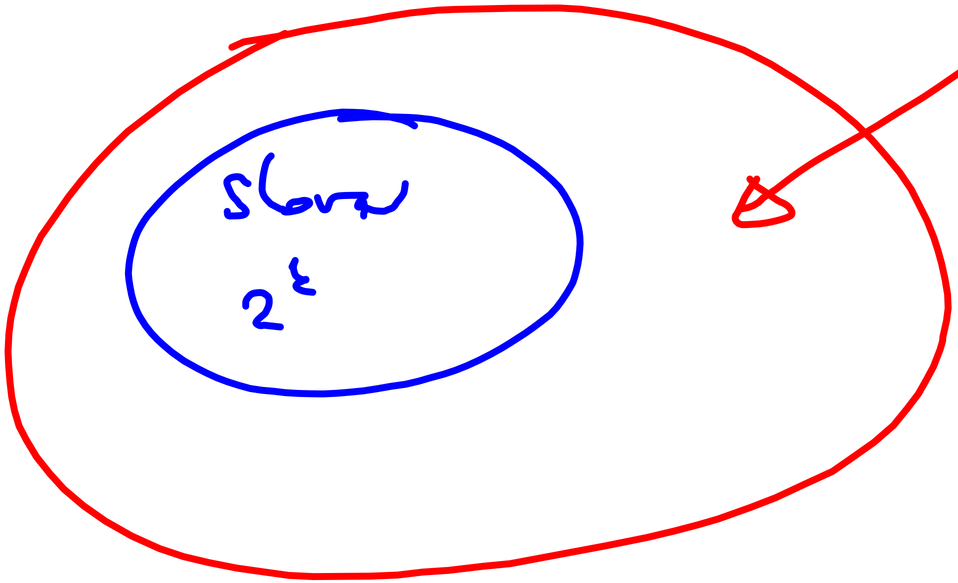
(6,3) - kód

3 bity ... zpráva

3 bity ... navíc

(n,k)



2^n

kódová slova

110, 001 nedělenost 3

$\boxed{2^n - 2^k}$

$a \mapsto aaa$

$m(x) \longleftrightarrow \underbrace{10101}$

$\parallel$

$1 + x^2 + x^4$

(n, k) – kód zpráva o k bitech $(m(x))$

$\downarrow$

$(v(x))$ kód o $k + (n-k)$ bitech

$v(x) = x^{n-k} m(x) + r(x)$ ← zbytek po dělení! $x^{n-k} m(x) / p(x)$

$p(x) = \underbrace{1 + x + x^3}$ $\boxed{(6,3)\text{ - kód}}$

$m(x) = 1 + x^2$ (zpráva 101)

$v(x) = \underbrace{x^5 + x^3} + r(x) = x^5 + x^3 + x^2$

$\Rightarrow m(x) \sim \underbrace{00}\,\underbrace{1101}$

4

$(x^5 + x^3) : (x^3 + x + 1) = x^2$

$x^5 + x^3 + x^2$

$-x^2$

$\sim \mathbb{Z}_2 ; \; -x^2 = x^2$

$$g: (\mathbb{Z}_2)^k \longrightarrow (\mathbb{Z}_2)^n$$

$$g(u+v) = g(u) + g(v)$$

$$g(\alpha u) = \alpha\, g(u)$$

$$\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \dots$$

$$G = \underbrace{n\left\{\begin{pmatrix} \cdot & \cdots & \\ \vdots & & \\ & & \end{pmatrix}\right.}_{k} \begin{pmatrix} \vdots \\ \vdots \end{pmatrix} = \left.\begin{pmatrix} \\ \\ \end{pmatrix}\right\} n$$

$$g(v) = G \cdot v$$

$\mu = C_n(v)$: $\quad u(x) = \underbrace{x^{n-k}\, v(x)}_{\%} + r(x)$

$r(x)$: zbytek dělení $\%$ $p(x)$

zbytek po dělení v r

(6, 3) kód $\quad p(x) = 1 + x + x^{3}$

$v(x) = 1$, $\quad v(x) = x$, $\quad v(x) = x^2$

$\% = x^3$

$$x^3 : (x^2 + x + 1) = x + 1$$

$$\begin{array}{l} x^3 + x^2 + x \\ \hline -x^2 - x \\ -x^2 - x - 1 \\ \hline 1 \end{array}$$

$r = 1$

první řádek: $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ ...

$$H = \begin{pmatrix} I_{n-k} & P \end{pmatrix} \qquad P = \underbrace{\left.\phantom{\begin{matrix} a \\ a \end{matrix}}\right\} n-k}_{k}$$

$$h : (\mathbb{Z}_2)^n \longrightarrow (\mathbb{Z}_2)^{n-k}$$

$$(\mathbb{Z}_2)^k \xrightarrow{g} (\mathbb{Z}_2)^n \xrightarrow{h} (\mathbb{Z}_2)^{n-k}$$

$$\ker h = \operatorname{Im} g$$

$$h \circ g : \mathbb{Z}_2^k \to \mathbb{Z}_2^{n-k}$$

$$H \cdot G = \left(I_{n-k} \; P \right) \begin{pmatrix} P \\ I_k \end{pmatrix} =$$

$$= I_{n-k} P + P I_k$$

$$= P + P = 0$$

$$\ker h \supset \operatorname{Im} g$$

$$|\ker h| = \frac{|\mathbb{Z}_2^n|}{|\operatorname{Im} g|} = \frac{2^n}{2^{n-k}} = 2^k$$

$V = \operatorname{tan} h$

symbol u

$$\boxed{u + V}$$