20SK – Signály a kódy

Přednáška 12 – Binární cyklické kódy (17.12.2018)

Probíraná témata:

- Souvislost mezi vektorem a polynomem
- Binární aritmetika modulo N
- Kódové slovo jako binární polynom. Rotace slova (cyklický posun).
- Binární cyklický kód: vlastnosti, generující a kontrolní polynom, konstrukce generujícího a kontrolního polynomu
- Kódování a dekódování binárního cyklického kódu. Posuvné registry.
- Vztah mezi binárním lineárním kódem a binárním cyklickým kódem.
- Vztah mezi generujícím polynomem a generující maticí.

Relevantní literatura je [1, kapitoly 2 a 3], [2, kapitoly 5 a 10], [3, kapitoly 3 a 4] a [4, kapitoly III a V].

Seznam literatury

[1] Morelos-Zaragoza, R. H.: *The Art of Error-Correcting Coding*. 2nd edition, John Wiley & Sons, 2006, 263pp.

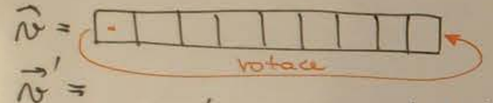
[2] Adámek, J: *Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory*. Wiley Interscience, 1991, 352 pp.

[3] Moon, T. K.: *Error Correction Coding – Mathematical Methods and Algorithms.* Wiley Interscience, 2005, 756 pp.

[4] Adámek, J: Kódování. Matematika pro vysoké školy technické, sešit XXXI. SNTL, 1989, 192 pp.

BINÁRNÍ CYKLICKÉ KÓDY

- podmnožina bin. lin. kódů



zrotováno o jeden bit je opět kódové slovo

Př: $K = \{0110, 1100, 1001, 0011\}$

→ lze realizovat pomocí HW posuvných registrů

Binární polynomy

$\vec{a} = 1001 \iff a(x) = x^3 \oplus 1$

$\vec{a} = (a_{n-1}, a_{n-2}, \dots, a_0) \Rightarrow a(x) = a_{n-1} \cdot x^{n-1} \oplus a_{n-2} \cdot x^{n-2} \oplus \dots \oplus a_1 x \oplus a_0$

→ generující polynom
  kontrolní polynom
  ⋮
} lze převést na G a H

$x^4 - 1 \equiv x^4 \oplus 1$
v binární aritmetice bez přenosu

Rotace doleva resp. doprava

$\vec{a} = 1001$ $\quad a(x) = x^3 + 1$
$\vec{a}^{(1)} = 0011$ $\quad a(x) = x + 1$
$\vec{a}^{(-1)} = 1100$ $\quad a(x) = x^3 + x^2$

zbyde $x \oplus 1$

rotace realizovat jako $x \cdot a(x)$ resp. $x^{-1} \cdot a(x)$

Př: $\vec{a}^{(1)} = x \cdot a(x) = \boxed{x^4} \oplus x$ (nemůžu reprezentovat!) $\Rightarrow x^4 \oplus x \bmod x^4 \oplus 1$

každá operace je následována modelárním dělením polynomem $x^n - 1$ $(x^4 - 1)$

Kódování a dekódování

$\vec{u}$ .... informace $\rightarrow u(x) = u_{k-1}x^k \oplus \dots \oplus u_0$

kódové slovo vzpresentováno jako

$$v(x) = u(x) \cdot g(x)$$

$g(x)$ ... generující polynom
ekvivalent generující matice

!! násobení je v mod $x^n \oplus 1$!!

dekódování probíhá jako

$$u(x) = v(x) \cdot h(x)$$

$h(x)$ ... kontrolní polynom

Vlastnosti $g(x)$ a $h(x)$

① $g(x)$ dělí $x^n \oplus 1$ beze zbytku

② $h(x) = \dfrac{x^n \oplus 1}{g(x)} \iff g(x) \cdot h(x) = x^n \oplus 1$

Příklad: $n = 7, k = 4$ $(7,4)$ kód

Zvolím: $g(x) = x^3 \oplus x \oplus 1$ $\quad \vec{g} = (0001011)$

$$(x^7 \oplus 1) : (x^3 \oplus x \oplus 1) = \underbrace{x^4 \oplus x^2 \oplus x \oplus 1}_{h(x)}$$

$$\begin{array}{r} x^7 \oplus x^5 \oplus x^4 \\ \hline x^5 \oplus x^4 \oplus 1 \\ x^5 \oplus x^3 \oplus x^2 \\ \hline x^4 \oplus x^3 \oplus x^2 \oplus 1 \\ x^4 \oplus x^2 \oplus x \\ \hline x^3 \oplus x \oplus 1 \end{array}$$

$g(x)$	=	$(0\,0\,0\,1\,0\,1\,1)$
$x \cdot g(x)$	=	$(0\,0\,1\,0\,1\,1\,0)$
$x^2 \cdot g(x)$	=	$(0\,1\,0\,1\,1\,0\,0)$
$x^3 \cdot g(x)$	=	$(1\,0\,1\,1\,0\,0\,0)$

↳ vždy jsou lineární součty

toto je G odpovídající lineárnímu kódu!

Př.: $x^4 g(x) = (0110001)$

$= x g(x) \oplus x^2 g(x) \oplus g$

Př: $g(x) = x^3 \oplus x \oplus 1$

$h(x) = x^4 \oplus x^2 \oplus x \oplus 1$

$n = 7, \; k = 4$

$\vec{u} = (u_3, u_2, u_1, u_0)$

$\vec{v} = (v_6, v_5, \dots, v_0)$

Kódujeme $\vec{u} = (0101)$

$v(x) = u(x) \cdot g(x)$

$= (x^2 \oplus 1)(x^3 \oplus x \oplus 1) =$

$= x^5 \oplus x^3 \oplus x^2 \oplus x^3 \oplus x \oplus 1 =$

$= x^5 \oplus x^2 \oplus x \oplus 1 \quad \Rightarrow \vec{v} = (0100111)$

$v(x) \cdot h(x) = (x^5 \oplus x^2 \oplus x \oplus 1)(x^4 \oplus x^2 \oplus x \oplus 1)$

$= x^9 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^6 \oplus x^4 \oplus x^3 \oplus x^2$
$\oplus x^5 \oplus x^3 \oplus x^2 \oplus x \oplus x^4 \oplus x^2 \oplus x \oplus 1$

$= x^9 \oplus x^7 \oplus x^2 \oplus 1$

Vlastnosti $g(x)$ a $h(x)$

① $g(x)$ dělí $x^n \oplus 1$ beze zbytku

② $h(x) = \dfrac{x^n \oplus 1}{g(x)} \iff g(x) \cdot h(x) = x^n \oplus 1$

Příklad: $n = 7, \; k = 4$ $(7,4)$ kód

Zvolím: $g(x) = x^3 \oplus x \oplus 1$ $\quad \vec{g} = (0001011)$

$(x^7 \oplus 1) : (x^3 \oplus x \oplus 1) = \underbrace{x^4 \oplus x^2 \oplus x \oplus 1}_{h(x)}$

$x^7 \oplus x^5 \oplus x^4$

$x^5 \oplus x^4 \oplus 1$

$x^5 \oplus x^3 \oplus x^2$

$x^4 \oplus x^3 \oplus x^2 \oplus 1$

$x^4 \oplus x^2 \oplus x$

$x^3 \oplus x \oplus 1$

$g(x)$	=	$(0\,0\,0\,1\,0\,1\,1)$
$x \cdot g(x)$	=	$(0\,0\,1\,0\,1\,1\,0)$
$x^2 \cdot g(x)$	=	$(0\,1\,0\,1\,1\,0\,0)$
$x^3 \cdot g(x)$	=	$(1\,0\,1\,1\,0\,0\,0)$

↳ vždy jsou lineárně nezávislé

Tato je G odpovídající lineárnímu kódu!

Př: $x^4 g(x) = (0110001)$

$= g(x) \oplus x \, g(x) \oplus x^2$

$g(x) = x^3 \oplus x \oplus 1$

$h(x) = x^4 \oplus x^2 \oplus x \oplus 1$

$n = 7, \; k = 4$

$\vec{u} = (u_3, u_2, u_1, u_0)$

$\vec{v} = (v_6, v_5, \dots, v_0)$

Kódujeme $\vec{u} = (0101)$

$v(x) = u(x) \cdot g(x)$

$= (x^2 \oplus 1)(x^3 \oplus x \oplus 1) =$

$= x^5 \oplus x^3 \oplus x^2 \oplus x^3 \oplus x \oplus 1 =$

$= x^5 \oplus x^2 \oplus x \oplus 1 \quad \Rightarrow \vec{v} = (0100111)$

$v(x) \cdot h(x) = (x^5 \oplus x^2 \oplus x \oplus 1)(x^4 \oplus x^2 \oplus x \oplus 1)$

$= x^9 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^6 \oplus x^4 \oplus x^3 \oplus x^2$
$\oplus x^5 \oplus x^3 \oplus x^2 \oplus x \oplus x^4 \oplus x^2 \oplus x \oplus 1$

$= x^9 \oplus x^7 \oplus x^2 \oplus 1$

Vlastnosti $g(x)$ a $h(x)$

① $g(x)$ dělí $x^n \oplus 1$ beze zbytku

② $h(x) = \dfrac{x^n \oplus 1}{g(x)} \iff g(x) \cdot h(x) = x^n \oplus 1$

Příklad: $n = 7, \; k = 4$ $(7,4)$ kód

Zvolím: $g(x) = x^3 \oplus x \oplus 1$ $\quad \vec{g} = (0001011)$

$x^7 \oplus 1 : x^3 \oplus x \oplus 1 = \underbrace{x^4 \oplus x^2 \oplus x \oplus 1}_{h(x)}$

$x^7 \oplus x^5 \oplus x^4$

$x^5 \oplus x^4 \oplus 1$

$x^5 \oplus x^3 \oplus x^2$

$x^4 \oplus x^3 \oplus x^2 \oplus 1$

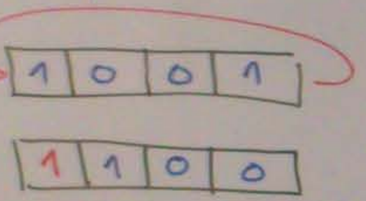
$x^4 \oplus x^2 \oplus x$

$x^3 \oplus x \oplus 1$

CYKLICKÉ KÓDY

bin. opt. kód: rotací o 1 bit doleva / doprava dostáváme opět kódové slovo

FF:



Výhoda: dobrá HW implementace v posuvných registrech (alespoň pro $d_{min} = 2$ a 3)

Kódové slovo $\vec{w} = (w_0, w_1, w_2, \dots)$ reprezentujeme jako binární polynom $w(x) = w_0 + w_1 x + w_2 x^2 + \dots$

Potřebujeme matematicky reprezentovat rotaci:

počítáme $\bmod x^n \oplus 1$

↖ zaručí, že výsledek je vždy max. n bitů

Příklad:

$\vec{w} = (0110) \Rightarrow w(x) = x \oplus x^2$ 4 bitové slovo: bity x^0, x^1, x^2, x^3

posun doprava o 2 bity: $x^2 \cdot w(x) = x^3 \oplus x^4 \bmod x^4 \oplus 1 =$

$= 1 \oplus x^3$

JAKTOŽE?

$x^3 \oplus x^4 : x^4 \oplus 1 = 1$

$x^4 \oplus 1$

$x^3 \oplus 0 \oplus 1$

$\Rightarrow x \cdot w(x)$ ... posun vpravo

$x^{-1} \cdot w(x)$ ... posun vlevo

CYKLICKÉ KÓDY

Kódování:

$u(x)$ ... otevřený text / zpráva

$$w(x) = u(x) \cdot g(x) \mod x^n \oplus 1$$

$g(x)$ ... generující polynom BCK

... $g(x) \mid x^n \oplus 1$

Dekódování:

$$w(x) \cdot h(x) = 0$$

$h(x)$ ... kontrolní polynom

...

$$h(x) = \frac{x^n \oplus 1}{g(x)}$$

$$w(x) \cdot h(x) = u(x) \cdot g(x) \cdot \frac{x^n \oplus 1}{g(x)}$$

$$= u(x)(x^n \oplus 1)$$

$$= u(x) \oplus u(x) = 0$$

Potřebuji matematicky reprezentovat **rotaci**:

počítám $\mod x^n \oplus 1$

↑ zaručí, že výsledek je vždy max. n bitů

Příklad:

$\vec{w} = (0110) \Rightarrow w(x) = x \oplus x^2$ — 4 bitové slovo: bity x^0, x^1, x^2, x^3

posun doprava o 2 bity: $x^2 \cdot w(x) = x^3 \oplus x^4 \mod x^4 \oplus 1 =$

$= 1 \oplus x^3$

JAKTOŽE?

$$(x^3 \oplus x^4) : (x^4 \oplus 1) = 1$$

$$x^4 \oplus 1$$

$$x^3 \oplus 0 \oplus 1$$

$\Rightarrow$ $x \cdot w(x)$ – posun vpravo

$x^{-1} \cdot w(x)$ ... posun vlevo

CYKLICKÉ KÓDY

Kódování:

$u(x)$ ... otevřený text / zpráva

$$w(x) = u(x) \cdot g(x) \mod x^n \oplus 1$$

$g(x)$ ... generující polynom BCK

... $g(x) \mid x^n \oplus 1$

Dekódování:

$$w(x) \cdot h(x) = 0$$

$h(x)$ ... kontrolní polynom

...

$$h(x) = \frac{x^n \oplus 1}{g(x)}$$

$$w(x) \cdot h(x) = u(x) \cdot g(x) \cdot \frac{x^n \oplus 1}{g(x)}$$

$$= u(x)(x^n \oplus 1)$$

$$= u(x) \oplus u(x) = 0$$

Jak získáme $g(x)$?

Pro $x^n \oplus 1$ platí: $x^n \oplus 1 = \prod \varphi_i(x) = \varphi_0(x) \cdot \varphi_1(x) \cdot \varphi_2(x)$

φ_i ... ireducibilní polynomy jakési polynomiální „prvočísla"

Příklad: $n = 7$

$g(x) = x^3 \oplus x \oplus 1$ $\Rightarrow$ Hamming (7,4) cyklický

$\deg(g(x)) = 3$ $\Rightarrow m = 3,\ k = 4$

stupeň $g(x)$ udává počet kontrolních bitů

$h(x) = x^7 \oplus 1 : x^3 \oplus x \oplus 1 = x^4$

$x^7 \oplus x^5 \oplus x^4$

$x^5 \oplus x^4 \oplus 1$

⋮

Příklad $n=7$; $g(x)=x^3 \oplus x \oplus 1$ $\quad h(x)\cdot g(x) - x^n \oplus 1 \equiv 0$ $\quad$ **Ověření:**

$n-k = \deg[g(x)] = 3$

$k=4 \rightarrow (7,4)$ kód $\Rightarrow$ Hamming $\Rightarrow h(x) = \varphi_1(x)\cdot\varphi_3(x)$

$= (x\oplus 1)(x^3 \oplus x^2 \oplus 1) =$

$= x^4 \oplus x^3 \oplus x \oplus x^3 \oplus x^2 \oplus 1$

$\boxed{h(x) = x^4 \oplus x^2 \oplus x \oplus 1}$

Pro $x^n \oplus 1$ je $x^n \oplus 1 = \varphi_1(x)\cdot\varphi_2(x)\cdots\varphi_m(x)$

$x^7 \oplus 1 = (x\oplus 1)(x^3 \oplus x \oplus 1)(x^3 \oplus x^2 \oplus 1)$

$\varphi_1(x)$ $\quad \varphi_2(x)$ $\quad \varphi_3(x)$

$g'(x) = \varphi_2(x)\cdot\varphi_3(x)$ $\quad \deg[g'(x)] = 6 \Rightarrow (7,6)$ kód

$\Rightarrow$ Parita!

$h'(x) = \varphi_1(x)$ je kontrolní polynom

$\Rightarrow$ duální kód: prohodím $h(x)$ a $g(x)$

$$\begin{array}{r} 01011 \\ \oplus\ 10110 \\ \hline 11101 \end{array} \qquad \begin{array}{l} x^4 \oplus x^3 \oplus x \\ x^3 \oplus x^2 \oplus 1 \end{array}$$

Jak zakóduji $\vec{u} = (0101)$? $\rightarrow$ $u = [0,1,0,1]$

$u[0] \Rightarrow u_0 \cdot x^0$

$u[1] \Rightarrow u_1 \cdot x^1$

$\vdots$

$u(x) = x^3 \oplus x$

$v(x) = (x^3 \oplus x)(x^3 \oplus x \oplus 1)$

$= x^6 \oplus x^4 \oplus x^3 \oplus x^4 \oplus x^2 \oplus x$

$= x^6 \oplus x^3 \oplus x^2 \oplus x$

$\vec{v} = (0111001)$

Příklad: $n=7$; $g(x)=x^3\oplus x\oplus 1$ $\qquad h(x)\cdot g(x)=x^n\oplus 1\equiv 0$

$n-k=\deg[g(x)]=3$

$k=4 \rightarrow (7,4)$ kód $\Rightarrow$ Hamming $\Rightarrow h(x)=\varphi_1(x)\cdot\varphi_3(x)$

$=(x\oplus 1)(x^3\oplus x^2\oplus 1)=$

$=x^4\oplus x^3\oplus x\oplus x^3\oplus x^2\oplus 1$

$\boxed{h(x)=x^4\oplus x^2\oplus x\oplus 1}$

Pro $x^n\oplus 1$ je $x^n\oplus 1=\varphi_1(x)\cdot\varphi_2(x)\dots\varphi_m(x)$

$x^7\oplus 1=(x\oplus 1)(x^3\oplus x\oplus 1)(x^3\oplus x^2\oplus 1)$

$\varphi_1(x)$ $\quad\varphi_2(x)$ $\quad\varphi_3(x)$

$g'(x)=\varphi_2(x)\cdot\varphi_3(x)$ $\quad\deg[g'(x)]=6 \Rightarrow (7,6)$ kód

$\Rightarrow$ Parita!

$h'(x)=\varphi_1(x)$ je kontrolní polynom

$\Rightarrow$ duální kód: prohodím $h(x)$ a $g(x)$

Jak zakóduji $\vec{u}=(0101)$?

$u(x)=x^3\oplus x$

$v(x)=(x^3\oplus x)(x^3\oplus x\oplus 1)$

$=x^6\oplus x^4\oplus x^3\oplus x^4\oplus x^2\oplus x$

$=x^6\oplus x^3\oplus x^2\oplus x$

$\vec{v}=(0111001)$

Ověření:

$v(x)\cdot h(x)=(x^6\oplus x^3\oplus x^2\oplus x)(x^4\oplus x^2\oplus x\oplus 1)$

$=x^{10}\oplus x^6\oplus x^7\oplus x^6\oplus$
$x^7\oplus x^5\oplus x^4\oplus x^3\oplus$
$x^6\oplus x^4\oplus x^3\oplus x^2\oplus$
$x^5\oplus x^3\oplus x^2\oplus x$

$=x^{10}\oplus x^3\oplus x^3\oplus x$ $\quad$ mod $x^7\oplus 1$

$10-7=3 \quad 8-7=1$

$=x\oplus x\oplus x^3\oplus x$

$=x^3\oplus x^3\oplus x\oplus x$

$=0$

$x^{10}=x^7\cdot x^3=1\cdot x^3$

$\rightarrow v(x)$ je kódové slovo!!

CYKLICKÝ vs. LINEÁRNÍ KÓD

cyklický (n,k) kód:

$$g(x) = g_{n-k-1} \cdot x^{n-k-1} \oplus g_{n-k-2} \cdot x^{n-k-2} \oplus \dots g_1 x \oplus g_0$$

$$\rightarrow \vec{g} = (g_0 g_1 \dots g_{n-k-1}) = \vec{g_0} \qquad \vec{g_1} = (0\, g_0 g_1 \dots g_{n-k-1}) \qquad \vec{g_2} = (00\dots)$$

$g(x), x\cdot g(x), x^2\cdot g(x), \dots, x^{k-1}\cdot g(x)$ tvoří bázové vektory

$$G = \begin{bmatrix} \vec{g_0} \\ \vec{g_1} \\ \vdots \\ \vec{g_{k-1}} \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \dots & g_{n-k-1} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & & & & & & \vdots \\ \vdots & & & & & & & & 0 \\ 0 & 0 & \dots & g_0 & g_1 & \dots & & & g_{n-k-1} \end{bmatrix}$$

nesystematický lin. kód

Příklad: $g(x) = x^3 \oplus x \oplus 1 \qquad \vec{g} = (1101)$

$x\cdot g(x) = x^4 \oplus x^2 \oplus x$

$$\vdots$$

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

Jak sestrojit systematické G z $g(x)$?

$G_{sys} = [\, I \,\vdots\, P \,] \Rightarrow$ sestavíme P

$$\left.\begin{aligned} r_0(x) &= x^{n-1} \bmod g(x) \\ r_1(x) &= x^{n-2} \bmod g(x) \\ &\vdots \\ r_{k-1}(x) &= x^{n-k} \bmod g(x) \end{aligned}\right\} \deg[r_i(x)] \le n-k \qquad P = \begin{bmatrix} \vec{r_0} \\ \vec{r_1} \\ \vdots \\ \vec{r_{k-1}} \end{bmatrix}$$

Příklad: $g(x) = x^3 \oplus x \oplus 1$

$r_0(x) = x^6 \bmod x^3 \oplus x \oplus 1$
$= x^2 \oplus 1 \Rightarrow \vec{r_0} = (101)$

$r_1(x) = x^5 \bmod x^3 \oplus x \oplus 1$
$= x^2 \oplus x \oplus 1 \Rightarrow \vec{r_1} = (111)$

$r_2(x) = x^4 \bmod x^3 \oplus x \oplus 1$
$= x^2 \oplus x \Rightarrow \vec{r_2} = (011)$

$r_3(x) = x^3 \bmod x^3 \oplus x \oplus 1$
$= x \oplus 1 \Rightarrow \vec{r_3} = (110)$

$x^6 : x^3 \oplus x \oplus 1 = x^3 \oplus x \oplus 1$
$x^6 \oplus x^4 \oplus x^3$
$x^4 \oplus x^3$
$x^4 \oplus x^2 \oplus x$
$x^3 \oplus x^2 \oplus x$
$x^3 \oplus x \oplus 1$
$x^2 \oplus 1$

$\Rightarrow P = \begin{bmatrix} 101 \\ 111 \\ 011 \\ 110 \end{bmatrix}$

$G_{SYS} = \begin{bmatrix} 1000 & 101 \\ 0100 & 111 \\ 0010 & 011 \\ 0001 & 110 \end{bmatrix}$

Příklad: $g(x) = x^3 \oplus x \oplus 1$ $\quad \vec{g} = (1101)$

$x \cdot g(x) = x^4 \oplus x^2 \oplus x$

$G = \begin{bmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{bmatrix}$

Jak sestrojit systematické G z $g(x)$?

$G_{SYS} = [\, I \,\vdots\, P \,] \Rightarrow$ sestavíme P

$r_0(x) = x^{n-1} \bmod g(x)$
$r_1(x) = x^{n-2} \bmod g(x)$
$\vdots$
$r_{k-1}(x) = x^{n-k} \bmod g(x)$

$\Big\} \deg[r_i(x)] < n-k$

$P = \begin{bmatrix} \vec{r_0} \\ \vec{r_1} \\ \vdots \\ \vec{r_{k-1}} \end{bmatrix}$

Příklad: $g(x) = x^3 \oplus x \oplus 1$

$r_0(x) = x^6 \bmod x^3 \oplus x \oplus 1$
$= x^2 \oplus 1 \Rightarrow \vec{r_0} = (101)$

$r_1(x) = x^5 \bmod x^3 \oplus x \oplus 1$
$= x^2 \oplus x \oplus 1 \Rightarrow \vec{r_1} = (111)$

$r_2(x) = x^4 \bmod x^3 \oplus x \oplus 1$
$= x^2 \oplus x \Rightarrow \vec{r_2} = (011)$

$r_3(x) = x^3 \bmod x^3 \oplus x \oplus 1$
$= x \oplus 1 \Rightarrow \vec{r_3} = (110)$

$x^6 : x^3 \oplus x \oplus 1 = x^3 \oplus x \oplus 1$
$x^6 \oplus x^4 \oplus x^3$
$x^4 \oplus x^3$
$x^4 \oplus x^2 \oplus x$
$x^3 \oplus x^2 \oplus x$
$x^3 \oplus x \oplus 1$
$x^2 \oplus 1$

$\Rightarrow P = \begin{bmatrix} 101 \\ 111 \\ 011 \\ 110 \end{bmatrix}$

$G_{SYS} = \begin{bmatrix} 1000 & 101 \\ 0100 & 111 \\ 0010 & 011 \\ 0001 & 110 \end{bmatrix}$

Příklad: $g(x) = x^3 \oplus x \oplus 1$ $\quad \vec{g} = (1101)$

$x \cdot g(x) = x^4 \oplus x^2 \oplus x$
$\vdots$

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

$H = \begin{bmatrix} 0 & 0 & h_3 & h_2 & h_1 & h_0 \\ 0 & h_3 & h_2 & h_1 & h_0 & 0 \\ h_3 & h_2 & h_1 & h_0 & 0 & 0 \end{bmatrix}$

Jak sestrojit systematické G z $g(x)$?

$G_{SYS} = [\, I \vdots P \,] \Rightarrow$ sestavíme P

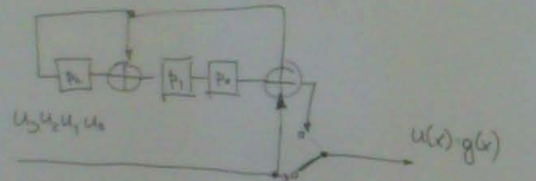
$r_0(x) = x^{n-1} \bmod g(x)$
$r_1(x) = x^{n-2} \bmod g(x)$
$\vdots$
$r_{k-1}(x) = x^{n-k} \bmod g(x)$

$\Big\}$ $\deg[r_i(x)] < n-k$

$P = \begin{bmatrix} \vec{r_0} \\ \vec{r_1} \\ \vdots \\ \vec{r_{k-1}} \end{bmatrix}$

Doplnění: LSR pro systematické kódování

Příklad: Hamming (7,4)



Dále: pro první 4 takty

$u(x)\ g(x) \rightarrow u(x) + x^{u} \cdot p(x)$

pomocné bity

původní slovo

Dekódování cyklických kódů

kódové slovo ⊕ porucha $e(x)$ → (se identifikovat pomocí syndromu $s(x)$)

$w(x) = u(x) \cdot g(x)$

$w(x) = w(x) + e(x)$ přijaté slovo, $e(x)$ může být 0

(?) jak najít $e(x)$?

→ vědět dělitele $g(x)$ je snadné!

$w(x) = u(x) \cdot g(x) + e(x)$ dělíme $g(x)$

$w'(x) = u(x) + s(x)$

↳ zbytek po dělení

Příklad: $g(x) = x^3 \oplus x \oplus 1$

$e(x)$	$s(x)$
0	0
1	1
x	x
x^2	x^2
x^3	$x+1$
⋮	⋮
x^6	x^2+1

opravuje jednoduché chyby

↓

$e(x)$ je x^i

⇒ nepraktické pro vyšší $\underline{t}$

Trik: Meggitt (1960)

$w(x) \rightarrow w^{(1)}(x) = x \cdot w(x)$

$s(x) \rightarrow s^{(1)}(x) = x \cdot s(x)$

⇒ posun $\underline{u(x)}$ (kotva) ideálně posune $\underline{s(x)}$ (kotvy)

→ **Meggittův dekodér**

používá pouze syndromy pro $\deg[e(x)] = \max$

(pouze x^6 u Hammingova kódu,

$0 + x^{14} \dots x^3 \oplus x^{14}$ u Golayova kódu)

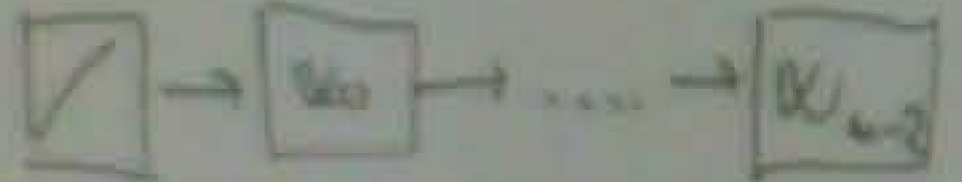
dvojnásobná chyba

jednoduchá chyba

Meggittův dekodér:

1. v prvních n taktech načte do LSR celé $w(x)$ počínaje w_{n-1} a konče w_0

2. dívá se na posledních m bitů po dělení a porovnává $s(x)$ s tabulkou
   → případně opraví bity, odpovídající $s(x)$
3. vyplivne ven nejvýznamnější bit
4. posun doprava



Jak konstruovat kód, opravující t/2 a detekující t chyb?

Bose, Chaudhuri, Hocquenghem (1960): **BCH kódy**

<u>Dáno:</u> m, $m \geq 3$ → $t < 2^{m-1}$

<u>Určuji:</u> délku bloku $n = 2^m - 1$

paritní symboly $n - k \leq m \cdot t$

$d_{min} \geq 2t + 1$

→ Určím délku než pro d_{min}

d_{min} ale může být vyšší, než požadovaný limit!

Reed-Solomonovy kódy (1960)

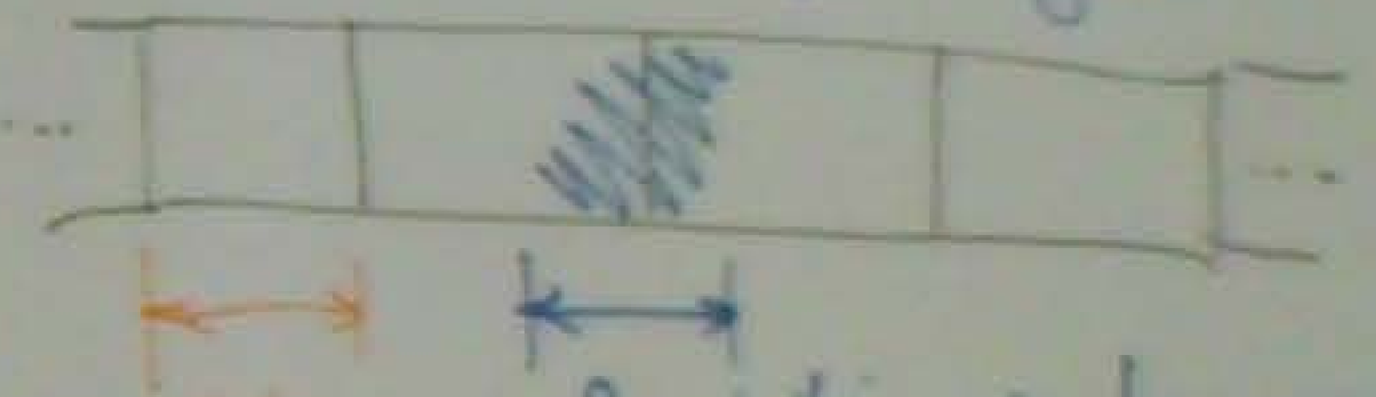
→ BCH kódy se symboly délky s bitů

<u>Použití:</u>

- datová úložiště
- bezdrátová komunikace (WiFi)
- satelitní komunikace
- čárové 2D kódy (QR, ...)
- ADSL, xDSL, ...

Díky délce symbolu s bitů opravují
a) shluky chyb
b) výpadky

Opravují chyby alespoň ve 2 symbolech
⇒ opraví shluk chyb délky s bitů



s bitů $< 2s$ bitů ⇒ lze opravit

Příklad: CD/DVD/BR

- hlavně: odolnost proti mechanickému poškození

CD:

↓

RS(32,28) je zkrácený RS(255,251)

↳ 28 bytů dat + 223 bytů nul

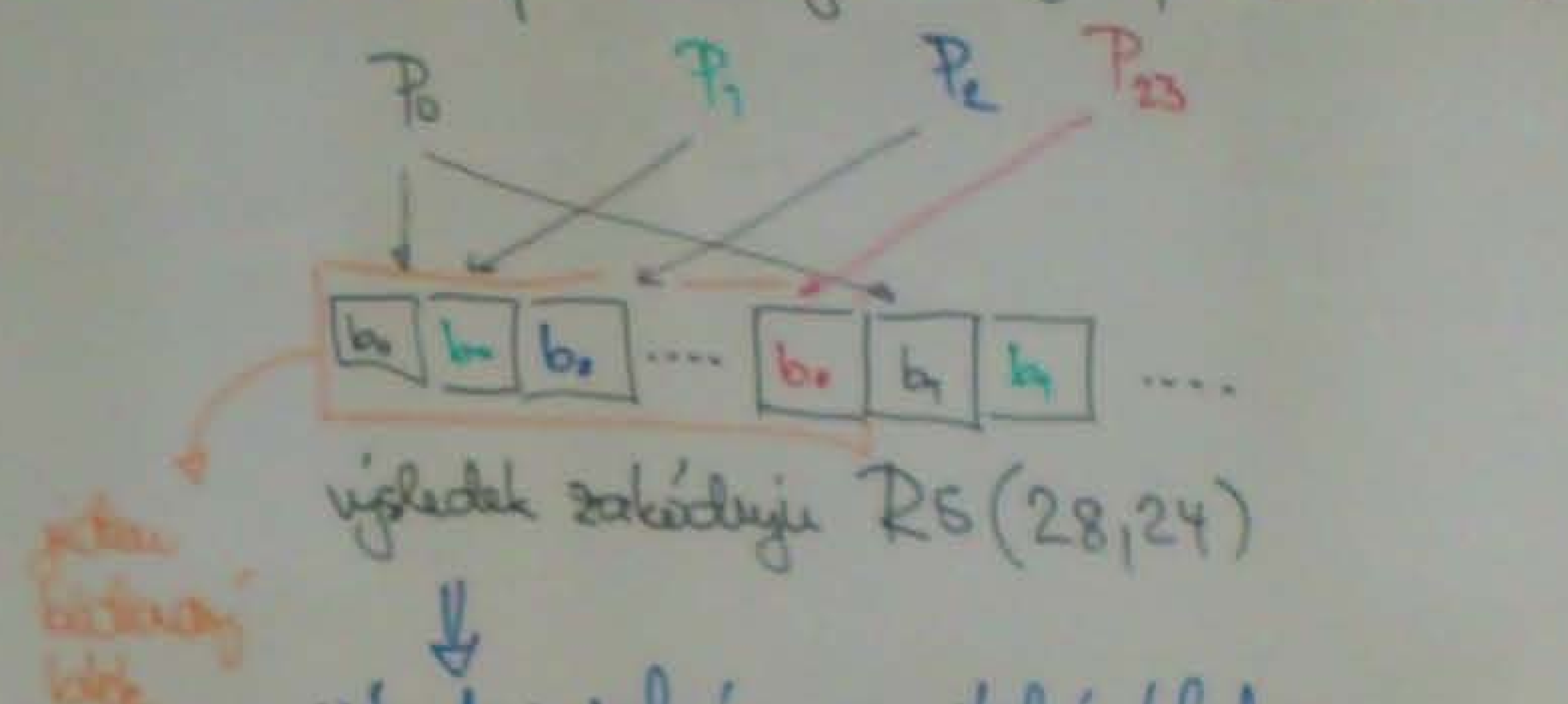
⇒ 4 byty parity

⇒ 32 byte uložím

⊕ prokládání

prokládání:

24 paketů délky 32 bytů, $P_0, P_1, \dots P_{23}$



výsledek zakóduju RS(28,24)

⇓

výhoda: velký neopravitelný shluk se rozpustí do opravitelných chyb v sousedních blocích

lze opravit shluky chyb cca 4 kbity

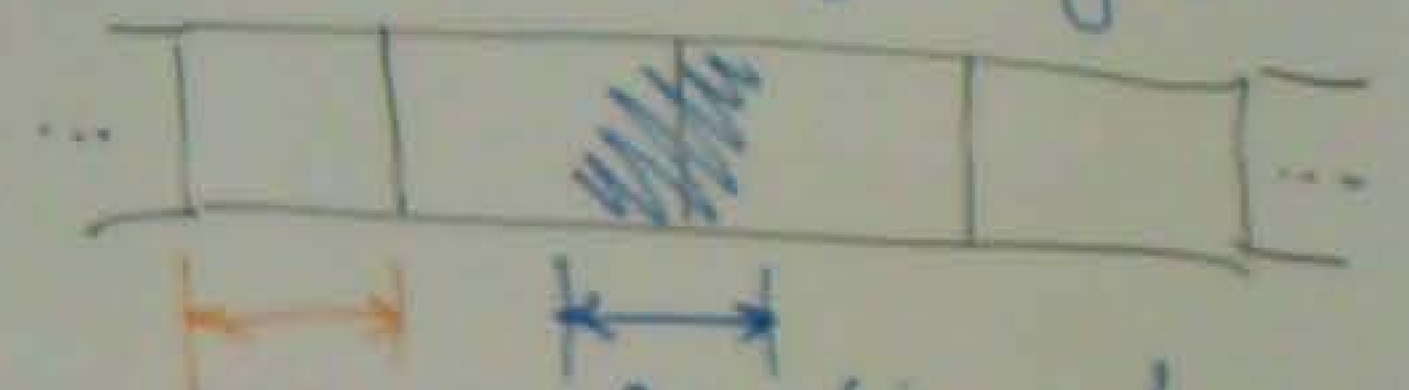
Díky délce symbolu s bitů opravují

a) shluky chyb

b) výpadky

Opravují chyby alespoň ve 2 symbolech

⇒ opraví shluk chyb délky s bitů



<2s bitů ⇒ lze opravit