Lineární kódy:

U - lineární prostor nad $\mathbb{Z}_2$ (binární abeceda)

Ham. metrika

C - podprostor U

$[n,k,d]_2$

n - délka $(U = \mathbb{Z}_2^n)$

k - dimenze $(\log_2 |C|)$

d - vzdálenost

G - generující matice

$(\forall d)\ dG \in C$ unikátní

H - kontrolní matice

$(\forall \bar{c} \in \mathbb{Z}_2^d = U)\quad \bar{c}H = \begin{cases} = 0 & \bar{c} \in C \\ \neq 0 & \bar{c} \notin C \end{cases}$

R - dekódovací matice

$cR = d \quad (\forall c \in C)$

Př. 1 $[n,k,d]$ - kód pro liché d. Rozšíříme všechny slova o paritní bit (paritu počtu jedniček)

Určete parametry výsledného kódu.

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

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

d - liché

pak musí mít odlišné parity tudíž to pak podle toho můžu rozlišit

$[n+1, k$

$\begin{array}{ccc} 0000 & & 00000 \\ (1,1,1,1) & \to & (1,1,1,1,0) \end{array}$ → tady je d sudé, dostal jsem d stejné

$\begin{array}{ccc} 1111 & & 11110 \\ (0,0,1,0) & \to & (0,0,1,0,1) \end{array}$ → tady je d liché, dostal jsem $d+1$

Př: 2

Ukažte, že pokud G je generující a kontrolní U, platí že $GU = \emptyset$

$$(dG)U = 0$$

$$d(GU) = 0$$

$yU = 0$ pokud $y \in C$

Generující matice má v řádcích bázických vektory, kontrolní má ve sloupcích ortogonální doplňky vektorů z G, tudíž to přenásobením musí dát nulu.

Př: 3

Mějme G generující matici kódu C ve std. tvaru: $G = [I_k | P]$

$$H = \left[-P^T \middle| I_{n-k}\right]^T = \begin{bmatrix} -P \\ \hline I_{n-k} \end{bmatrix}$$

$$\left.\begin{pmatrix} -P \\ I_{n-k} \end{pmatrix}\right\} n \longrightarrow \text{rank} = n-k$$

$$\text{rank} = k \leftarrow k\left\{ \underbrace{\begin{pmatrix} \underbrace{I_k}_{k} & \underbrace{P}_{n-k} \end{pmatrix}}_{n} \right. \begin{pmatrix} -P + P \end{pmatrix} = \emptyset$$

Potřebujeme $(dG)\underline{R} = d$, tedy $d(GR) = d$, tedy $(GR) = I_k$

vyžadujeme nějaký „pseudo-inverz" v hodnosti „k".

Př.: 4

Navrhněte bin. kód rel. 16, opravující jednu chybu. Navíc, chceme aby syndrom binárně kódoval pozici, kterou je potřeba opravit

$[n,k,d]_2$ $\quad n = 7$, $k = 4$, $d = 3$ $\quad \to \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$

data $\to$ code

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = H$$

$$(a, b, c, d, e, f, g) \begin{pmatrix} x & y & z \end{pmatrix} = S$$

→ tohle je binární repr. pozice s chybou - podstatné, že umíme opravit jen jednu chybu

$\emptyset = z = a + c + e + g$

$\emptyset = y = b + c + f + g$

$\emptyset = x = d + e + f + g$

Operace nad $\mathbb{Z}_2$ $\to$ $2f = 0f$

$3g = g$

$+ = -$ ...

$e + g = a + c$ $\qquad g = a + b + d$

$f + g = b + c$ $\qquad e = b + c + d$

$e + f + g = d$ $\qquad f = a + c + d$

$$G_2 = \left(\begin{array}{cccc|ccc} 1 & & & \emptyset & 0 & 1 & 1 \\ & 1 & & & 1 & 0 & 1 \\ & & \ddots & & 1 & 1 & 0 \\ \emptyset & & & 1 & 1 & 1 & 1 \end{array}\right)$$

! Generující matice není nijak souvislá s kontrolní !