2020 november 4. Kódoláselmélet

$B \in \mathbb{Z}_2^{12\times 12}$, $B^T = B$

$G = (E \mid B) \in \mathbb{Z}_2^{12\times 24}$ gen. mátrixa a kiterjesztett Golay kód

$G G^T = 0$

minimális távolság 8.

egy másik gen. mátrix $(B \mid E)$

ellenőrző mátrix $\left(\frac{B}{E}\right)$ és $\left(\frac{E}{B}\right)$

kódolás $u \in \mathbb{Z}_2^{12}$ üzenet $uG = (u, uB) \in \mathbb{Z}_2^{24}$

dekódolás $v \in C$ kódszó és z hibavektor $z = (x, y)$, $x \in \mathbb{Z}_2^{12}$, $y \in \mathbb{Z}_2^{12}$

$v+z$ elrontott szó, ezt kell dekódolni

$$(v+z)\left(\frac{B}{E}\right) = 0 \iff z = 0$$

8 min távolság $\Rightarrow$ 7-hiba jelző

$\Rightarrow$ 3-hiba javító

cél: legfeljebb 3-hibát kijavítani.

azaz $\|z\| \le 3$

$\boxed{(v+z)\left(\frac{B}{E}\right)}$ szindrómát ki tudjuk számolni

$$\| \quad z\left(\frac{B}{E}\right) = (xB + yE) \in \mathbb{Z}_2^{12}$$

(1) $\|x\| = 0$ és $\|y\| \le 3$ akkor

$$(xB + yE) = (0 + y) = y$$

kódszó az első három sor összege G-vel.

$v = (111000000000, \boxed{01}00\cancel{1}1011000)$

$v\begin{pmatrix} B \\ E \end{pmatrix} = (0 \dots 0) \in \mathbb{Z}_2^{12}$

$z = (\underbrace{000 \qquad 0}_{x}, \underbrace{110 \dots \qquad 0}_{y})$

$(v+z)\begin{pmatrix} B \\ E \end{pmatrix} = \underbrace{\left(v \begin{pmatrix} B \\ E \end{pmatrix}\right)}_{0} + z\begin{pmatrix} B \\ E \end{pmatrix} = xB + yE = yE = y$

$v+z = (111000000000, 100011011000)$

$(v+z)\begin{pmatrix} B \\ E \end{pmatrix} = (110000000000)$

(2) $\|x\| = 1$ és $\|y\| \leq 2$

$\cancel{x}$ $(v+z)\begin{pmatrix} B \\ E \end{pmatrix} = xB + yE$ ← szindróma

ekkor a szindróma B valamelyik sorától legfeljebb 2 távolságra van.

(3) $\|x\| \leq 3$ és $\|y\| = 0$

ekkor $\boxed{(v+z)\begin{pmatrix} E \\ B \end{pmatrix}}$ szindrómát $= \cancel{x}$

$(v + (\underbrace{10\dots0}_{x}, \underbrace{0\dots0}_{y}))\begin{pmatrix} E \\ B \end{pmatrix} = (100\dots0)$

(4) $\|x\| \leq 2$ és $\|y\| = 1$ hasonlóan (2)-höz.

(5) minden más esetben legalább 4 hiba történt.

Def: Golay-kód generátor mátrixa $G' \in \mathbb{Z}_2^{12\times 23}$

amit $G=(E|B)$-ből úgy kapunk,

hogy az utolsó oszlopot elvesszük. 23-hosszú

12-dim, minimális távolság 7.

Áll: Golay-kód tökéletes

Biz: 3-sugarú gömb.

$$\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}=$$

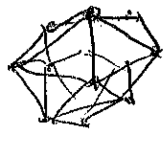
$$1+23+253+1771=2048=2^{11}$$

kódszavak száma 2^{12} $\qquad 2^{23}=2^{12}\cdot 2^{11}$ ✓.

összes szó száma 2^{23}

Áll: A kiterjesztett Golay-kód egy másik generátor rendszere

$(E|A)$ $\quad$ A az icosahedronban amely pontok össze vannak kötve, ott 0 van, különben 1.



(minden sorban 7 db 1-es)

Def: $C \le \mathbb{Z}_2^n$ lineáris kód szimmetria csoportja

$$\{\pi \in S_n \mid \forall c=(c_1\dots c_n)\in C \quad (c_{1\pi}, c_{2\pi},\dots,c_{n\pi})\in C\}$$

Def: M_{23} az a Golay kód szimmetria csop.

M_{24} kiterjesztett Golay-kód

Mathieu csoportok.

<u>Def</u>: $C \subseteq K^n$ <u>ciklikus</u>, ha

$$(a_0 a_1 \dots a_{n-1}) \in C \Leftrightarrow (a_1 a_2 \dots a_{n-1} a_0) \in C.$$

<u>Megj</u> ciklikus kódolnál a kódszavakat polinomokkal azonosítom

$$(a_0 a_1 \dots a_{n-1}) \in C$$

$$a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1} \in K[x].$$

<u>Tétel</u>: $C \subseteq K^n$ lineáris ciklikus kód, $C \neq \{0\}$
$g \in C$ minimális fokszámú főpolinom kódszó. Ekkor
1. g egyértelműen meghatározott (<u>generátor polinom</u>)
2. $h \in K^n$ $\quad h \in C \Leftrightarrow g \mid h$
3. g valódi osztója $x^n - 1$ polinomnak
4. C dimenziója $n - \deg(g)$.

<u>Biz</u>: ① Ha $g_1, g_2 \in C$ főpolinomok
és $\deg(g_1) = \deg(g_2)$ minimális fokszám
akkor $g_1 = g_2$, mert

$g_1 - g_2 \in C \qquad \deg(g_1 - g_2) < \deg(g_1)$
kiesik a főegyüttható

ha $g_1 - g_2 \neq 0$, akkor
$c(g_1 - g_2)$ főpolinom és kisebb fokszámú
ami ellentmondás, azaz $g_1 - g_2 = 0$.

② ha $g \mid h$ akkor $h = \underset{\in C}{b_0 g} + b_1 \underbrace{gx}_{\in C} + \dots \in C$ mert ciklikus

$h = (b_0 + b_1 x + \dots) g$

$\deg(h) \leq n-1$

másik irány: $h \in C$

$$h = g \cdot f + q \qquad f, q \in K[x]$$

maradékos osztás

$$h - gf = q \qquad \deg(q) < \deg(f)$$

$$\uparrow$$
$$C$$

de ez a minimalitás miatt csak a 0 polinom lehet.

3 $\quad x^n - 1 = g \cdot f + q$

1 mert főpolinom

$$g = a_0 + a_1 x + a_2 x^2 + \dots + \underset{1}{a_k} x^k \qquad k \le n-1$$

$$gx = a_0 x + a_1 x^2 + \dots + a_{k-1} x^k + a_k x^{k+1}$$

$$\vdots$$

lineáris független

$$g \cdot x^{n-k} = \cancel{a_k} + a_0 x^{n-k} + a_1 x^{n-k+1} + \dots + a_{k-1} x^{n-1} + \underset{a_k}{x^n}$$

$$g \cdot x^{n-k} - x^n + 1 =$$

$$= 1 + 0x + \dots + a_0 x^{n-k} + a_1 x^{n-k+1} + \dots + a_{k-1} x^{n-1} \in C$$

$$g x^{n-k} - x^n + 1 = g f$$

$$g(x^{n-k} - f) = x^n - 1$$

4 $\quad g, gx, \dots, gx^{n-k-1}$ lineárisan függetlenek, a főegyütthatók miatt, és generálnak minden kódszót, mert $h \in C \Leftrightarrow g \mid h$

C dimenziója $n - k = n - \deg(g)$.

Példa:

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \in \mathbb{Z}_2^{4\times 7}$$

Áll: ez ~~lineáris~~ ciklikus, mert elég megmutatni, hogy a ~~generátor~~ bázisvektorok eltoltja is a kódban van.

$$(1\,0\,0\,0\,1\,0\,1) \overset{?}{\in} C$$

ez éppen az első, harmadik és negyedik sorok összege.

Áll: $(1\,0\,1\,1\,0\,0\,0) = \underbrace{1 + x^2 + x^3}_{g}$ ez a min. fokszámú kódszó.

$$(b_0, b_1, b_2, b_3) \neq (0,0,0,0)$$

$$\deg\left(b_0 g + b_1 g x + b_2 g x^2 + b_3 g x^3\right) = \cancel{\deg(}$$

$$\deg(b_0 + b_1 x + b_2 x^2 + b_3 x^3) + \deg(g)$$

Programozás a titkosítás részhez:

1. RSA titkosítás gyors hatványozás, adott két prím p, q, válasszuk e-t és határozzuk meg d-t. és diofantoszi egyenlet nagy számokra
2. Miller-Rabin teszt (gyors hatványozás + algoritmus) és maradékos osztás
3. Legendre-szimbólum számolása
4. Solovay-Strassen teszt
5. Lineáris egyenletrendszer megoldása $\mathbb{Z}_2$ felett
6. Fermat faktorizáció
7. $\sqrt{n}$ lánctörtes közelítése
8. Pollard ϱ-módszer
9. Diffie-Hellman kulcscsere
10. Primitív elem keresése $GF(q)$-ban.
11. Silver-Pohlig-Hellman alg.
12. Kínai maradéktétel (kongruencia rendszer megoldása)
13. Elliptikus görbében számolni (Abel-csop.)