Kódoláselmélet 2020. október 28. ①

Def: $C \le K^n$ lineáris kód duális kódja

$$C^\perp = \{ y \in K^n \mid \forall x \in C \ \underbrace{\langle x, y\rangle}_{x_1y_1+\dots+x_ny_n} = 0 \} \le K^n.$$

Példa: $K = \mathbb{Z}_2^*$, $C = \{00, 11\} \subseteq \mathbb{Z}_2^2$

$$C^\perp = \{00, 11\} = C$$

Példa: C-nek ~~G generátor mátrixa~~, P ellenőrző mátrix

$$C = (P^T \text{ által gen kód})^\perp$$

Tétel: Tetszőleges $C \le K^n$-re

$$\dim(C) + \dim(C^\perp) = n$$

$$(C^\perp)^\perp = C$$

Lemma: Ha $G = (E|H) \in K^{r\times n}$ gen mátrixa C-nek, $r = \dim(C)$
akkor $P^T = (-H^T | E) \in K^{(n-r)\times n}$ gen. mátrixa a $C^\perp$-nek.
$\quad$ ($H^T \in K^{(n-r)\times r}$)

Biz: (1) P^T által gen kód $\subseteq C^\perp$

mivel $\langle , \rangle$ bilineáris, ezért elég megmutatni hogy P^T minden sora G minden sorára merőleges. $\iff GP = 0$

ez teljesül, mert $GP = (E|H)\left(\frac{-H}{E}\right) = E(-H) + HE = 0.$

(2) $C^\perp \subseteq P^T$ által gen kód.

$$y \in C^\perp \Leftrightarrow G y^T = 0 \Leftrightarrow y G^T = 0 \Leftrightarrow y \left(\frac{E}{H^T}\right) = 0$$

$$K^n \ni y = (y_1, y_2) \in K^r \times K^{n-r}$$

$$y \overset{?}{=} z P^T \quad \text{létezik-e ilyen } z \in K^{n-r}$$

$$\cancel{(y_1, y_2) = (z_1, z_2)(-H^T | E) = (-z_1 H^T, z_2)}$$

$$(y_1, y_2) = z P^T = z(-H^T | E) = (-z H^T, z)$$

csak a $z = y_2$ lehet megoldás.

$y - y_2 P^T \in C^\perp$ ezt tudjuk, de 0-e?

$$(y_1, y_2) - (\overline{y_2} H^T, y_2) = (\underbrace{y_1 + y_2 H^T}, 0) = (0, 0)$$

$$y\left(\frac{E}{H^T}\right) = 0.$$

Ezzel megmutattuk, hogy P^T által gen kód $= C^\perp$. ■

Biz (Tétel): Ha C gen. mátrixa $G = (E | H)$ alakú, akkor $\dim(C) = r$ és $\dim(C^\perp) = n - r$ azaz a dim összege n.

A lemma $G = (H | E)$ és $P^T = (E | -H^T)$-re is igaz.

azaz ha C gen mátrixa $G = (E | H)$ akkor

$C^\perp$ $\quad P^T = (-H^T | E)$ és

$(C^\perp)^\perp$ $\quad (E | -(-H^T)^T) = (E | H)$

Általában egy megfelelő permutációt véve van C-vel ekvivalens C' kód, melynek gen. mátrixa $(E | H)$ alakú. ■

Golay-kód

$$B = \left(\begin{array}{c|ccc|cccc|cccc}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
\hline
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
\hline
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{array}\right) \in \mathbb{Z}_2^{12\times 12}$$

B-nek ~~az also~~ jobb alsó 11×11 része forgás-szimmetrikus, $B^T = B$, minden sor-ban és oszlopban páratlan sok 1 (7 vagy 11 db)

Def: A kiterjesztett Golay-kód gen. mátrixa

$$G = (E\,|\,B) \in \mathbb{Z}_2^{12\times 24}$$

Áll: A kiterjesztett Golay-kód önduális

Biz G minden sorában 8 vagy 12 db 1-es van.
azaz minden sor önmagára merőleges.
első sor és bármely másik sor belső szorzatakor
6 db 1-est kell összeadni $\mathbb{Z}_2$-ben, azaz $=0$.
második és harmadik vagy lejjebb levő sor
belső szorzata 4 db 1-est ~~tartalmaz~~ összege, azaz $=0$.

$12+12=24.$

$GG^T = 0 \Longrightarrow$ tehát a duális kódban G
sorai ott vannak és éppen generálják a dim miatt.

Áll: A kiterjesztett Golay kódban minden szó Hamming-súlya 4-el osztható

Biz: Ez teljesül a generátor vektorokra

Ez a tulajdonság öröklődik a generált vektorokra

$$
\begin{array}{lccccl}
 & \overbrace{\quad}^{s\text{ db}} & \overbrace{\quad}^{t\text{ db}} & \overbrace{\quad}^{k} & \overbrace{\quad}^{l} & s+t+k+l=n \\
C \ni x & 1\ldots 1 & 1\ldots 1 & 0\ldots 0 & 0\ldots 0 & =24 \\
C \ni y & 1\ldots 1 & 0\ldots 0 & 1\ldots 1 & 0\ldots 0 & \\
C \ni x+y & 0\ldots 0 & 1\ldots 1 & 1\ldots 1 & 0\ldots 0 &
\end{array}
$$

$$4 \mid s+t = \|x\| \qquad \overset{?}{\Longrightarrow} \quad 4 \mid t+k$$
$$4 \mid s+k = \|y\|$$

x és y merőlegesen $\langle x, y\rangle = 0$

$$2 \mid s$$

$$4 \mid s+t+s+k = \underbrace{2s}_{4 \mid} + t + k$$

■

$\boxed{\text{Köv: A kiterjesztett Golay kód távolsága 8. min.}}$

Áll: Nincs olyan ~~ne~~ kódszó, melynek normája 4.

Biz: Ez a 4-súlyú szó az generátorok összege.

1 generátornak nem lehet az összege.
2 —//— —//— véges sok esetet végignézve.

3 vagy 4.

$$C \text{ gen. mátrixa } (\overset{\geq 3}{E} \mid B)$$

$$\overset{\parallel}{C^{\perp}} \quad —//— \quad (-B^T \mid \underset{\geq 3}{E}) = (B \mid \underset{\geq 3}{E})$$

itt a súly legalább 6.

■