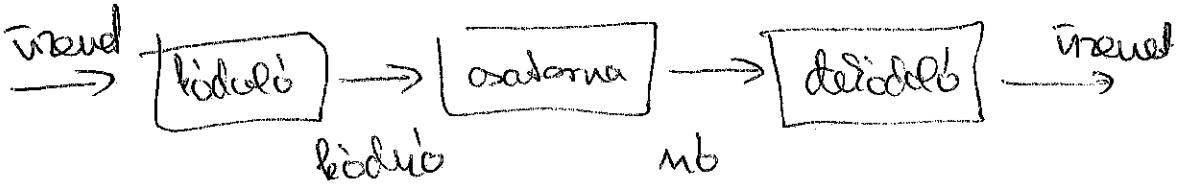
Kódoláselmélet 2020. október 21.



Def $\varphi : M \to C$ **kódolás** kijelölő leképezés

$M, C \subseteq K^* = \{ a_0 a_1 \dots a_{n-1} \mid n \geq 0,\ a_i \in K \}$

üzenetek, kódszavak, ábécé

dekódolás: $\psi : K^* \to M$ parciális leképezés

Def.: C kód **blokk kód**, ha minden szó vagyon olyan hosszú. $C \subseteq K^n$. (n a **kód hossza**)

Def.: C kód **lineáris**, ha K test és $C \leq K^n$ altér.

Def.: C blokk kód **információs rátája** (**kód sebesség**)

$$\frac{\log_{|K|} |C|}{n} \quad \leftarrow \text{"adatbitek száma"} \quad \leftarrow \text{"kódbitek száma"}$$

Példa: $C = \{000, 111\} \subseteq \mathbb{Z}_2^3$ infó rátája $\frac{1}{3}$

Def: A csatorna **szimmetrikus**, ha

(1) a szavak hosszát nem változtatja meg,

(2) minden betűt azonos sorrendben egymástól függetlenül továbbít vagy elront.

(3) helyesen p valószínűséggel továbbít minden elrontott szimbólumot azonos valószínűséggel ront $\frac{1-p}{|K|-1}$

$$p > \frac{1-p}{|K|-1}$$

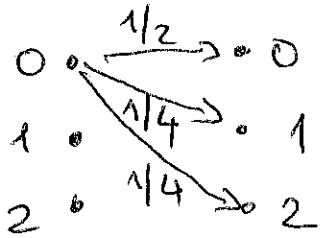
Def $u, v \in K^n$ **Hamming-távolsága**

$$d(u,v) = |\{ i < n \mid u_i \neq v_i \}|$$

Áll: $d(u,v) = 0 \iff u = v$, és teljesül a Δ-egyenlőtlenség.

Tétel: $C \subseteq K^n$ blokk kód, $v \in K^n$ a csatornából kijövő szó, és a csatorna szimmetrikus. Ekkor a legnagyobb valószínűséggel a csatorna azt az $u \in C$ kódszót rontotta el, amelynek Hamming-távolsága minimális v-től. Ha több ilyen van, akkor azok egyenlő valószínűséggel lehetnek a bemenő kódszó.

Példa $C = \{000, 111, 222\} \subseteq \mathbb{Z}_3^3$ $\quad p = 1/2$



$v = 121$

$d(000, v) = 3$

$d(111, v) = 2$

$d(222, v) = 1$

Példa:
1-hibajavító
2-hibajelző

$u = 111$ $\quad \frac{1}{2} \cdot \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{16}$

$u = 222$ $\quad \frac{1}{4} \cdot \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{32}$ $\quad$ V

Def: A ~~standard~~ hibajavító dekódoló

$\varphi: K^n \to C$ $\quad v\varphi = \begin{cases} u\varphi^{-1} & \text{ha } d(u,v) \text{ minimális, } u \in C. \\ - & \text{különben.} \end{cases}$

Def. A ~~standard~~ hibajelző dekódoló

$\varphi: K^n \to C$ $\quad v\varphi = \begin{cases} v\varphi^{-1} & \text{ha } v \in C \\ - & \text{különben.} \end{cases}$

hogy üzenet legyen

Def A $C \subseteq K^n$ blokk kód **t-hibajelző**, ha tetszőleges kódszót egyféleképp t helyen elrontva a standard hibajelző dekódoló észreveszi a hibát.

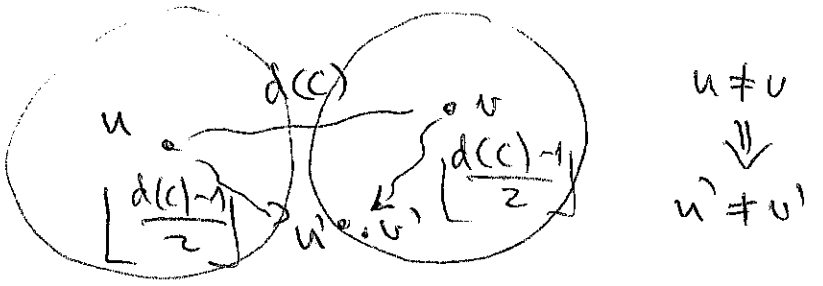
Def ..... **t-hibajavító** ..... a standard hibajavító dekódoló helyesen kijavítja.

Def: $C \subseteq K^n$ **minimális távolsága**

$$d(C) = \min_{\substack{u,v \in C \\ u \neq v}} d(u,v)$$

Tétel: Tetszőleges $C \subseteq K^n$ blokk-kódra $d(C)-1$ hibajelző és $\left\lfloor \frac{d(C)-1}{2} \right\rfloor$ hibajavító.

Biz



Tétel (Hamming-korlát) Ha $C \subseteq K^n$ t-hibajavító, akkor

$$|K|^n \geq |C| \cdot \underbrace{\sum_{i=0}^{t} \binom{n}{i} \cdot (|K|-1)^i}_{\text{a szóhossz hány t-nagyi gömbben a szavak száma.}}$$

Biz: ezek a gömbök diszjunktak.

Példa: Maximum hány hibajavító kódot lehet egy 7-hosszú 4/7 infó szóhosszú kód?

$K = \mathbb{Z}_2$ kínálja $\binom{7}{0} + \binom{7}{1} = 8$

$2^7 \geq 16 \cdot 8$ 1-hibajavító elvileg lehet.

Def: $C \subseteq K^n$ <u>**hibajelző**</u>, ha eleget a Hamming-korlátjának.

Példa: $C = \{000, 111\} \subseteq \mathbb{Z}_2^3$ hibajelző 1-hibajavító kód.

Def: $C \subseteq K^n$ <u>**lineáris**</u>, ha K test és $C \leq K^n$ altér.
ekkor C információs rátája $\frac{\dim(C)}{n} = \log_{|K|}|C|$.
ekkor feltehető, hogy az üzenetek halmaza
$M = K^{\dim(C)}$.

Def: $C \leq K^n$ lineáris kód <u>**generátor mátrixa**</u>
$G \in K^{r \times n}$ ahol $r = \dim(C)$.
G sorai a C altér bázisát alkotják.

Példa: $G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \in \mathbb{Z}_2^{2\times 3}$ kód hossza = 3
dim = 2

$C = \{000, 101, 011, 110\}$

Def: C kód <u>**nintematikus**</u>, ha van olyan generátormátrixa, amely $G = (E \mid H)$ alakú.
↑ egység mátrix.

Def: lineáris kódoknál a kódolás = mátrix szorzás

$\varphi : M \to C$ $\quad M = K^r$, $C \leq K^n$, $\dim(C) = r$

$u \mapsto uG$
$\uparrow \quad \uparrow$
$K^r \quad K^n$

Áll: G nintematikus, akkor $u \mapsto uG = u(E \mid H) = (u)(uH)$
a kódnak első r betűje az üzenet.

Tétel: Minden lineáris kód ekvivalens egy mintegy mátrixos kóddal.

Def $C, D \leq K^n$ **ekvivalensek**, ha létezik olyan $\pi \in S_n$ permutáció, hogy

$$a_1 a_2 \dots a_n \in C \iff a_{1\pi} a_{2\pi} \dots a_{n\pi} \in D.$$

Biz: $C = \{0000, 1010, 0111, 1101\}$

$$G = \begin{pmatrix} 1010 \\ 0111 \end{pmatrix}$$

$$C = \{0000, 1010, 0011, 1001\}$$

$$G = \begin{pmatrix} \boxed{1}010 \\ 00\boxed{1}1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} \boxed{1}00\boxed{1} \\ 00\boxed{1}\boxed{1} \end{pmatrix}$$

$$\pi = (23)$$

ekvivalens kód gen. mátrixa $\begin{pmatrix} 1001 \\ 0101 \end{pmatrix}$.

Tétel: $C \leq K^n$ lineáris, akkor

$$d(C) = \min_{\substack{u \in C \\ u \neq 0}} d(u, 0)$$

Biz: $d(u, v) = d(u - v, 0)$.

Def: $C \leq K^n$ r-dimenziós lin. kód. A kódnak $P \in K^{n \times (n-r)}$ **ellenőrző mátrixa**, ha

$$u \in C \iff uP = 0$$

Áll: Ha C mintegy mátrixos a $G = (E|H)$ gen. mátrixszal akkor $P = \begin{pmatrix} -H \\ E \end{pmatrix}$ választható ellenőrző mátrixnak.

$$(uG)P = u(GP) = u0$$

Def: Legyen K tetszőleges véges test, $r \geq 2$

$$n = \frac{|K|^r - 1}{|K| - 1}$$ ← az 1-dim alterek száma K^r-ben.

$P \in K^{n \times r}$ olyan mátrix, amelynek sorai páronként lineárisan függetlenek (semelyik sem skalárszorosa a másiknak). Erről a P által meghatározott lineáris kódot Hamming-kódnak nevezzük.

Példa: $K = \mathbb{Z}_2$, $r = 3$

$$P = \begin{pmatrix} 011 \\ 101 \\ 110 \\ 111 \\ \hline 100 \\ 010 \\ 001 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ -H \\ \\ E \end{matrix} \qquad G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \begin{matrix} \nwarrow u \\ \swarrow v \end{matrix}$$

igaz vala 4/7

$u+v\,(1100|110)$
$\#2 \qquad \geq \#1$

Áll: minimális távolság $= 3$.

G minden u sorára $d(u,0) \geq 3$.

G minden $u+v$ sorára $d(u+v,0) \geq 3$

$u \neq v \neq w \neq u$ sorára $d(u+v+w,0) \geq 3$

Példa: $K = \mathbb{Z}_3$ $r = 2$

$$P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ \hline 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{matrix} \\ \\ -H \\ E \end{matrix} \qquad \begin{matrix} E & \quad H \end{matrix} \quad G = \left(\begin{array}{cc|cc} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{array}\right)$$

Tétel: A Hamming-kód tökéletes, min. távolsága 3.

azaz 1-hibajavító.

Példa

Hamming-kód dekódolása

$$G = \left(\begin{array}{cccc|ccc} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{array}\right) \qquad P = \begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \\ \hline 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix} \qquad K = \mathbb{Z}_2$$

dekódoljuk $u = (1110101)$ -át

szindróma

$uP = (101)$ $\quad u \notin C$.

szindróma dekódolás

$u = v + h \quad v \in C$ és h hiba

$h \in \{0000000, 1000000, 0100000, \ldots, 00\ldots01\}$

$uP = (v+h)P$

$= \underbrace{vP}_{0} + hP = hP$

$(1000000)P = (011)$

$(0100000)P = (101)$ $\quad$ hiba a 2. bitben van.

kódszavan $u - h = (1010101)$ üzenet (1010).

Példa:

Ugyanezt meg lehet csinálni más testre is

$$G = \left(\begin{array}{cc|cc} 1&0&2&2 \\ 0&1&2&1 \end{array}\right) \qquad P = \begin{pmatrix} 1&1 \\ 1&2 \\ \hline 1&0 \\ 0&1 \end{pmatrix}$$

hP ← hiba

$(1000)P = (11)$

$(2000)P = (22)$

$(0100)P = (12)$

$\vdots$

$(0001)P = (01)$

$(0002)P = (02)$