Př.1: $p(x) = 1+x$

(n, n−1)-kód kontroly parity (?)

$v(x) = q(x)\cdot p(x) = q(x)\cdot(1+x)$

$p(1) = 0 \Rightarrow 1$ je kořenem $v(x) \in \mathbb{Z}_2[x]$

tzn. $v(x)$ má sudý počet koef. $= 1$.

Př.2: $p(x) = 1+x+x^2$

$n=3, k=1$ (3,1) kód

kódujme: $1\cdot x^{n-k} = 1\cdot x^2 \equiv 1+x \pmod{p(x)}$

$m(x) = 1$, $r(x)$

$v(x) = 1\cdot x^2 + r(x) = 1+x+x^2$ kód: 111

$m(x) = 0$: $0\cdot x^2 = 0$

$v(x) = 0 = 0+0x+0\cdot x^2$ kód: 000

3 27-15:50

Uvažme polynom $p(x) = 1+x+x^2$ pro $n = 5$, $k = 3$. Kódovými slovy jsou

kódujme 011, tj. $m(x) = x+x^2$

$v(x) = x^2\cdot m(x) + r(x)$, kde

$r(x)$ je zbytek po dělení $x^2\cdot m(x)$ polynomem $p(x)$:

$(x^4+x^3) : (x^2+x+1) = x^2+1$

$-(x^4+x^3+x^2)$

x^2

$-(x^2+x+1)$

$x+1$ zb.

Tedy $r(x) = 1+x$, kódové slovo je $v(x) = x^4+x^3+x+1$, tj.

11011

3 27-16:26

Primitivní polynom:

$p(x)$ ireducibilní nad $\mathbb{Z}_2$

$p(x) \mid x^{2^m-1} - 1$

a nedělí $x^k - 1$ pro $k < 2^m - 1$

Pozn.: $p(0) \neq 0$

3 27-16:34

Platí: prim. polynomů stupně n nad $\mathbb{Z}_2$ je právě

$$\frac{\varphi(2^n-1)}{n}$$

$n=3$: $\frac{\varphi(7)}{3} = 2$

$n=6$: $\frac{\varphi(63)}{6} = \frac{\varphi(7)\cdot\varphi(9)}{6} = 6$

3 27-16:37

Dk vlastnosti o prim. polynomech:

Uvažme výsledek přenosu $u(x) = v(x) + e(x)$

Rozpoznáme chybu $\Leftrightarrow p(x) \nmid u(x)$

$\Leftrightarrow p(x) \nmid e(x)$

• Jedna chyba v přenosu znamená, že $e(x) = x^i$, $i \in \{0,1,\dots,n-1\}$

To, že dojde k chybě poznáme, neboť $p(x) \nmid x^i$

[0 není kořen $p(x)$]

• Dvě chyby: $e(x) = x^i + x^j$, $i,j \in \{0,1,\dots,n-1\}$, $i<j$

$p(x) \mid e(x) \Leftrightarrow p(x) \mid x^i(1+x^{j-i})$

ale $p(x) \nmid x^i$, $p(x)$ je ired.

$\Rightarrow p(x) \mid 1+x^{j-i}$, spor s def. prim. pol.

$j-i \le n-1 < 2^m-1$

$x^k - 1$

3 27-16:40

Úvod do kódování — Pár slov o šifrách

Věta

Každý polynomiální (n, k)–kód je lineární kód.

Dk: ukážeme, že polynomiální kód udává lineární zobrazení $g: \mathbb{Z}_2^k \to \mathbb{Z}_2^n$

(i) $u \in \mathbb{Z}_2^k$, $a \in \mathbb{Z}_2$: $g(a\cdot u) = a\cdot g(u)$

$a=0$: $g(0) = 0$ ✓

$a=1$: $g(u) = g(u)$ ✓

(ii) $u \in \mathbb{Z}_2^k$, $v \in \mathbb{Z}_2^k$: $g(u+v) = g(u) + g(v)$

$g(u) = x^{n-k}\cdot u(x) + r_u(x)$, kde

$x^{n-k}\cdot u(x) = q_u(x)\cdot p(x) + r_u(x)$

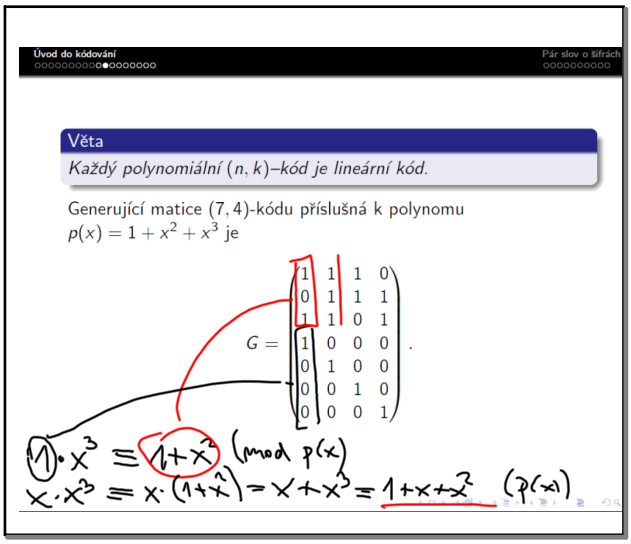
$g(v) = x^{n-k}\cdot v(x) + r_v(x)$, kde ...

Pak ale $g(u+v) = x^{n-k}(u(x)+v(x)) + r_{u+v}(x)$

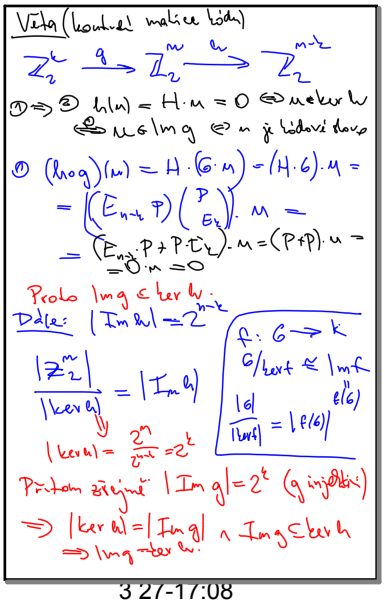
pro které zřejmě $r_{u+v}(x) = r_u(x) + r_v(x)$

□

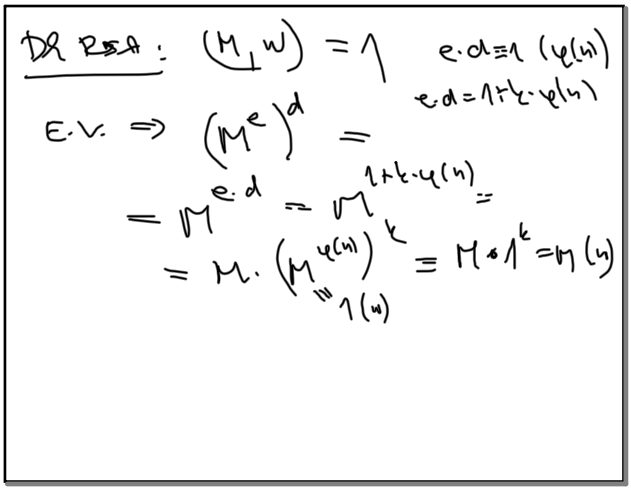
3 27-16:56



3 27-17:03



3 27-17:08



3 27-17:37