

Pr. 1:  $p(x) = 1+x$   
 $(n, n-1)$ -kód kontrolní parity (?)  
 $r(x) = q(x) \cdot p(x) = q(x) \cdot (1+x)$   
 $p(1) = 0 \Rightarrow 1$  je kořenem  $r(x) \in \mathbb{Z}_2[x]$   
 tj.  $r(x)$  má sudý počet koef. = 1.  
 Pr. 2:  $p(x) = 1+x+x^2$   
 $n=3, k=1$  (3,1) kód  
 kódujeme:  $1 \cdot x^{n-k} = 1 \cdot x^2 \equiv 1+x \pmod{p(x)}$   
 $m(x) = 1 \Rightarrow r(x) = 1 \cdot x^2 + r(x) = 1+x+x^2$  kód: 111  
 $m(x) = 0 \Rightarrow 0 \cdot x^2 = 0$   
 $r(x) = 0$  kód: 000  
 $= 0+0x+0 \cdot x^2$

3 27-15:50

Uvažme polynom  $p(x) = 1+x+x^2$  pro  $n=5, k=3$ .  
 Kódovými slovy jsou  
 kódujeme 011, tj.  $m(x) = x+x^2$   
 $r(x) = x^2 \cdot m(x) + r(x)$ , kde  
 $r(x)$  je zbytek po dělení  $x^2 \cdot m(x)$   
 polynomem  $p(x)$ :  
 $(x^3+x^4) : (x^2+x+1) = x^2+1$   
 $-(x^3+x^2+x)$   
 $-(x^2+x+1)$   
 $-(x^2+x+1)$  zb.  
 Tedy  $r(x) = 1+x$  kódové slovo je  
 $r(x) = x^3+x^2+x+1$   
 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

Pr. 1. prim. polynomi 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

Dě vĕty o prim. polynomech:  
 Uvažme vĕstřední přenos  $u(x) = r(x) + d(x)$   
 Rozpoznáme dĕln  $\Leftrightarrow p(x) \mid u(x)$   
 $\Leftrightarrow p(x) \mid e(x)$   
 • Jedna dĕln  $n$  přenos znamená, že  
 $e(x) = x^i, i \in \{0, 1, \dots, n-1\}$   
 To je dĕln  $\Leftrightarrow$  dĕlní pravidlo  $p(x) \mid x^i$   
 [0 není kořen  $p(x)$ ]  
 • Dvě dĕly:  $e(x) = x^i + x^j, i, j \in \{0, 1, \dots, n-1\}$   
 $p(x) \mid e(x) \Leftrightarrow p(x) \mid x^i(1+x^{j-i})$   
 ale  $p(x) \nmid x^i, p(x)$  je irred.  
 $\Rightarrow p(x) \mid 1+x^{j-i}$ , spor  
 $j-i \leq n-1 < 2^m-1$   
 $x^2-1$

3 27-16:40

Vĕta  
 Každý polynomiální  $(n, k)$ -kód je lineární kód.  
 Dĕ: uĕtíme ěe polynomiální kód udĕlná  
 lineární zobrazení  $g: \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2^n$   
 (i)  $m \in \mathbb{Z}_2^k, a \in \mathbb{Z}_2: g(a \cdot m) = a \cdot g(m)$   
 $a=0: g(0) = 0 \checkmark$   
 $a=1: g(m) = g(m) \checkmark$   
 (ii)  $m, n \in \mathbb{Z}_2^k, p \in \mathbb{Z}_2^k: g(m+n) = g(m) + g(n)$   
 $g(m) = x^{n-k} \cdot u(x) + r_n(x)$ , kde  
 $x^{n-k} \cdot u(x) = q_n(x) \cdot p(x) + r_n(x)$   
 $g(n) = x^{n-k} \cdot v(x) + r_n(x)$ , kde ...  
 Pak ale  $g(m+n) = x^{n-k}(u(x)+v(x)) + r_{m+n}(x)$   
 potom zĕjme  $r_{m+n}(x) = r_n(x) + r_n(x)$

3 27-16:56

Uvod do kódování

Pár slov o šířích

**Věta**

Každý polynomiální  $(n, k)$ -kód je lineární kód.

Generující matice  $(7, 4)$ -kódu příslušná k polynomu  $p(x) = 1 + x^2 + x^3$  je

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

$x \cdot x^3 \equiv 1 + x^2 \pmod{p(x)}$   
 $x \cdot x^3 \equiv x \cdot (1 + x^2) = x + x^3 \equiv 1 + x + x^2 \pmod{p(x)}$

3 27-17:03

**Věta** (kontrolní matice kódu)

$$\mathbb{Z}_2^k \xrightarrow{g} \mathbb{Z}_2^n \xrightarrow{h} \mathbb{Z}_2^m$$

$h(u) = H \cdot u = 0 \Leftrightarrow u \in \ker h$   
 $\Leftrightarrow u \in \text{Im } g \Leftrightarrow u$  je kódová slovo

$(h \circ g)(u) = H \cdot (G \cdot u) = (H \cdot G) \cdot u = 0$   
 $= \begin{pmatrix} E_n + P \\ 0 \end{pmatrix} \cdot u = \begin{pmatrix} E_n + P + P^T \cdot L \\ 0 \end{pmatrix} \cdot u = (P + P^T) \cdot u = 0$

Proč  $\text{Im } g \subseteq \ker h$ ?

Dále:  $|\text{Im } g| = 2^k$

$f: G \rightarrow K$   
 $G/\ker f \cong \text{Im } f$   
 $|G| = |\ker f| \cdot |\text{Im } f|$   
 $|\ker f| = \frac{2^n}{2^k} = 2^t$

Přitom zřejmě  $|\text{Im } g| = 2^k$  (g injektivní)

$\Rightarrow |\ker h| = |\text{Im } g| = 2^k$  a  $\text{Im } g \subseteq \ker h$   
 $\Rightarrow \text{Im } g = \ker h$

3 27-17:08

DR RSA:  $(M, u) = 1 \quad e \cdot d \equiv 1 \pmod{\varphi(n)}$   
 $e \cdot d = 1 + k \cdot \varphi(n)$

E.v.  $\Rightarrow (M^e)^d = M^{e \cdot d} = M^{1 + k \cdot \varphi(n)} = M \cdot (M^{\varphi(n)})^k = M \cdot 1^k = M \pmod{n}$

3 27-17:37