CYKLICKÉ KÓDY

CYKLICKÉ KÓDY JSOU ZVLÁŠTNÍM PŘÍPADEM LINEÁRNÍCH KÓDŮ.

=> PLATÍ PRO NĚ VŠE, CO BYLO ŘEČENO PRO LINEÁRNÍ KÓDY + JEŠTĚ NĚCO NAVÍC (CYKLIČNOST)

S KAŽDOU ZNAČKOU $v \in K$ JE PRVKEM KÓDU K I LIBOVOLNÝ CYKLICKÝ POSUV v:

$$v_0 v_1 \dots v_{n-1} \in K \Rightarrow v_{n-1} v_0 v_1 \dots v_{n-2} \in K$$

JAK VYJÁDŘIT CYKLIČNOST MATEMATICKY?

ZNAČKY BUDEME REPREZENTOVAT POLYNOMY:

$$v_0 v_1 \dots v_{n-1} \sim v_0 + v_1 x + \dots + v_{n-1} x^{n-1} = \sum_{i=0}^{n-1} v_i x^i$$

POSUVU ZNAČKY DOPRAVA ODPOVÍDÁ OPERACE NÁSOBENÍ x

PŘ: $00111010 \sim x^2+x^3+x^4+x^6$

$$\downarrow \cdot x$$

$00011101 \sim x^3+x^4+x^5+x^7$

PROBLÉM: KDYŽ MÁ ZNAČKA „V NEJVYŠŠÍM ŘÁDU" (TJ. V PRAVÉM KONCOVÉM PRVKU) NENULOVÝ PRVEK, PAK PŘESTÁVÁ VÝSLEDEK NÁSOBENÍ KORELOVAT S POSUVEM (DOJDE „K PŘETEČENÍ").

ZAVEDEME TAKOVÉ NÁSOBENÍ POLYNOMŮ, VE KTERÉM BUDE PLATIT $x^n = 1$, TÍM DOSÁHNEME „EKVIVALENCE" NÁSOBENÍ POLYNOMŮ A CYKLICKÉHO POSUVU ZNAČKY.

OKRUHY POLYNOMŮ

POLYNOM PROMĚNNÉ x NAD TĚLESEM T:
$a_0 + a_1 x + \dots + a_n x^n$. STUPEŇ POLYNOMU JE NEJVĚTŠÍ ČÍSLO $k = \mathrm{st}\, a(x)$ TAKOVÉ, ŽE $a_k \neq 0$.

PŘ: POLYNOMY NAD $Z_2 = \{0,1\}$.
SČÍTÁNÍ POLYNOMŮ ODPOVÍDÁ SČÍTÁNÍ V LINEÁRNÍM VEKTOROVÉM PROSTORU.

$$
\begin{array}{lcl}
001110 & \sim & x^2 + x^3 + x^4 \\
011011 & \sim & x + x^2 + x^4 + x^5 \\
\hline
010101 & \sim & x + x^3 + x^5
\end{array}
$$

SČÍTÁNÍ POLYNOMŮ NAD TĚLESEM T

$a(x) = a_0 + a_1 x + \dots + a_n x^n$

$b(x) = b_0 + b_1 x + \dots + b_n x^n$

$c(x) = a(x) + b(x) \qquad c_i = a_i + b_i \quad \forall i = 0 \dots n$

NÁSOBENÍ POLYNOMŮ NAD TĚLESEM T

$c(x) = a(x) \cdot b(x)$ $\qquad c_i = a_0 b_i + a_1 b_{i-1} + \dots + a_i b_0$

$\forall\, i = 0, 1, \dots, m$

PŘ: V $\mathbb{Z}_2$

$$(1+x+x^2+x^3)+(1+x+x^4) = 1+1+x+x+$$
$$+x^2+x^3+x^4 = \underline{x^2+x^3+x^4}$$

$$(1+x+x^2+x^3)\cdot(1+x+x^4) = 1+x+x^2+x^3+$$
$$+x+x^2+x^3+x^4+x^4+x^5+x^6+x^7 =$$
$$= \underline{1+x^5+x^6+x^7}$$

PŘ: V $\mathbb{Z}_3$

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

$$(1+x+x^2+x^3)\cdot(1+x+x^4) = 1+x+x^2+x^3+$$
$$+x+x^2+x^3+x^4+x^4+x^5+x^6+x^7 =$$
$$= \underline{1+2x+2x^2+2x^3+2x^4+x^5+x^6+x^7}$$

MNOŽINA VŠECH POLYNOMŮ NAD TĚLESEM T TVOŘÍ OKRUH. ZNAČENÍ: $T[x]$.

DĚLENÍ POLYNOMŮ NAD TĚLESEM T

$a(x) : b(x) \rightarrow$ PODÍL $q(x)$, ZBYTEK $r(x)$

$$a(x) = q(x) \cdot b(x) + r(x)$$

$$\text{st } r(x) < \text{st } b(x)$$

PŘ: V $\mathbb{Z}_2$

$$
\begin{array}{l}
(x^3+x+1):(x+1) = x^2+x = q(x) \\
-\underline{(x^3+x^2)} \\
\quad x^2+x+1 \\
\quad -\underline{(x^2+x)} \\
\qquad 1 = r(x)
\end{array}
$$

$$-1 = 1$$

PŘ: V $\mathbb{Z}_3$

$$
\begin{array}{l}
(x^3+x+1):(x+1) = x^2+2x = q(x) \\
-(x^3+x^2) \\
\hline
\quad 2x^2+x+1 \\
\quad -(2x^2+2x) \\
\hline
\qquad 2x+1 \\
\qquad -(2x+2) \\
\hline
\qquad\quad 2 = r(x)
\end{array}
$$

$-1 = 2$

OKRUH POLYNOMŮ MODULO $q(x)$ STUPNĚ $m \geq 1$

ZNAČENÍ $T/q(x)$.

PRVKY OKRUHU $T/q(x)$ JSOU VŠECHNY POLYNOMY STUPNĚ $< m$.

SČÍTÁNÍ: $a(x) + b(x)$

NÁSOBENÍ: $a(x) * b(x)$ JE ZBYTEK PO DĚLENÍ $a(x) \cdot b(x)$ POLYNOMEM $q(x)$

Pr: $\mathbb{Z}_2 / x^2+1$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	1	x+1
x+1	0	x+1	x+1	0

$$x^2 : (x^2+1) = 1 \qquad (x^2+x) : (x^2+1) = 1$$

$$\frac{-(x^2+1)}{1} \qquad \frac{-(x^2+1)}{x+1}$$

OKRUH POLYNOMŮ $T^{(n)}$

MNOŽINA VŠECH SLOV DÉLKY n V TĚLESE T

ZÁPIS POLYNOMEM $a_0+a_1x+\dots+a_{n-1}x^{n-1}$

POLYNOMY JSOU PRVKY OKRUHU POLYNOMŮ

$T/(x^n-1)$

DŮSLEDEK:

- SEČÍTÁNÍ – KLASICKY
- NÁSOBENÍ – URČENO VZTAHEM $x^n=1$

SOUVISLOST OKRUHU POLYNOMŮ $T^{(n)}$ A CYKLICKÝCH KÓDŮ

PRO LIBOVOLNÝ POLYNOM $v(x)\in K$ JSOU VŠECHNY NÁSOBKY $q(x)*v(x)$ (KDE $q(x)\in T^{(n)}$) TAKÉ POLYNOMY KÓDU K.

PŘ. CYKLICKÉHO KÓDU:

KÓD CELKOVÉ KONTROLY PARITY DÉLKY $n=4$.
CYKLIČNOST JE ZŘEJMÁ.

0000	~ 0	$= 0\cdot(1+x)$
1100	$\sim 1+x$	$= 1\cdot(1+x)$
1010	$\sim 1+x^2$	$= (1+x)\cdot(1+x)$
1001	$\sim 1+x^3$	$= (1+x+x^2)\cdot(1+x)$
0110	$\sim x+x^2$	$= x\cdot(1+x)$
0101	$\sim x+x^3$	$= (x+x^2)\cdot(1+x)$
0011	$\sim x^2+x^3$	$= x^2\cdot(1+x)$
1111	$\sim 1+x+x^2+x^3$	$= (1+x^2)\cdot(1+x)$

$(1+x)$ ... NENULOVÝ POLYNOM NEJNIŽŠÍHO STUPNĚ.

OSTATNÍ MNOHOČLENY JSOU NÁSOBKEM $(1+x)$.

KAŽDÝ NETRIVIÁLNÍ CYKLICKÝ (n,k) KÓD K OBSAHUJE POLYNOM $g(x)$ STUPNĚ $n-k$. TEN MÁ TYTO VLASTNOSTI:

1) KÓD K SESTÁVÁ ZE VŠECH NÁSOBKŮ POLYNOMU $g(x)$ V $T^{(n)}$, TJ.

$$K = \{ q(x) g(x) \mid q(x) \in T^{(n)} \}$$

2) POLYNOMY $g(x), x \cdot g(x), \dots, x^{k-1} g(x)$ TVOŘÍ BÁZI KÓDU K.

3) POLYNOM $g(x)$ JE DĚLITELEM POLYNOMU $x^n - 1$ (DĚLÍ JEJ BEZE ZBYTKU)

$g(x)$ SE NAZÝVÁ GENERUJÍCÍ MNOHOČLEN. JE JEDINÝ (AŽ NA NÁSOBNÝ KOEFICIENT).

GENERUJÍCÍ MATICE CYKLICKÉHO KÓDU

$$G = \left[\begin{matrix} \overbrace{g_0 \quad g_1 \quad \cdots\cdots \quad g_{n-k}}^{n-k+1} & \overbrace{0 \quad 0 \quad \cdots\cdots \quad 0}^{k-1} \\ 0 \quad g_0 \quad g_1 \quad g_{n-k-1} \quad g_{n-k} & 0 \quad \cdots\cdots \quad 0 \\ \underbrace{0 \quad 0 \quad 0 \quad \cdots}_{k-1} & \underbrace{g_0 \quad g_1 \quad g_2 \quad \cdots\cdots \quad g_{n-k}}_{n-k+1} \end{matrix}\right] \Bigg\} k$$

1. ŘÁDEK – ZÁPIS POLYNOMU $g(x)$

2. ŘÁDEK – ZÁPIS POLYNOMU $x \cdot g(x)$

$\vdots$

K. ŘÁDEK – ZÁPIS POLYNOMU $x^{k-1} \cdot g(x)$

KÓDOVÁNÍ INFORMAČNÍCH ZNAKŮ

$$G = \begin{bmatrix} g(x) \\ x \cdot g(x) \\ \vdots \\ x^{k-1} \cdot g(x) \end{bmatrix} \qquad v = G^T \cdot u =$$

$$= u_0 g(x) + u_1 x g(x) + \dots + u_{k-1} x^{k-1} g(x) =$$

$$= g(x) \cdot (u_0 + u_1 x + \dots + u_{k-1} x^{k-1}) = \underline{g(x) \cdot u(x)}$$

KÓDOVÁNÍ: Z INFORMAČNÍCH ZNAKŮ VYTVOŘÍME POLYNOM STUPNĚ $< k$ A TÍM NÁSOBÍME POLYNOM $g(x)$.

PŘ: KÓD CELKOVÉ KONTROLY PARITY

JAK KÓDOVAT INFORMAČNÍ ČÁST $m_0 m_1 m_2$?

$$(m_0 + m_1 x + m_2 x^2) \cdot (1 + x) =$$
$$= m_0 + (m_1 + m_0) \cdot x + (m_1 + m_2) x^2 + m_2 x^3$$

PRO $m = [110]^T$ JE $v = 1 + x^2 \sim [1010]^T$

CYKLICKÝ KÓD OBECNĚ NENÍ SYSTEMATICKÝ (ZŘEJMÉ Z TVARU G).

JE EKVIVALENTNÍ SE SYSTEMATICKÝM LINEÁRNÍM KÓDEM.

POLYNOMY BUDEME ZAPISOVAT OBRÁCENĚ (OD NEJVYŠŠÍ MOCNINY K NEJNIŽŠÍ). BUDE NÁS ZAJÍMAT ZBYTEK PO DĚLENÍ $g(x)$.

SYSTEMATICKÉ CYKLICKÉ KÓDY (BINÁRNÍ)

INFORMAČNÍ ČÁST: $m(x)$

m_{k-1}	m_{k-2}	.....	m_1	m_0
$k-1$	$k-2$		1	0

$\sim m_{k-1}x^{k-1}+\dots+m_1x+m_0$

PŘIDAT $n-k$ NUL: $m(x)\cdot x^{n-k}$

m_{k-1}	m_{k-2}	......	m_1	m_0	$00\,.\,\dots\,.\,.0$
$n-1$	$n-2$		$n-k+1$	$n-k$	$n-k-1$ ... 0
k					$n-k$

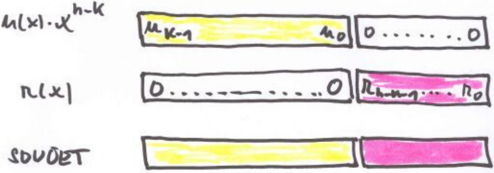
DĚLIT $g(x)$:

$$m(x)\cdot x^{n-k} = q(x)\cdot g(x) + r(x)$$

$$\operatorname{st}(r(x)) < n-k$$

$$\underbrace{m(x)\cdot x^{n-k} + r(x)} = q(x)\cdot g(x)$$

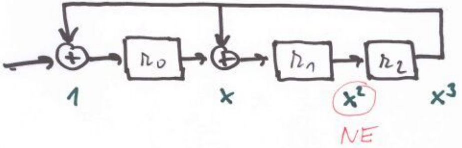
JE TO NÁSOBEK GENERUJÍCÍHO MNOHO-ČLENU, JE TO TEDY ZNAČKA CYKL. KÓDU.



JE VIDĚT, ŽE JE TO SYSTEMATICKÝ KÓD.

HW REALIZACE SYSTEMATICKÉHO CYKLICKÉHO KODÉRU

PŘ: $g(x) = 1 + x + x^3$

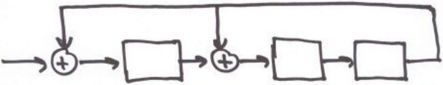


PŘ: $101\,000 : 1011 = \boxed{100}$ PODÍL

$-(1011)$

$000\boxed{100}$ ZBYTEK

$r_2 r_1 r_0$



0.	8.	1.	4.	7.	2.	5.	3.	6.	
1	1	0	0	0	0	0	0	0	
0	0	1	1	1	0	0	0	0	
1	1	0	0	0	1	1	0	0	
0	1	1	1	0	0	0	1	1	PODÍL
0	0	1	1	1	0	0	0	0	
0	0	0	0	0	1	1	0	0	
	0	0	0	0	0	0	1	1	
		r_0			r_1		r_2		

KONTROLNÍ POLYNOMY

$$h(x) = (x^n - 1) : g(x)$$

STUPEŇ $h(x)$: $n-(n-k) = k$

KONTROLNÍ MATICI LZE VYTVOŘIT POMOCÍ $h(x)$.

PŘ: KÓD CELKOVÉ KONTROLY PARITY DÉLKY $n=4$.

$$g(x) = 1 + x$$

$$\underline{h(x)} = (x^4+1):(x+1) = \underline{x^3+x^2+x+1}$$

$$\begin{array}{l}
\underline{-(x^4+x^3)} \\
\quad x^3+1 \\
\quad \underline{-(x^3+x^2)} \\
\qquad x^2+1 \\
\qquad \underline{-(x^2+x)} \\
\qquad\quad x+1 \\
\qquad\quad \underline{-(x+1)} \\
\qquad\qquad 0
\end{array}$$

CYKLICKÝ KÓD S KONTROLNÍM POLYNOMEM $h(x)$ SESTÁVÁ PRÁVĚ Z TĚCH POLYNOMŮ $v(x)$ V OKRUHU $T^{(n)}$ PRO KTERÉ PLATÍ $v(x) * h(x) = 0$ V $T^{(n)}$.

KONTROLNÍ MATICE

$$
\begin{array}{cc}
 & \overbrace{\hphantom{0 \quad 0 \quad \cdots \quad 0}}^{n-k+1} \qquad \overbrace{\hphantom{h_k \quad h_{k-1} \quad \cdots \quad h_1 \quad h_0}}^{k+1} \\
H = n-k \left\{ \right. & \begin{bmatrix}
0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 \\
0 & 0 & \cdots & 0 \; h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 \\
 & & & & \vdots & & & & \\
0 & & & & & & & & \\
h_k & h_{k-1} & & & h_1 & h_0 & 0 & \cdots & 0
\end{bmatrix} \\
 & \underbrace{\hphantom{h_k \quad h_{k-1} \quad \cdots \quad h_1 \quad h_0}}_{k+1} \qquad \underbrace{\hphantom{0 \quad \cdots \quad 0}}_{n-k+1}
\end{array}
$$

KONTROLA PŘIJATÉ ZNAČKY SE BUDE V OBECNÉM CYKLICKÉM KÓDU PROVÁDĚT NÁSOBENÍM ZNAČKY S KONTROLNÍM POLYNOMEM V $T^{(n)}$.

CYKLICKÉ KÓDY V PRAXI

ZABEZPEČENÍ PŘENÁŠENÝCH DAT V POČÍTAČOVÝCH SÍTÍCH.

DETEKCE SHLUKOVÝCH CHYB. NEPOUŽÍVAJÍ SE K OPRAVOVÁNÍ CHYB.

POUŽÍVANÉ GENERUJÍCÍ POLYNOMY:

CRC-16 $x^{16}+x^{5}+x^{2}+1$

CRC-CCITT

$$x^{16}+x^{12}+x^{5}+1$$

CRC-32

$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+$$
$$+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

ZABEZPEČOVACÍ VLASTNOSTI RŮZNÝCH CYKLICKÝCH KÓDŮ (ILUSTRACE)

Tab. 1.5 Přehled cyklických kódů a jejich teoretické zabezpečovací schopnosti

z	Generační mnohočlen	Zabezpečení lichého počtu chyb	Zabezpečení shluků chyb délky $z+1$ (v %)	Zabezpečení shluků chyb délky větší než $z+1$ (v %)	Zabezpečení platí pro max. délku bloku (v bitech)	Zabezpečení 2 shluků chyb: max. součet shluků chyb (v bitech)	Zabezpečení 2 shluků chyb: max. délka kratšího shluku (v bitech)	Zabezpečení 2 shluků chyb: platí pro max. celkovou délku bloku (v bitech)
5	x^5+x^2+1 $x^5+x^4+x^2+1$ x^5+x^3+x+1	ne ano ano	93,75	96,9	31	2 2 3	1 1 1	31 15 14
6	x^6+x+1 x^6+x^4+x+1 $x^6+x^5+x^4+x^2+x+1$ $x^6+x^4+x^3+x^2+x+1$ $x^6+x^5+x^3+x^2+x+1$	ne ano ano ano ano	96,9	98,4	63	2 4 5 3 2	1 2 2 1 1	63 20 12 30 31
7	x^7+x^3+1 $x^7+x^5+x^4+1$ $x^7+x^5+x^4+x^3+x+1$	ne ano ano	98,4	99,2	127	2 3 5	1 1 2	127 62 28
8	$x^8+x^4+x^3+x^2+1$ x^8+x^5+x+1	ne ano	99,2	99,6	255	2 5	1 2	255 60
9	x^9+x^4+1 $x^9+x^6+x^5+x^4+x^2+1$	ne ano	99,6	99,8	511	2 5	1 2	511 124
10	$x^{10}+x^3+1$ $x^{10}+x^7+x^2+1$	ne ano	99,8	99,9	1023	2 6	1 3	1023 155
11	$x^{11}+x^2+1$ $x^{11}+x^3+x+1$ $x^{11}+x^8+x^7+x^4+x+1$	ne ano ano	99,9	99,95	2047	2 6 8	1 3 4	2047 315 105
12	$x^{12}+x^6+x^4+x+1$ $x^{12}+x^7+x+1$ $x^{12}+x^9+x^8+x^4+x+1$	ne ano ano	99,95	99,975	4095	2 7 9	1 3 4	4095 126 120