Když máme kód se slovy délky n,

jak dekódovat původní zprávu?

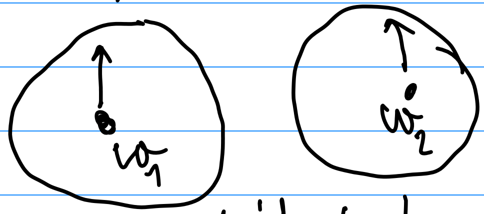
$f: q^n \to \mathcal{C} \cup$ [illegible]

slovo ⇝ $f($ slovo $) =$ původní zpráva (slovo $\in \mathcal{C}$)

chyba e ⇝ $f($slovo $+ e) =$ opravené slovo

$f($zbytek$) =$ "NEOPRAVITELNÉ"

$w_i \in \mathcal{C}$



2^n

pole[index] < kódové slovo / NEOPRAVITELNÉ

BÚNO binární kód

Př: Hammingův kód délky 7

velikost: 128

$2^{(2^k - 1)}$ $k = 7$

2^{127} ≈ MOC

CÍL: EFEKTIVNĚJI

mějme lineární kód $\mathcal{C}$ nad $\mathbb{Z}_2$ délky n

2^n slov

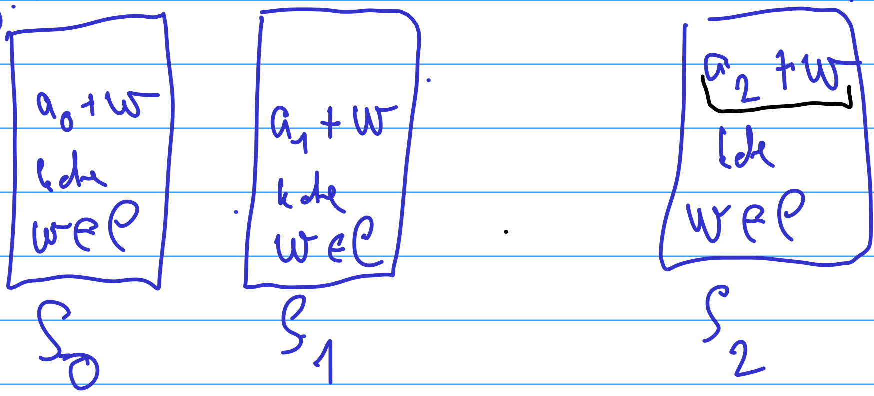
původní zpráva z $\xrightarrow{G \cdot z =}$ kódové slovo w $\xrightarrow{\text{posílání } +e}$ $w + e$ přijem ($e \in \mathbb{Z}_2^n$)

Trik: použít ověřovací matici H

$$H \cdot w = 0 \iff w \in \mathcal{C}$$

rozdělme si všechna slova délky n do $2^n/|C| = 2^{n-k}$ skupin

$a_0 := 0\ldots0$ $\quad a_1 \in \{0,1\}^n \setminus S_0$ lib. $\quad a_2 := \{0,1\}^n \setminus (S_0 \cup S_1)$



$\underbrace{a_2 + w}_{\in C} + \underbrace{w}_{\in C} = a_2$

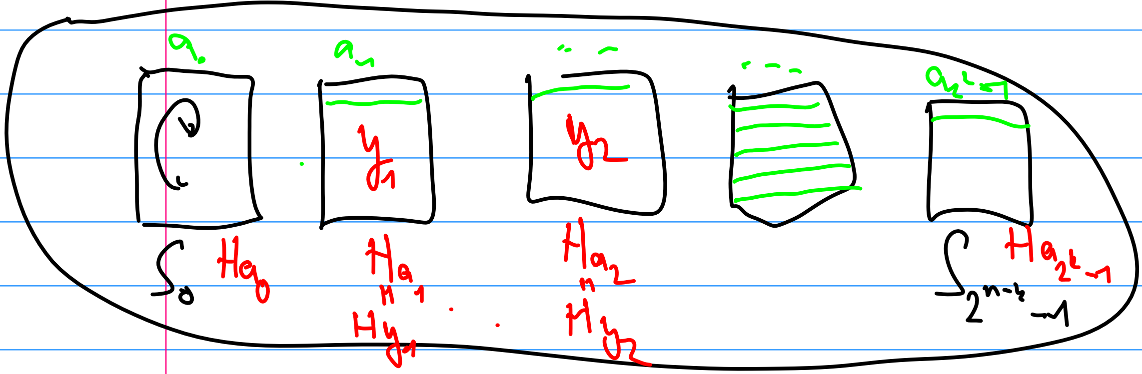
S_2 disjunktní od S_0

proč S_2 disjunktní od S_1?

Kdyby: $a_1 + w_1 = a_2 + w_2$ $\quad w_1, w_2 \in C$

$S_1 \ni a_1 + \underbrace{(w_1 - w_2)}_{\in C} = a_2$ tak $a_2 \in S_1$ ↯ s volbou a_2.

$a_k := \{0,1\}^n \setminus \bigcup_{i=0}^{k-1} S_i \qquad S_k := \{a_k + w : w \in C\}$



Mějme $w \in C$, chyba $e \in \{0,1\}^n$, položme $y := w + e$

Pak e a y jsou ve stejném bloku S_i

Dk: $S_i \ni e = a_1 + w_1 \quad w_1 \in C$

$S_i \ni y = a_2 + w_2 \quad w_2 \in C$

$a_2 + w_2 = y = w + e = w + a_1 + w_1$

$$a_2 = a_1 + \underbrace{(w + w_1 - w_2)}_{\in C}$$

nutně a_2 je ve stejné skupině jako a_1

a tedy $a_2 = a_1$

Nechť H je kontrolní matici C,

$$y, z \in S_i \iff H y^T = H z^T$$

$$\Updownarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$y - z \in C \iff H(y - z)^T = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$a_i + w_1 - a_i - w_2$

Def: Pro slovo y, Hy^T syndrom y

$\forall$ skupinu S_i, $b_i :=$ minarg váha(y), $y \in S_i$

↑ # $\neq 0$ souřadnic y

$w \rightsquigarrow y = w + e$ ($\in C$) $\boxed{Hy} \longrightarrow S_k$

$\forall$ slovo $z \in S_k$ $\quad z + y \in C$ protože $H(z + y) = 0$

po přijetí y zvolme $w := y - b_i$ kde i index skupiny syndromu Hy

pole [syndrom] = b_i

$(128 \cdot 16)$ bytů $\sim$ 2KB $\quad 2^{n-k}$

dekódovací funkce (y): return $y + pole[H_y]$

Př.: Hamming pro $l = 7$ nad $\mathbb{Z}_2$ $\rightsquigarrow$ kódová slova délky 127

$\dim |\mathcal{C}| = (2^k - 1) - k$ $\quad$ hodnost$(H) = k = 7$

Pravděpodobnost že kód "selže", nebo-li dekódujeme jiné kódové slovo, než bylo zasláno

$C \ni w \rightsquigarrow y = w + e \rightsquigarrow w' \in C \qquad w \neq w'$

Př: $(0,\dots,0)$ $\qquad e = w'$ $\qquad e$

Def: Komunikační kanál má chybovost p pokud každý bit je přenesen s pravděpodobností p nezávisle na ostatních

Pokud lineární kód umí opravit t chyb $\equiv t = \lfloor \frac{d-1}{2} \rfloor$

P_{ERR} ↙ dekódovali jsme jiné slovo než bylo odesláno

Př: $C = \{0,1\}^n \qquad P_{ERR} = 1 - (1-p)^n$

$$\overline{P_{ERR}} = \sum_{i=0}^{t} \binom{n}{i} \cdot p^i (1-p)^{n-i}$$

$$\rightsquigarrow P_{ERR} = 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}$$

4bitová zpráva $\xrightarrow{Ham}$ 7bitová kódová slova $d=3 / t=1$

Př: $p = 1/10$

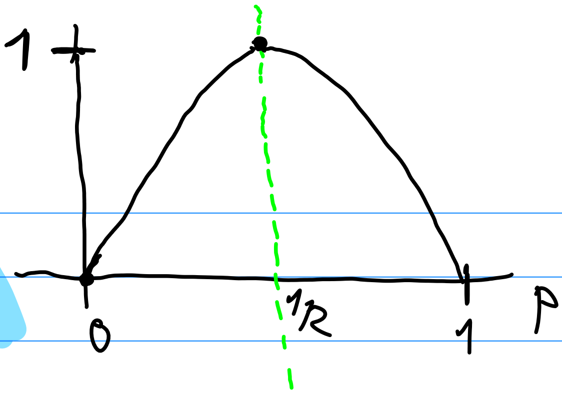
$$P_{ERR} \sim 15\%$$

4 bitová zpráva $\rightsquigarrow$ 4bitová kódová slova $d=1 / t=0$

$$P_{ERR} = 1 - \left(\frac{9}{10}\right)^4 > 34\%.$$

Binární entropie $\equiv$ kolik bitů je potřeba pro "zachycení" náh.

velikosti, např. $P_{ERR}(p)$



$H(p) := -p\log_2(p) - (1-p)\cdot\log_2(1-p)$

$p = i/n$ $\quad \frac{\#\text{slov délky } n \text{ s } i \text{ 1kami}}{2^n} \approx \frac{2^{H(p)\cdot n}}{2^n}$

kapacita

$$n\cdot C(p) = n - nH(p) = n\left(1 + p\log_2 p + (1-p)\cdot\log_2(1-p)\right)$$

horní mez DATA — ŠUM

$$C(p) := 1 + p\log_2 p + (1-p)\cdot\log_2(1-p)$$

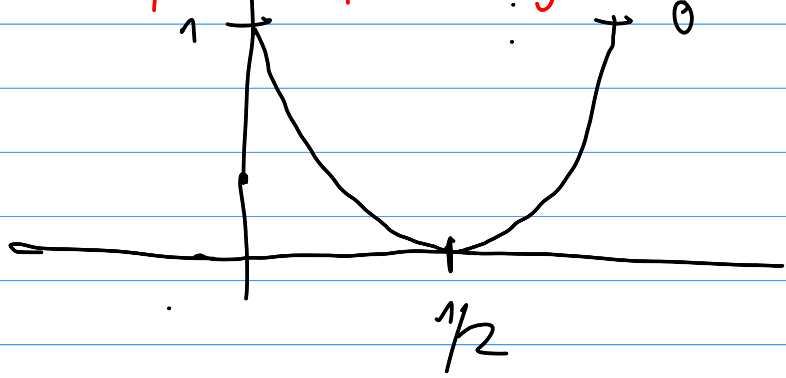
Věta (Shannon): $\forall p < 1/2$, $\forall \varepsilon > 0$, $\exists n \in \mathbb{N}$

a lineární kód $\mathcal{C}$ délky n t.ž. $\frac{\dim \mathcal{C}}{n} > C(p) - \varepsilon$

a zároveň $P_{ERR}(p) < \varepsilon$

"existuje, až na ε, nejlepší možný kód opravující chyby $p \cdot n$"

$C(p)$



Doporučuji o kurzu Teorie informace

Idea důkazu: vezmi náhodnou (kontrolní) matici dimenze odpovídající "chybovosti" měřenou entropií