

7. demonstrační cvičení \* kódu #převodů zpr. n > k

Polynomiální kód generovaný polynomelem  $p(x)$  je  $(n, k)$ -kód jehož slova jsou polynomy  $m(x)$  modulo  $n$  dělitelné  $p(x)$ . Zpráva  $m(x)$  je zakódována jako  $v(x) = r(x) + x^{n-k}m(x)$ , kde  $r(x)$  je zbytek po dělení polynomu  $x^{n-k}m(x)$  polynomelem  $p(x)$ .

Pozor, konvence: Zprávu  $b_0b_1 \dots b_{k-1}$  reprezentujeme polynomelem  $m(x) = b_0 + b_1x + \dots + b_{k-1}x^{k-1}$ . nad  $\mathbb{Z}_2$

Příklad 1. Zakódujte zprávu 1101 pomocí  $(9, 4)$  kódu generovaného polynomelem  $1+x+x^2$ .  $n=4, k=2$

$p(x) \dots$  polynom stupně  $n-k$

1101  $\dots 1 + 1 \cdot x + 0 \cdot x^2 + 1 \cdot x^3 = 1 + x + x^3$

Kódujeme:  $x^2 \cdot m(x) = x^2 + x^3 + x^5$

4 5-15:54

Polynom  $x^2 m(x) = x^5 + x^3 + x^2$  vydělíme se zbytkem  $p(x)$ !

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

$$-(x^5 + x^4 + x^3)$$

$$\hline x^4 + x^2$$

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

$$\hline x^3$$

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

$$\hline x^2 + x + 1$$

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

$$\hline 0$$

$r(x) = 1 + x^2 \cdot (m(x)) = 1 + x^2 + x^3 + x^5$

101101

1

4 5-16:09

Průběh: stačí vidět jak kódovat básové polynomy  $b_1, x, x^2, x^3$ :

$p(x) = x^2 + x + 1$

(i)  $x^3 \cdot 1 = x^3$   
 $x^3 \div (x^2 + x + 1) = 1$   
 $-(x^2 + x + 1)$   
 $\hline x^2 + x + 1 \dots 1011000$

(jinak)  $x^3 \equiv x^2 + 1$  (mod  $p(x)$ )  
 neboť  $x^3 + (x^2 + 1)$  je násobek  $p(x)$

(ii)  $x^2 \cdot x = x^3 \equiv x^2 + 1$   
 $x^2 \cdot x \equiv x^2 + 1$   
 $\hline 1110100$

(iii)  $x^2 \cdot x^2 = x^4$   
 $x^4 \div (x^2 + x + 1) = x^2 + x + 1$   
 $-(x^4 + x^3 + x^2)$   
 $\hline x^3 + x^2$   
 $-(x^3 + x^2 + x)$   
 $\hline x^2 + x + 1$   
 $-(x^2 + x + 1)$   
 $\hline 0$

(iv)  $x^2 \cdot x^3 = (x^2 + 1)(x^2 + 1) = x^4 + 1 = x^2 + x + 1 + 1 = x^2 + x$   
 $\hline 011:0001$

4 5-16:12

$G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$   $n=7, k=4$

generující matice (kód zprávy z  $\mathbb{Z}_2^4$ )  
 je  $G \cdot z$

$P = (n-k)/k = 3/4$

$H = (E_{n-k} P) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$

Pozn: platí např.  $H \cdot (0110001)^T = (0000)^T$

4 5-16:29

Příklad 3. a) Určete generující matici a matici kontroly parity pro lineární kód  $(9, 4)$  generovaný polynomelem  $1 + x^2 + x^4 + x^5$ .

b) Vypočítejte část tabulky syndromů a vedoucích reprezentantů pro tento kód. Kolik bude mít rádků?

c) Jaký nejvyšší počet chyb detekuje/opravuje tento kód?

d) Dekódujte slova 100110010, 100100101, 111101100 a 000111110.

$G \dots$  typu  $n/k$  (zde 9/4)

$H \dots$  typu  $n-k/n$  (zde 5/9)

syndromy jsou  $H \cdot v$  pro  $v \in \mathbb{Z}_2^9$

4 5-16:35

a)  $p(x) = 1 + x^2 + x^4 + x^5$  kód  $(9, 4)$

$1 \cdot x^5 \equiv 1 + x^2 + x^4$  ( $p(x)$ )  
 $101011000$

$x \cdot x^5 \equiv x(1 + x^2 + x^4) = x + x^3 + (1 + x^2 + x^4) = 1 + x + x^2 + x^3 + x^4$   
 $111110100$

$x^2 \cdot x^5 \equiv x^2(1 + x^2 + x^4) = x^2 + x^4 + (1 + x + x^2 + x^3 + x^4) = 1 + x + x^3$   
 $110100010$

$x^3 \cdot x^5 \equiv x^3(1 + x^2 + x^4) = x^3 + (1 + x^2 + x^4) + (1 + x + x^2) = x + x^2 + x^4$   
 $011010001$

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

4 5-16:47

b) tabulka bude mít  $2^5$  řádků, v každém  $2^{5-2} = 16$  prvků  $\mathbb{Z}_2^3$

00000 ..... 00000000 =  $m_1$  ( $H \cdot m_1 = \vec{0}$ )  
 01101  $H \cdot (00000001)^T$  "chyba v posledním"  
 10000  $H \cdot (10000000)^T$  "chyba v 1. bitu"  
 ...  
 10111  $H \cdot (00000001)^T$

9 syndromů pro dle  $n=1$  bitů

kód opravy 1 chyby, detekuje 2 nebo 3 chyby  
 ale už ve 4 chyby: slova

00000000 a 100001110  
 (= 1. řádek H)

mají stejný syndrom

Pozn:  
 $H \cdot (000100110)^T = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

Polud by m přenosu 00000000 došlo ke 3 chyby,  
 takže to poznáme, Syndrom není (00000)<sup>T</sup>

4 5-16:54

an d) dekodujte

$m$	10010010	100100101	11101100	00011110
$Hm$	01000	00000	10111	10011
ved. repr.	010...0	0...0	0...011	00101000
kód	110110010	100100101	111011111	001010110
zpráva	0010	0101	1111	0110

kód = repr + m

4 5-17:09

$P=4$  RSA  $p=23, q=31$

$n=23 \cdot 31 = 713$   
 $\varphi(n) = 22 \cdot 30 = 660$   
 $e=17, 17a \equiv 1 \pmod{660}$

Řešení:  $660 = 17 \cdot 38 + 14$   
 $17 = 1 \cdot 14 + 3 \quad \begin{matrix} 17 = 4 \cdot 3 + 2 \\ 3 = 1 \cdot 2 + 1 \end{matrix}$

$1 = 3 - 2 = 3 - (14 - 6 \cdot 3) = 5 \cdot 3 - 1 \cdot 14 =$   
 $= 5(17 - 14) - 14 = 5 \cdot 17 - 6 \cdot 14 =$   
 $= 5 \cdot 17 - 6(660 - 17 \cdot 38) = -6 \cdot 660 + 235 \cdot 17$

$d = 233$

$m=12$  šifra  $C = m^e = 12^{17} \pmod{713}$   
 $= 12^{(40001)_2} = 12 \cdot 12^6 =$   
 $= 12 \cdot ((12^2)^4)^2 = 538 \pmod{713}$

$m = 538^{233}$

4 5-17:14

The screenshot shows the Sage Notebook interface. The main content area contains a table with the following entries:

Integer (42, 47)
(-19, 17, 1)
Mod (-19, 47) * 45
Mod (38, 47)
Mod (538, 713) * 233
Mod (12, 713)

At the bottom, there is an input field with the number 1 and an 'evaluate' button.

4 5-17:35

$P=5, p=23, q=5$

např.  $a=13$

$5^{13} \equiv 21 \pmod{23}$        $5^{20} \equiv 12 \pmod{23}$

DLP neuvinná metoda  $\approx 21$  od 13

$12^{13} \equiv 6 \pmod{23}$        $21^{20} \equiv 6 \pmod{23}$

$K=6$

4 5-17:35