoriság szerint csökkenő sorrendbe a betűket.
Osszuk el maradékosan $n-2$-t $r-1$-gyel:
$n-2 = q(r-1)+m \quad 0 \leq m < r-1$, és legyen $t = m+2$.
Helyettesítsük az utolsó t betűt egy új betűvel, amihez az elhagyott betűk relatív gyakoriságainak összegét rendeljük, és az így kapott gyakoriságoknak megfelelően helyezzük el az új betűt a sorozatban.
Ezek után ismételjük meg az előző redukciót, de most már minden lépésben r betűvel csökkentve a kódolandó halmazt, mígnem már csak r betű marad.
Most a redukált ábécé legfeljebb r betűt tartalmaz, és ha volt redukció, akkor pontosan r-et.
Ezeket a kódoló ábécé elemeivel kódoljuk, majd a redukciónak megfelelően visszafelé haladva, az összevont betűk kódját az összevonásként kapott betű már meglévő kódjának a kódoló ábécé különböző betűivel való kiegészítésével kapjuk.

Példa Huffman-kódra

Legyen $A = \{a, b, \ldots, j\}$, a relatív gyakoriságok $0,17; 0,02; 0,13; 0,02; 0,01; 0,31; 0,02; 0,17; 0,06; 0,09$, a kódoló ábécé pedig $\{0, 1, 2\}$. $10 - 2 = 4 \cdot (3 - 1) + 0$, így $t = 0 + 2 = 2$.

f	0,31	
a	0,17	
h	0,17	
c	0,13	
j	0,09	
i	0,06	
b	0,02	
d	0,02	
g	0,02	0, 03
e	0,01	

f	0,31	
a	0,17	
h	0,17	
c	0,13	
j	0,09	
i	0,06	
(g,e)	0,03	
b	0,02	0, 07
d	0,02	

f	0,31	
a	0,17	
h	0,17	
c	0,13	
j	0,09	
((g,e),b,d)	0,07	0, 22
i	0,06	

f	0,31	
(j,((g,e),b,d),i)	0,22	
a	0,17	
h	0,17	0, 47
c	0,13	

(a,h,c)	0,47
f	0,31
(j,((g,e),b,d),i)	0,22

Példa Huffman-kódra folyt.

(a,h,c)	0,47
f	0,31
(j,((g,e),b,d),i)	0,22

Kódolás:

(a,h,c)$\mapsto$0	a$\mapsto$00		
	h$\mapsto$01		
	c$\mapsto$02		
f$\mapsto$1			
(j,((g,e),b,d),i)$\mapsto$2	j$\mapsto$20		
	((g,e),b,d)$\mapsto$21	(g,e)$\mapsto$210	g$\mapsto$2100
			e$\mapsto$2101
		b$\mapsto$211	
		d$\mapsto$212	
	i$\mapsto$22		

Entrópia: $\approx 1,73$.
Átlagos szóhossz: $1,79$.

Betűnkénti kódolás

Tétel (Huffman-kód optimalitása, NB)

A Huffman-kód optimális.

Példa Shannon-kódra

Az előző példában használt ábécét és eloszlást fogjuk használni. Rendezzük sorba az ábécét relatív gyakoriságok szerinti csökkenő sorrendben:

f	0,31
a	0,17
h	0,17
c	0,13
j	0,09
i	0,06
b	0,02
d	0,02
g	0,02
e	0,01

Példa Shannon-kódra folyt.

Határozzuk meg a szükséges szóhosszúságokat:
$\frac{1}{9} \leq 0,31; 0,17; 0,13 < \frac{1}{3}$, ezért f, a, h és c kódhossza 2.
$\frac{1}{27} \leq 0,09; 0,06 < \frac{1}{9}$, ezért j és i kódhossza 3.
$\frac{1}{81} \leq 0,02 < \frac{1}{27}$, ezért b, d és g kódhossza 4.
$\frac{1}{243} \leq 0,01 < \frac{1}{81}$, ezért e kódhossza 5.
Az f kódja 00, az a kódja 01, a h kódja 02, és ez utóbbihoz 1-et adva hármas alapú számrendszerben kapjuk c kódját, ami 10. Ehhez 1-et adva 11-et kapunk, de j kódjának hossza 3, ezért ezt még ki kell egészíteni jobbról egy 0-val, tehát j kódja 110. Hasonlóan folytatva megkapjuk a teljes kódot:

f	00
a	01
h	02
c	10
j	110
i	111
b	1120
d	1121
g	1122
e	12000

Átlagos szóhossz: $2,3 < 1,73 + 1$.

Betűnkénti kódolás

Kódfa

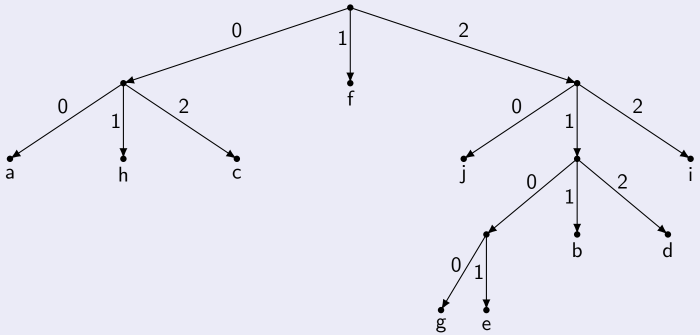
A betűnkénti kódolás szemléltethető egy címkézett irányított fával.
Legyen $\varphi : A \to B^*$ egy betűnkénti kódolás, és tekintsük $\mathrm{rng}(\varphi)$ prefixeinek halmazát. Ez a halmaz részbenrendezett a „prefixe” relációra. Vegyük ennek a Hasse-diagramját. Így egy irányított fát kapunk, aminek a gyökere az üres szó, és minden szó a hosszának megfelelő szinten van.
A fa éleit címkézzük úgy B elemeivel, hogy ha $\beta = \alpha b$ valamely $b \in B$-re, akkor az α-ból β-ba vezető él címkéje legyen b.
A kódfa csúcsait is megcímkézhetjük: az $a \in A$ kódjának megfelelő csúcs címkéje legyen $a \in A$; azon csúcs címkéje, amely nincsen $\mathrm{rng}(\varphi)$-ben, legyen „üres”.

Megjegyzés

Az előbbi konstrukció meg is fordítható. Tekintsünk egy véges, élcímkézett irányított fát, ahol az élcímkék halmaza B, az egy csúcsból kiinduló élek mind különböző címkéjűek, továbbá az A véges ábécének a csúcsokra való leképezését, amelynél minden levél előáll képként.
Az $a \in A$ betű kódja legyen az a szó, amelyet úgy kapunk, hogy a gyökértől az a-nak megfelelő csúcsig haladó irányított út mentén összeolvassuk az élek címkéit.

Kódfa

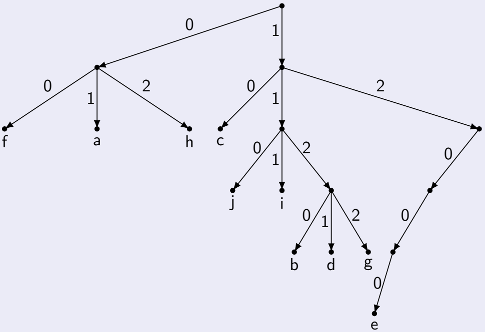
Példa



A Huffman-kódos példában szereplő kódhoz tartozó kódfa.
$\varphi(a)=$00, $\varphi(b)=$211, $\varphi(c)=$02, $\varphi(d)=$212, $\varphi(e)=$2101, $\varphi(f)=$1, $\varphi(g)=$2100, $\varphi(h)=$01, $\varphi(i)=$22, $\varphi(j)=$20.
A kódszavak prefixeinek halmaza:
$\{\lambda, 1, 00, 0, 01, 02, 20, 2, 22, 211, 21, 212, 2100, 210, 2101\}$

Kódfa

Példa



A Shannon-kódos példában szereplő kódhoz tartozó kódfa.
$\varphi(a) =$01, $\varphi(b) =$1120, $\varphi(c) =$10, $\varphi(d) =$1121, $\varphi(e) =$12000,
$\varphi(f) =$00, $\varphi(g) =$1122, $\varphi(h) =$02, $\varphi(i) =$111, $\varphi(j) =$110.
A kódszavak prefixeinek halmaza:
$\{01, 0, \lambda, 1120, 112, 11, 1, 10, 1121, 12000, 1200, 120, 12, 00, 1122, 02, 111, 110\}$

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 (t-hibajelző és pontosan t-hibajelző kódok)

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 (Hamming-távolság)

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:

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

Példa

$$\begin{array}{ccccc} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ \hline \neq & \neq & = & \neq & \neq \end{array} \qquad \begin{array}{cccc} \mathrm{A} & \mathrm{L} & \mathrm{M} & \mathrm{A} \\ \mathrm{A} & \mathrm{N} & \mathrm{N} & \mathrm{A} \\ \hline = & \neq & \neq & = \end{array}$$

$d(01110{,}10101)=4$ $\qquad$ $d(\mathrm{ALMA},\mathrm{ANNA})=2$

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 (kód távolsága)

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

Példa (*)

$$\begin{array}{lcccc}
(0,0) \mapsto (0,0,0,0,0) & & & & \\
 & 3 & & & \\
(0,1) \mapsto (0,1,1,1,0) & & 3 & & \\
 & 4 & & & 4 \\
(1,0) \mapsto (1,0,1,0,1) & & & 3 & \\
 & 3 & & & \\
(1,1) \mapsto (1,1,0,1,1) & & & &
\end{array}$$

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)

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 (t-hibajavító és pontosan t-hibajavító kódok)

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.
$(0,0,0,0,0) \rightsquigarrow (1,0,0,0,1) \to (1,0,1,0,1)$

Példa (ismétléses kód)

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

Hibakorlátozó kódolás

Tétel (Singleton-korlát)

Ha $K \subseteq A^n$, $|A| = q$ 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 (MDS-kód)

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 $K \subseteq A^n$, $|A| = q$ 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 (perfekt kód)

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 (lineáris kód)

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 (szó súlya és kód súlya)

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 (Kapcsolat lineáris kód távolsága és súlya között)

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 (lineáris kód generátormátrixa)

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 (lineáris kód ellenőrző mátrixa)

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 (szisztematikus kódolás)

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 (Szisztematkus kódolás egy ellenőrző mátrixa)

Legyen $\boldsymbol{G} \in \mathbb{F}_q^{n\times k}$ *egy szisztematikus kód generátormátrixa:*
$\boldsymbol{G} = \begin{pmatrix} \boldsymbol{I}_k \\ \boldsymbol{P} \end{pmatrix}$. *Ekkor* $\boldsymbol{H} = \begin{pmatrix} -\boldsymbol{P} & \boldsymbol{I}_{n-k} \end{pmatrix}$ *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 $\mathrm{Im}(\mathbf{G}) \subseteq \mathrm{Ker}(\mathbf{H})$, 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 (Lineáris kód ellenőrző mátrixa és súlya)

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 (szindróma)

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 (hibavektor)

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 (mellékosztályok)

Valamely $\underline{e}$ hibavektorhoz tartozó mellékosztály az $\{\underline{e} + \underline{c} : \underline{c} \text{ kódszó}\}$ 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 (mellékosztály-vezető)

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 (A szindrómadekódolás minimális távolságú dekódolás)

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 $K \subseteq A^n$, $|A| = q$ 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 (Hamming-kód)

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 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 (ciklikus kód)

A $K \subseteq \mathbb{F}_q^n$ 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: $101 + 111 = 010 \notin K$.