Start 11:42

Mějme komunikační kanál - binární 0/1, zpracuj ℓ-bitů
občas kanál přenese opačný bit

$1110 \rightsquigarrow 1101$

Cíl 1: poznat chybu - pošleme každý bit 2x

$11\ 11\ 00\ 00 \rightsquigarrow 11\ 10\ 11\ 00$

každých k bitům poslat kontrolní součet $\boxplus \sum_k b_i$ (k-bitový)

ℓ bitů $\rightsquigarrow \left\lceil \frac{k+1}{k} \cdot \ell \right\rceil$ bitů

Cíl 2: poznat & opravit chybu - pošleme každý bit 3x

$111\ 111\ 111\ 000 \rightsquigarrow 111\ 111\ 101\ 000$

$1\ 1\ 1\ 0$

ℓ bitů $\rightsquigarrow 3\ell$ bitů

Chceme lepší!

① $k=7 \rightsquigarrow 4$ bity

kódovací matice $\rightsquigarrow \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ 1 & 1 & 1 & & 1 & & \\ & 1 & 1 & 1 & & 1 & \\ 1 & & 1 & 1 & & & 1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_7 \end{pmatrix} \in \mathbb{Z}_2^7 = \begin{pmatrix} b_1 \\ \vdots \\ b_7 \\ \sum b_i \end{pmatrix} \in \mathbb{Z}_2^8$

② $G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} \in \mathbb{Z}_2^7$

ℓ bitová zpráva $\rightsquigarrow \left(\frac{7\ell}{4}\right)$-bitový výstup

$\mathbb{Z}_2^4$

kanál

$(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3, \tilde{b}_4, \tilde{\sigma}_1, \tilde{\sigma}_2, \tilde{\sigma}_3)$

pokud dojde při přenosu 7-ice k jedné chybě

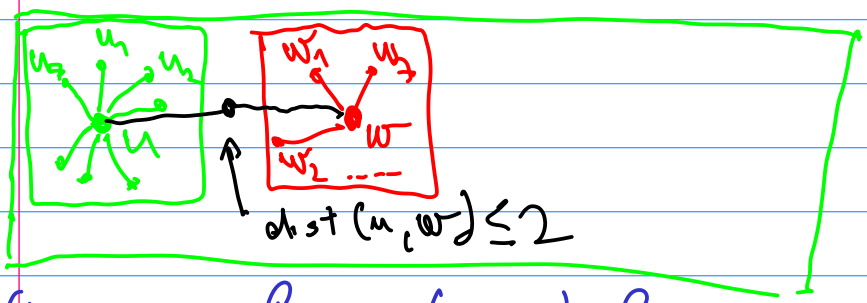
popíšeme vektory $w \in \underbrace{Im(G)}_{\text{lineární}} \subseteq \mathbb{Z}_2^7$ podprostor dim. 4

$C := Im(G)$ množina kódových slov kódu s maticí G

Tvrzení: $\nexists u \neq w$ $\quad dist(u,w) \geq 3$

$\uparrow \quad \exists$ $\quad \uparrow$ #souřadnic i kde se $u_i \neq w_i$

C



$u, w \in C \Rightarrow (u-w) \in C$

Tvrzení $\Leftrightarrow \forall w \in C : 3 \leq dist(w, \emptyset) = \#1$ ve slově w

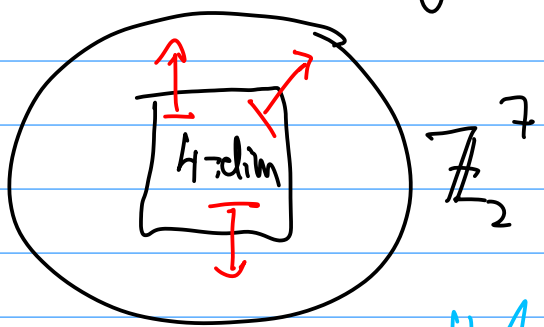
Chceme $\nexists w \in C$, $w \neq \emptyset$ obsahuje ≥ 3 bity s hodnotou 1

$H = G^{\perp}$ bazickou maticí ortogonální komplement podprostoru generovaného maticí G (řádky)

(jaká for G)

$G = 7 \times 4$

$H = 3 \times 7$



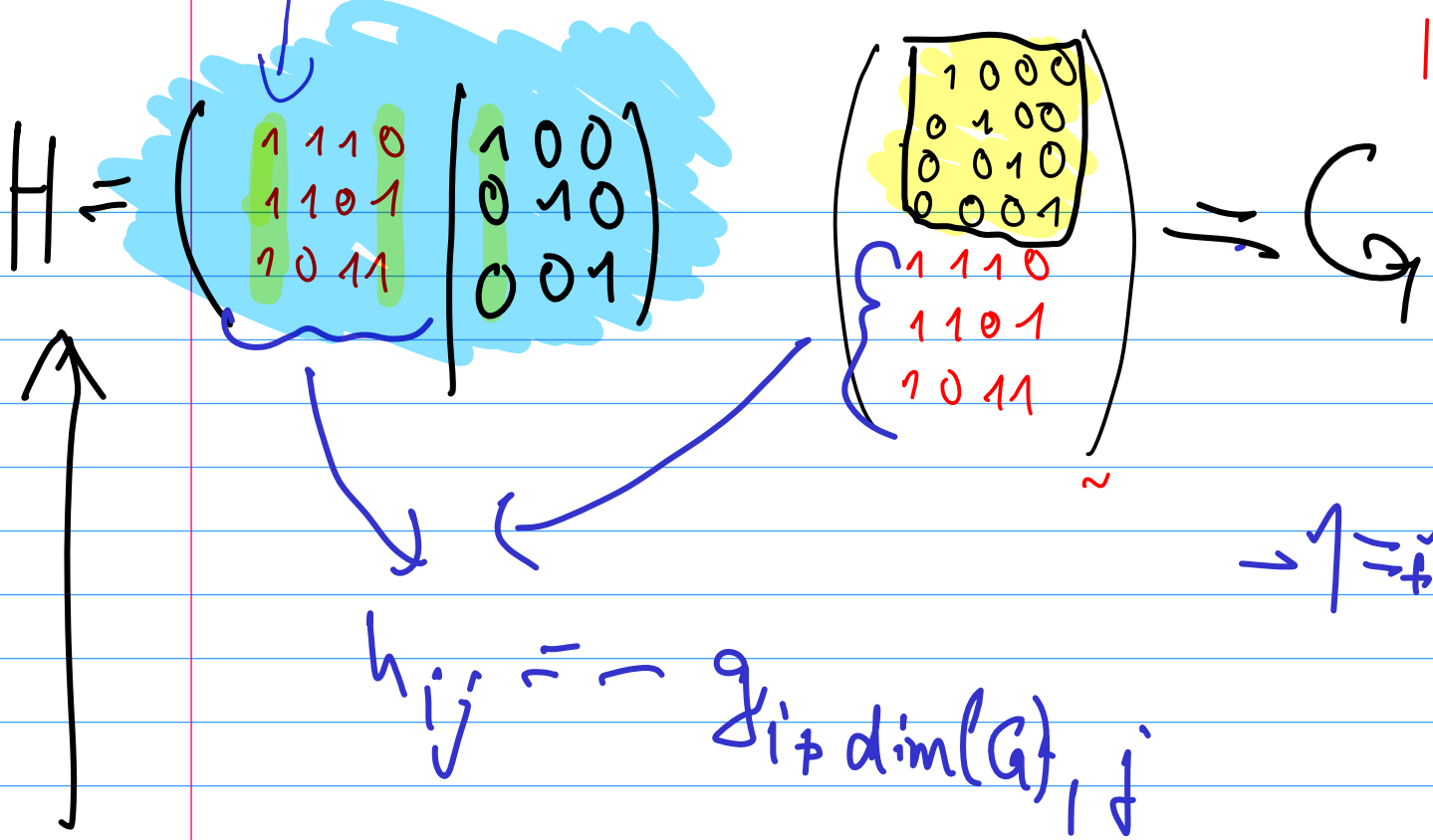
1) $H \cdot G = \begin{pmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix}$

2) $G \oplus H = \mathbb{Z}_2^7$

#1 ve $w \geq 2$

Stačí $H \equiv 7$ nenulových navzájem různých vektorů $\mathbb{Z}_2^3$

#1 ve $w \geq 3$



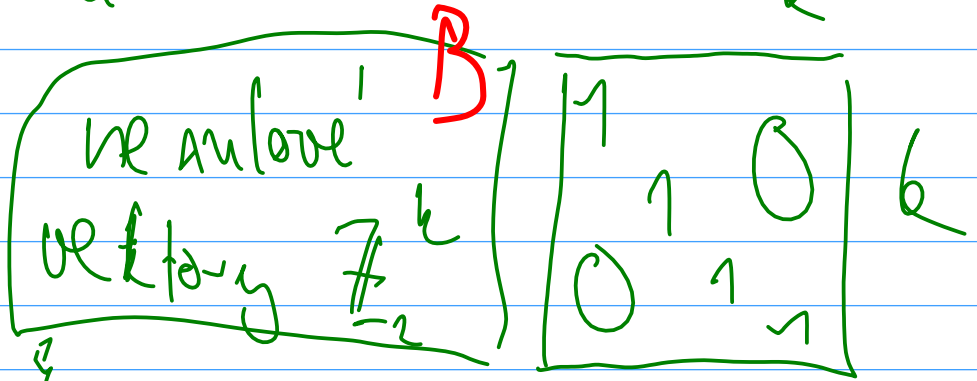
tohle je matice jejíž řádky popisují bázi $G^\perp$ aka $\ker(G)$

$\forall w \in C \quad H \cdot w = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

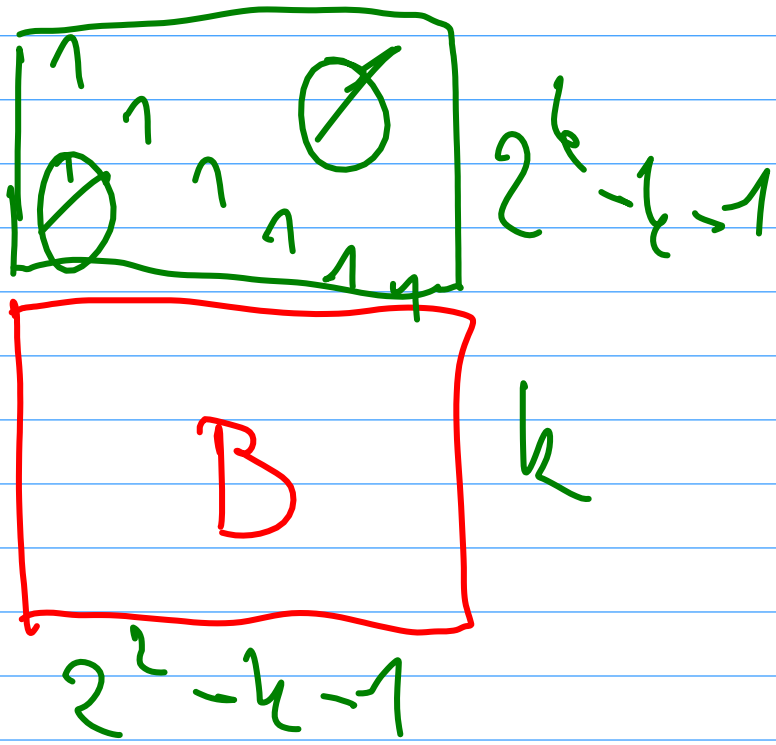
pokud $w \neq 0$ tak 1 ve sloupci w popisují lineární kombinaci sloupců H t.ž. dané sloupce se sečtou na $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

proto $w \neq 0$ má alespoň 3 souřadnice s 1 ∎

$\mathbb{Z}_2^k$ $\rightsquigarrow (2^k - 1)$ nenulových vektorů



$G :=$



Hammingova konstrukce

Z konstrukce, $\forall w \in \operatorname{Im} G$ má alespoň $w_0 \equiv \operatorname{dist}(u, w) \geq 3$

3 nenulové sousložky

H. Kód $(2^k - k - 1)$ bitů $\rightsquigarrow (2^k - 1)$ bitů

co umí opravit 1 chybný bit

Def: (n, M, d) – kód C nad tělesem $\mathbb{F}$

kód = podmnožina slov z $\mathbb{F}^n$

$\#$ slov v kódu $C = M$

$\forall u, w \in C: \; dist(u, w) \geq d$

$C \subseteq \mathbb{F}^n$, $|C| = M$

Sestrojili jsme $(7, 2^4, 3)$ – kód nad $\mathbb{Z}_2$

$\forall k \geq 2$ $(2^k - 1, 2^{2^k - k - 1}, 3)$ – kód nad $\mathbb{Z}_2$

$k = 2$

$(3, 2, 3)$ – kód

$C = \{000, 111\}$

$G = (1\ 1\ 1)$. □