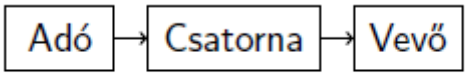
Add meg a kommunikáció vázlatos és részletes ábráját !



A kommunikáció vázlatos ábrája

Kodólás , dekódolás , zaj kerül még az ábrába !

Definiáld az információ fogalmát , hogyan mérjük ?!

Definíció

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

Definiáld a gyakoriság / relatív gyakoriság fogalmát !

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

Definiáld az üzenetek eloszlásának fogalmát !

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

Definiáld egy üzenet egyedi információ tartalmát !

Az a_j üzenet egyedi információtartalma $I_j = -\log_r p_j$, ahol r egy nagyobb valós szám, ami az információ egységét határozza meg.

Definiáld üzenetek átlagos információ tartalmát !

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.

Mit nevezünk eloszlásnak és definiáld entrópiáját ?

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

Definiáld a konvex és a szigorúan konvex függvény fogalmát !

Definíció

Legyen $I \subset \mathbb{R}$. 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.

Hogyan szól a Jensen-egyenlőtlenség ?

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 $I \subset \mathbb{R}$ 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 $q_1 = q_2 = \ldots = q_k$.

Milyen felső korlát adható az entrópiára ? Bizonyítás !

Tétel

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:

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

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

Definiáld a kódolás fogalmát !

A kódolás alatt a legáltalánosabb értelemben az üzenetek halmazának egy másik halmazba való leképezését értjük.

Mit nevezünk kódnak ?

Definíció

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

Definiáld a felbontható /egyértelműen dekódolható/veszteségmentes kódolást!

Ha a leképezés injektív, akkor azt mondjuk, hogy a kódolás felbontható, egyértelműen dekódolható, vagy veszteségmentes, egyébként veszteségesnek nevezzük, mert információvesztéssel jár.

Definiáld az ábécé , betű , szó fogalmát !

ábécé : betükből all.

betű: karakterek

szó : betuk sorozata

Mást nem találtam hozzas!

Definiáld az A+ és az A* halmazokat !

Definíció

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^*.

Definiáld a betünkénti kódolást !

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.

Mit érdemes feltenni egy betünkénti kódolás alapjául szolgáló leképzésről ?

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.

Definiáld prefix, infix , szuffix fogalmát !

Definíció

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.

Definiáld a valódi prefix/infix/szufix fogalmát !

Definíció

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

Definiáld a triviális prefix/infix/szufix fogalmát !

Definíció

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

Definiáld a prefix kód fogalmát !

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.

Definiáld az egyenletes / fix hosszuságú / blokk kód fogalmát !

Ha $\mathrm{rng}(\varphi)$ elemei azonos hosszúságúak, akkor egyenletes kódról, fix hosszúságú kódról, esetleg blokk-kódról beszélünk.

Definiáld a vesszős kód fogalmát !

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.

Milyen kapcsolat van a prefix , egyenletes ,vesszős és felbonthatatlan kódok között ? Bitonyitás!

Állítás

Prefix kód felbontható.

Bizonyítás

Konstruktív: nézzük az eddig beérkezett betűkből összeálló szót. Amint ez kiadja a kódolandó ábécé valamely betűjéhez tartozó kódszót, azonnal dekódolhatunk a megfelelő betűre, mert a folytatásával kapott jelsorozat egyetlen betűhöz rendelt kódszó sem lehet.

Állítás

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

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.

Adj példát nem prefix , de felbontható kódra !

01

011

11

Hogyan szól a McMillan egyenlőtlenség és a „megfordítása”?

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 $l_j = |\varphi(a_j)|$ jelöléssel

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

Tétel (McMillan-egyenlőtlenség megfordítása, NB)

Az előző tétel jelöléseit használva, ha $l_1, l_2, \ldots, l_n$ olyan pozitív egész számok, hogy $\sum_{j=1}^{n} r^{-l_j} \leq 1$, akkor van az A-nak a B elemeivel való olyan felbontható (sőt prefix) kódolása, hogy az a_j betűhöz rendelt kódszó hossza l_j.

Definiáld a kód átlagos szóhosszát!

Definíció

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 $l_j = |\varphi(a_j)|$.
Ekkor $\overline{l} = \sum_{j=1}^{n} p_j l_j$ a kód átlagos szóhossza.

Definiáld az optimális kód fogalmát !

Ha adott elemszámú ábécével és eloszlással egy felbontható betűnkénti kód átlagos szóhosszúsága minimális, akkor optimális kódnak nevezzük.

Mit mondhatunk optimális kód létezésével kapcsolatosan ? Bizonyítás!

Állítás

Adott ábécé és eloszlás esetén létezik optimális kód.

Bizonyítás

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

Hogyan szól Shannon tétele zajmentes csatornára ? Bizonyítás !

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 $l_j = |\varphi(a_j)|$.
Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $H_r(p_1, p_2, \ldots, p_n) \leq \overline{l}$.

Bizonyítás

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

$$= -\sum_{j=1}^{n} p_j \log_r r^{-l_j} - \sum_{j=1}^{n} p_j \log_r \frac{1}{p_j} = -\sum_{j=1}^{n} p_j \log_r \frac{r^{-l_j}}{p_j} \geq$$

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

Mit mondhatunk Shannon-kód átlagos szóhosszáról ? Bizonyítás!

Tétel (Shannon kód létezése)

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

Bizonyítás

Válasszunk olyan $l_1, l_2, \ldots, l_n$ természetes számokat, amelyekre $r^{-l_j} \leq p_j < r^{-l_j+1}$, ha $j = 1, 2, \ldots, n$ (Miért tudunk ilyeneket választani?). Ekkor $\sum_{j=1}^{n} r^{-l_j} \leq \sum_{j=1}^{n} p_j = 1$, így a McMillan-egyenlőtlenség megfordítása miatt létezik prefix kód az adott l_j hosszakkal. Mivel $l_j < 1 - \log_r p_j$ (Miért?), ezért

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

Hogyan konstruálunk Huffman-kódot?

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.

Hogyan konstruálunk Shannon-kódot?

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

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: $2,3 < 1,73 + 1$.

Definiáld a kódfa fogalmát !

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. (Miért?)
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".

Hogyan működik az ISBN kódolása ? Bizonyítás ! (Milyen hibákat jelez !)

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 $d_j = d_{j+1}$.

Mi a paritásbites kód ?

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.

Mi az a kétdimenziós paritásellenőrzés?

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.

Definiáld a t-hibajelző és pontosan t-hibajelző kód fogalmát!

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.

Definiáld a Hamming-távolságot!

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:

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

Milyen tulajdonságokkal rendelkezik a Hamming-távolság?

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).

Definiáld a kód távolságot !

Definíció

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

Mit jelent a minimális távolságú dekódolás?

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.

Definiáld a t-hibajavító és a pontosan t-hibajavító kód fogalmát!

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.

Mi az az ismétléses kód?

Példa (ismétléses kód)

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

Fogalmazd meg a Singleton-korlátra vonatkozó állítást! Bizonyítás !

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.

Definiáld az MDS-kód fogalmát!

Definíció

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

Fogalmazd meg a Hamming-korlátra vonatkozó állítást! Bizonyítás !

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?).

Definiáld a perfekt kód fogalmát!

Definíció

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

Mi a kapcsolat kód távolsága és hibajelző képessége között? Bizonyítás!

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 különböző 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.

Mi a kapcsolat kód távolsága és hibajavító képessége között? Bizonyítás !

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 a d pozícióból $t \geq \frac{d}{2}$ 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.

Definiáld a lineáris tér és kód fogalmát és milyen műveletekkel alkot lineáris teret F^n!

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.

Milyen paraméterekkel jellemezzük a lineáris kódokat?

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.

Milyen alakot ölt a Singleton-korlát lineáris kód esetén?

Megjegyzés

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

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

Adj példát lineáris kódra!

Példa

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

Definiáld a kódszó és kód súlyát!

Definíció

Az $\mathbb{F}$ véges test mint 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:

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

Milyen összefüggés van lineáris kód súlya és távolsága között? Bizonyítás !

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?).

Definiáld lineáris kód generátormátrixát!

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.

Definiáld lineáris kód ellenörző mátrixát!

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.

Mi a kapcsolat a generátormátrix és ellenörző mátrix között?

Megjegyzés

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

Definiáld a szisztematikus , üzenetszegmens , a paritásszegmens kódolás fogalmát!

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.

Mi a kapcsolat szisztematikus kód generátormátrixa és ellenörző mátrixa között ? Bizonyítás !

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 $\mathrm{Im}(\mathbf{G}) = \mathrm{Ker}(\mathbf{H})$.

Hogyan dekódolunk szisztematikus kódolás esetén?

Megjegyzés

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

Mi a kapcsolat az ellenörző mátrix és a kód távolsága között? Bizonyítás !

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.

Definiáld a szindróma fogalmát!

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.

Definiáld a hibavektor fogalmát!

Definíció

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

Definiáld egy adott hibavektorhoz tartozó mellékosztályt!

Definíció

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

Hogyan jellemezhetőek az azonos mellékosztályban lévő szavak a szindrómájuk segítségével?

Állítás

Az azonos mellékosztályban lévő szavak szindrómája megegyezik.

Definiáld a mellékosztálytvezető fogalmát!

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.

Írd le a szindrómadekódolást!

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.

Mi a kapcsolat a szindrómadekódolás és a minimális távolságú dekódolás között? Bizonyítás !

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.

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 $\underline{e} = \underline{e_s}$.