7. demonstrační cvičení

Polynomiální kód generovaný polynomem $p(x)$ je (n, k)-kód jehož slova jsou polynomy stupně menšího než 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 $x^{n-k}m(x)$ polynomem $p(x)$.

Pozor, konvence: Zprávu $b_0b_1 \dots b_{k-1}$ reprezentujeme polynomem $m(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1}$.

Příklad 1. *Zakódujte zprávu 1101 pomocí binárního kódu generovaného polynomem* $1 + x + x^3$.

4 5-15:54

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

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

$-(x^5 + x^2 + x^3)$

x^3

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

$x^2 + x$

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

1

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

101101

4 5-16:09

Příp.: stačí vědět jak kódovat báze. polynomy $1, x, x^2, x^3$:

$p(x) = x^3 + x^2 + 1$.

(i) $x^3 \cdot 1 = x^3$

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

$-(x^3 + x^2 + 1)$

$x^2 + 1$ ... 101 1000

(jinak: $x^3 \equiv x^2 + 1 \pmod{p(x)}$

neboť $x^3 + (x^3 + x^2 + 1)$ je násobek $p(x)$)

(ii) $x^3 \cdot x = x^4 \equiv (x^2 + 1) \cdot x = x^2 + x + 1 \pmod{p(x)}$

1110 0100

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

$-(x^5 + x^4 + x^2)$

$x^4 + x^2$

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

$x^3 + x^2 + x$

$-(x^3 + x^2 + 1)$

$x + 1$

1110 0010

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

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

0111 0001

4 5-16:12

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

$n = 7, k = 4$

E_k

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

$H = (E_{mk} \mid P) =$

1 0 0 1 1 1 0
0 1 0 0 1 1 1
0 0 1 1 1 0 1

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 polynomem*

$$1 + x^2 + x^4 + x^5.$$

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

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

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

G ... typu n/k (zde 9|4)

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

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

$\in \mathbb{Z}_2^5$

4 5-16:35

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

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

1010 1000

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

1111 0100

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

1101 0010 $\approx 1 + x + x^3$

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

0110 1000 $\approx x + x^2 + x^4$

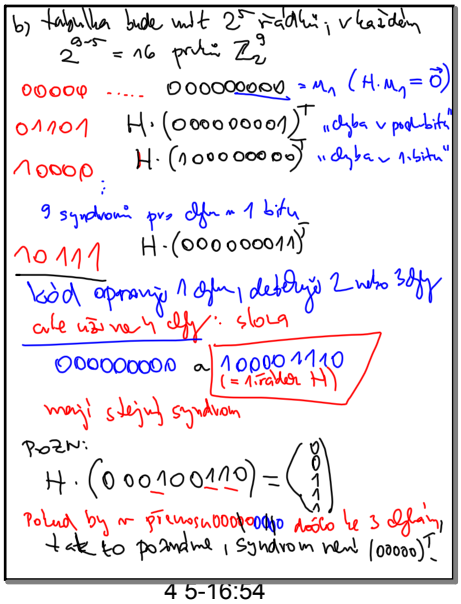
$G =$

1 1 1 0
0 1 1 1
1 1 0 1
0 1 1 0
1 1 0 0
1 0 0 0
0 1 0 0
0 0 1 0
0 0 0 1

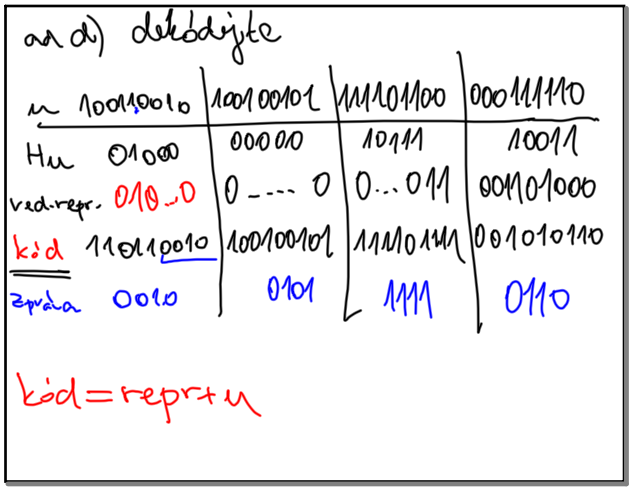
, $H =$

1 0 0 0 0 1 1 1 0
0 1 0 0 0 1 1 1 1
0 0 1 0 0 1 1 0 1
0 0 0 1 0 0 1 1 0
0 0 0 0 1 1 1 0 1

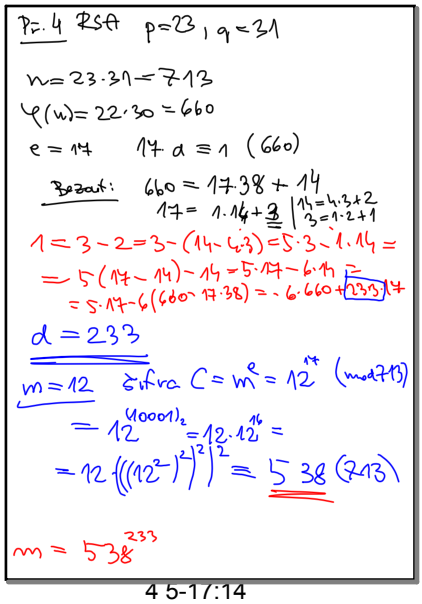
4 5-16:47



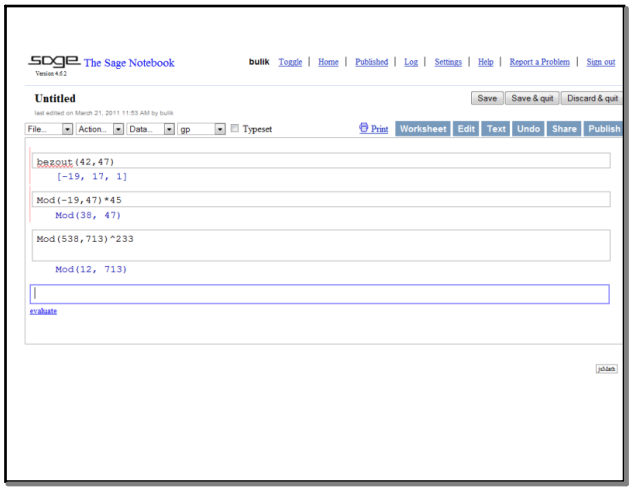
4 5-16:54



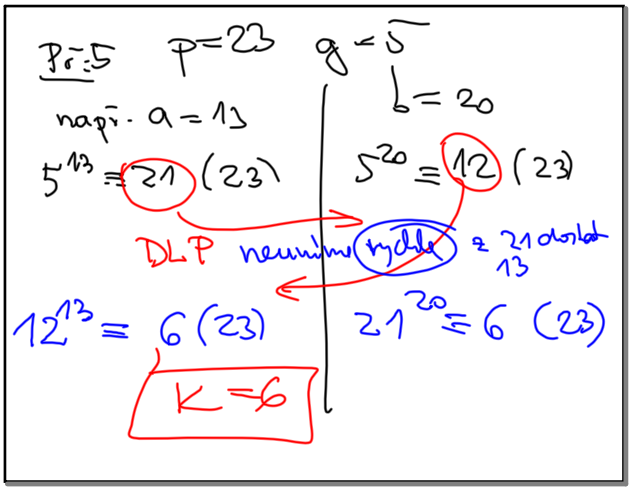
4 5-17:09



4 5-17:14



4 5-17:35



4 5-17:35