V kódové slovo
u obdržení zpráva
detekce: $|u-v| \le r \Rightarrow u$ není kódové slovo
max. r chyb
opravování: $|u-v| \le r \Rightarrow |u-w| \ge r+1$
(jinak by $|v-w| \le 2r$)

4 11-13:58

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

4 11-14:14

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

Věta: dány $m, p \in \mathbb{Z}_2[x]$
$\exists!\ q, r$: $m(x) = p(x) \cdot q(x) + r(x)$
$\deg r(x) < \deg p(x)$
$p \mid m$, jestliže $r = 0$
$m(x) = (x+1)\,q(x) + r$ ← stupeň 0 = číslo
$m(1) = 0 \cdot q(1) + r \Rightarrow r = m(1)$
$(x+1) \mid m(x) \iff m(1) = 0$

4 11-14:19

$p(x) = 1 + x + x^2$
$m(x) = 1 + x^2$
$V(x) = \underbrace{r(x)}_{\text{st. } 1} + x^2(1+x^2)$
$r(x)$ = 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

$p(x) \mid 1 + x^{2^m - 1}$ $m = \deg p$
$p(x) \nmid 1 + x^k$ $k < 2^m - 1$
ireducibilní =
není součin polynomů
menšího stupně
+ není konst.
dělení se zbytkem
→ Eukleidův algoritmus
→ Bezoutovo lemma
→ $m(x) \mid p(x)\,q(x)$, $(m(x), p(x)) = 1$
$\Rightarrow m(x) \mid q(x)$

4 11-14:39

$p(x) \mid 1 + x^{2^m - 1}$ $p(x)$ ired stupně m
$p(x) \nmid 1 + x^k$, $k < 2^m - 1$
detekce jednoduchých chyb:
$u(x) = v(x) + e(x)$
$e(x) = x^i$ … odpovídá $0 \dots 0\,1\,0 \dots 0$ (1 na i-tém místě)
chceme: $p(x) + e(x) = x^i$ $i < 2^m - 1$
kdyby ano, tak $p(x) \mid x^{2^m-1} + 1$
a z $p(x) \mid 1 + x^{2^m-1} \Rightarrow p(x) \mid 1$
$p(x) = 1$ ✗
dvojité chyby:
$e(x) = x^i + x^j = x^i(1 + x^{j-i})$ $i < j$
chceme: $p(x) + g(x) = x^i(1 + x^{j-i})$
víme, že $(p(x), x^i) = 1$
(protože je ired a nedělí x^i)
$\Rightarrow$ kdyby $p(x) \mid e(x) \Rightarrow p(x) \mid 1 + x^{j-i}$
nelze podle def., protože $j - i < 2^m - 1$

4 11-14:48

$p(x)$ nerozponá chybu $e(x)$
$\Leftrightarrow$ $p(x) \mid e(x)$
$p(x) = q(x)(1+x)$
$e(x) = x^i + x^j + x^k$
potom $(1+x) + e(1)$
protože $e(1) = 1$
Dále: detekce ≤ 3 chyby
$\Rightarrow$ Hammingova vzd. ≥ 4
$\Rightarrow$ opravování jedné chyby

4 11-14:59

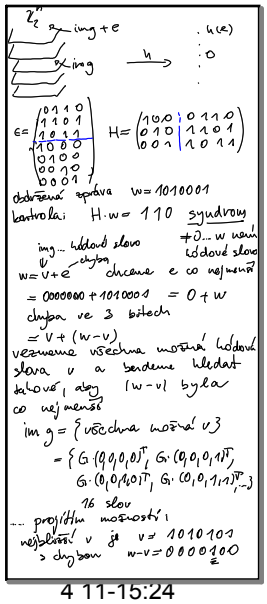
$1 \longmapsto 1+x+x^3$
$x \longmapsto x+x^2+x^4$
$x^2 \longmapsto x^2+x^3+x^5$
$+1+x+x^3$
$= 1+x+x^2+x^5$
$(1,0,0)^T \longmapsto (1,1,0,1,0,0)^T$
$(0,1,0)^T \longmapsto (0,1,1,0,1,0)^T$
$(0,0,1)^T \longmapsto (1,1,1,0,0,1)^T$

$$G = \left(\begin{array}{c} \begin{matrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{matrix} \\ \hline \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \end{array}\right) \qquad G \cdot u = \begin{pmatrix} ? \\ ? \\ ? \\ u \end{pmatrix}$$

4 11-15:09

$\ker h \supseteq \operatorname{Im} g \ (=) \ h(g(u)) = 0$
$H \cdot G \cdot u = 0$
toto platí, protože $H \cdot G = 0$
$\left(G \cdot u = \begin{pmatrix} P \cdot u \\ u \end{pmatrix} \quad H \cdot G \cdot u = (P u + P u) = 0 \right)$

4 11-15:21



4 11-15:24