

V hódově slovo  
 u obdržení správné  
 detekce:  
 $|u-v| \leq r \Rightarrow u$  vová hódově slovo  
 max. r dých opravování:  
 $|u-v| \leq r \Rightarrow |u-w| \geq r+1$   
 (jinak by  $|v-w| \leq 2r$ )

4 11-13:58

polynom nad  $\mathbb{Z}_2$   
 $m(x) = b_0 + b_1x + \dots + b_k x^k$   
 kde  $b_0, b_1, \dots, b_k \in \mathbb{Z}_2$   
 polynom  $\neq$  polynomiální funkce  
 $x(x+1)$  jako funkce:  $0 \mapsto 0$   
 $1 \mapsto 0$   
 $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$   
 $x(x+1) \neq 0$  jako polynom  
 $=$  jako funkce  $\neq$  nekone  
 $101 \dots 1 + 0x + 1x^2$

4 11-14:14

$(x^3 + x^2 + x) : (x^2 + x + 1) = x^2 + x + 1$   
 $\frac{x^3}{-(x^2 + x^2 + x)}$   
 $\frac{x^2 + x}{-(x^2 + x + 1)}$   
 $\frac{1}{1}$   
 Trzeme: dany  $m, p \in \mathbb{Z}_2[x]$   
 $\exists! q, r: m(x) = p(x) \cdot q(x) + r(x)$   
 $\deg r(x) < \deg p(x)$   
 $p | m_1$  jestliže  $r = 0$   $\leftarrow$  stupen 0  
 $m(x) = (x+1)q(x) + r = \text{číslo}$   
 $m(1) = 0 \cdot q(1) + r \Rightarrow r = m(1)$   
 $(x+1) | m(x) \Leftrightarrow m(1) = 0$

4 11-14:19

$p(x) = 1 + x + x^2$   
 $m(x) = 1 + x^2$   
 $v(x) = r(x) + x^2(1 + x^2)$   
 st. 1  
 $r(x) = \text{zbytek po dělení}$   
 $x^2(1 + x^2) = x^2 + x^4; 1 + x + x^2$   
 $= 1$   
 $v(x) = 1 + x^2(1 + x^2)$

4 11-14:29

$p(x) | 1 + x^{2^m - 1}$   $m = \deg p$   
 $p(x) \nmid 1 + x^k$   $k < 2^m - 1$   
 ireducibilní =  
 nemá součin polynomů  
 menšího stupně  
 + nemá konstanty  
 dělení se zbytekem  
 $\rightarrow$  Eukleidův algoritmus  
 $\rightarrow$  Bezoutova lemma  
 $\rightarrow m(x) | p(x)q(x), (m(x), p(x)) = 1$   
 $\Rightarrow m(x) | q(x)$

4 11-14:39

$p(x) | 1 + x^{2^m - 1}$   $p(x)$  ired. stupně  $m$   
 $p(x) \nmid 1 + x^k, k < 2^m - 1$   
 dělení jednoduchých dých:  
 $u(x) = v(x) + e(x)$   
 $e(x) = x^i$  ... odpovídá  $0 \dots 010 \dots 0$   
 chceme:  $p(x) + e(x) = x^i, i < 2^m - 1$   
 kdyby ano, tak  $p(x) | x^{2^m - 1}$   
 a z  $p(x) | 1 + x^{2^m - 1} \Rightarrow p(x) | 1$   
 $p(x) = 1$   
 dvojité dých:  
 $e(x) = x^i + x^j = x^i(1 + x^{j-i})$   $i < j$   
 chceme:  $p(x) | e(x) = x^i(1 + x^{j-i})$   
 už víme, že  $(p(x), x^i)$   
 (protože je ired. a nedělí  $x^i$ )  
 $\Rightarrow$  kdyby  $p(x) | e(x) \Rightarrow p(x) | 1 + x^{j-i}$   
 nelze podle def., protože  $j-i < 2^m - 1$

4 11-14:48

$p(x)$  nerozpočet dýchů  $e(x)$   
 $\Leftrightarrow p(x) \mid e(x)$   
 $p(x) = q(x) (1+x)$   
 $e(x) = x^1 + x^0 + x^2$   
 potom  $(1+x) \nmid e(x)$   
 protože  $e(1) = 1$   
 Důst: detekce s3 dýchů  
 $\Rightarrow$  Hammingova vzd.  $\geq 4$   
 $\Rightarrow$  opravování jedné dýchů

4 11-14:59

$$\begin{array}{r} 1 \longmapsto 1+x \quad + x^3 \\ x \longmapsto \quad x+x^2 \quad + x^4 \\ x^2 \longmapsto \quad +1+x \quad x^2+x^3 \quad + x^5 \\ \hline = 1+x+x^2 \quad + x^5 \end{array}$$

$$\begin{aligned} (110)^T &\mapsto (1, 1, 0, 1, 0, 0)^T \\ (0, 1, 0)^T &\mapsto (0, 1, 1, 0, 1, 0)^T \\ (0, 0, 1)^T &\mapsto (1, 1, 1, 0, 0, 1)^T \end{aligned}$$

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad G \cdot u = \begin{pmatrix} ? \\ ? \\ ? \\ ? \\ ? \\ u \end{pmatrix}$$

4 11-15:09

$\ker h \supseteq \text{Im } g \Leftrightarrow h(g(u)) = 0$   
 $H \cdot G \cdot u = 0$   
 toto platí, protože  $H \cdot G = 0$   
 $(G \cdot u = \begin{pmatrix} P \cdot u \\ u \end{pmatrix} \quad H \cdot G \cdot u = (P_H + P_V) \cdot u = 0)$

4 11-15:21

$$\begin{aligned} \mathbb{Z}_2^n & \xrightarrow{h} \mathbb{Z}_2^m \\ \text{im } g & \xrightarrow{h} 0 \\ \text{ker } h & \xrightarrow{h} 0 \end{aligned}$$

$$E = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$
 obdrželi správu  $w = 1010001$   
 kontrola:  $H \cdot w = 110$  s nulou  
 $\text{im } g$  - kód slova  $+0$  - w nach  
 $v$  - chyb  $\text{ker } h$  - kód slova  
 $w = v + e$  - chybě e co nejmenší  
 $= 0000000 + 1010001 = 0 + w$   
 chyb je 3 bítů  
 $= v + (w - v)$   
 vezmeme všechna možná kódová slova  $v$  a budeme hledat takové, aby  $(w-v)$  byla co nejmenší  
 $\text{im } g = \{ \text{všechna možná } v \}$   
 $= \{ G \cdot (0, 0, 0, 0)^T, G \cdot (0, 0, 0, 1)^T, G \cdot (0, 0, 1, 0)^T, G \cdot (0, 0, 1, 1)^T, \dots \}$   
 16 slov  
 ... prořítli možnosti  
 nejblíže k  $w = 1010101$   
 $>$  dýchů  $w - v = 0000100$

4 11-15:24