<KIV> KATEDRA INFORMATIKY A VÝPOČETNÍ TECHNIKY

FAKULTA APLIKOVANÝCH VĚD
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

Předmět KIV/TI - přednáška 9

Cyklické kódy

Ing. Václav Vais, Ph.D.

vais@kiv.zcu.cz

Ekvivalentní kódy

- Dva blokové kódy K a K' délky n jsou *ekvivalentní* , jestliže existuje permutace $[\pi_1, \pi_2, \ldots, \pi_n]$ čísel 1, 2, ….., n taková, že platí

  $\forall\, v_1, v_2, \ldots, v_n \in T^n : \; v_1, v_2, \ldots, v_n \in K \;\Leftrightarrow\; v_{\pi_1}, v_{\pi_2}, \ldots, v_{\pi_n} \in K'$.

- Jinými slovy:
  - existuje vzájemně jednoznačné přiřazení mezi kódovými značkami obou kódů
  - odpovídající si značky obou kódů se navzájem liší jen záměnou pořadí prvků. U všech odpovídajících si dvojic je to pořadí zaměněno stejně.

Ekvivalentní kódy

- Ke každému lineárnímu kódu existuje ekvivalentní systematický kód.
- Jak z generující matice $\boldsymbol{G}$ zkonstruovat generující matici $\boldsymbol{G}'$ ekvivalentního systematického kódu?
  - $\boldsymbol{G}$ má *k* lineárně nezávislých řádků, *n* > *k*, matice má tedy i *k* lineárně nezávislých sloupců (vlastnosti matic, viz LA)
  - pokud je lineárně nezávislých prvních *k* sloupců matice $\boldsymbol{G}$, vytvoříme matici $\boldsymbol{G}'$ ekvivalentními řádkovými úpravami matice $\boldsymbol{G}$; získáme tak jinou bázi prostoru kódových značek generovaných maticí $\boldsymbol{G}$, tedy jinou bázi téhož kódu

Ekvivalentní kódy

- pokud prvních *k* sloupců matice G není lineárně nezávislých, provedeme takovou permutaci sloupců matice G, abychom dostali nezávislé sloupce do prvních *k* pozic; pak vytvoříme systematickou matici G' ekvivalentními řádkovými úpravami (sloupcově permutova-né) matice G; v tomto případě budou množiny značek generované maticemi G a G' různé, ale bude mezi nimi existovat vzájemně jednoznačné zobrazení dané provedenou záměnou sloupců matice G, kódy tedy budou ekvivalentní

Cyklické kódy

- Cyklické kódy jsou zvláštním případem lineárních kódů.

  ⇒ platí pro ně vše, co bylo řečeno pro lineární kódy + něco navíc

  (cykličnost)

  POZOR ! Změníme indexování prvků ve značce $\boldsymbol{v}$ (dříve 1 až *n*, nyní 0 až *n*-1)

- S každou kódovou značkou $\boldsymbol{v} \in \mathbf{K}$ je prvkem kódu $\mathbf{K}$ i cyklický posuv značky :

$$\boldsymbol{v} = [v_0\, v_1 \ldots \ldots v_{n-1}]^T \in \boldsymbol{K} \Rightarrow [v_{n-1} v_0\, v_1 \ldots \ldots v_{n-2}]^T \in \boldsymbol{K}$$

  popsán cyklický posuv o jednu pozici doprava; indukce ⇒ množina kódových značek je uzavřená vůči **libovolnému** cyklickému posuvu

Cyklické kódy

- Značky nebudeme reprezentovat vektory, ale polynomy:

$$\boldsymbol{v} = [v_0\, v_1 \ldots v_i \ldots v_{n-1}\,]^{\boldsymbol{T}} \quad \approx \quad v(x) = v_0 + v_1 \cdot x + \cdots + v_i \cdot x^i + \cdots + v_{n-1} \cdot x^{n-1}$$

Například

$$\boldsymbol{v} = [00111010]^{\boldsymbol{T}} \quad \approx \quad v(x) = x^2 + x^3 + x^4 + x^6$$

- Posuv značky o jednu pozici doprava $\approx$ násobení $v(x) \cdot x$

$$\bar{v}(x) = v(x) \cdot x = x^3 + x^4 + x^5 + x^7 \quad \approx \quad \bar{\boldsymbol{v}} = [00011101]^{\boldsymbol{T}}$$

cyklický posuv $\boldsymbol{v}$ o jednu pozici doprava

$$\bar{\bar{v}}(x) = \bar{v}(x) \cdot x = x^4 + x^5 + x^6 + x^8$$

nejvyšší mocnina „přetekla“ mimo rozsah

násobení činitelem x cyklickému posunu už neodpovídá

Cyklické kódy

- Násobení *x* „částečně odpovídá“ posuvu značky doprava.
- Problém: Když má značka v pravém krajním prvku (odpovídá koeficientu u nejvyšší mocniny x) nenulový prvek, dojde k „přetečení mimo rozsah“
- Je třeba najít mechanizmus, který do operace násobení mnohočlenů zavede identitu $x^n = x^0 = 1$,

  jinak řečeno: „u proměnné *x* musíme počítat s exponenty v režimu modulo *n*“
- Zavedeme operaci násobení polynomů $u(x) * v(x)$ s vlastností $x^n = x^0 = 1$, bude to *násobení polynomů v okruhu polynomů modulo* $x^n - 1$.

Cyklické kódy

- Analogie k operacím v prvočíselných tělesech:
  - Sečítání modulo *p v prvočíselném tělese*:

    $a \oplus b = (a + b) \bmod p$ (zbytek po dělení součtu číslem p, $\Rightarrow p = 0$)

- Násobení mnohočlenů v okruhu polynomů modulo $x^n - 1$:

  Má-li platit $x^n = 1$, musí platit $x^n - 1 = 0$

  $u(x) * v(x) = [u(x) \cdot v(x)] \bmod (x^n - 1)$

  Výsledkem násobení $u(x) * v(x)$ je tedy zbytek po dělení „standardního součinu polynomů“ „modulovým polynomem“ $x^n - 1$.

Okruh polynomů modulo $x^n - 1$

- Tento okruh je tvořen všemi polynomy stupně menšího než *n* .
- Operace sečítání: standardní sečítání mnohočlenů.
- Operace násobení: výsledkem je zbytek po dělení „standardního součinu polynomů“ „modulovým polynomem“ $x^n - 1$, tedy s identitou $x^n = 1$.

Ilustrační příklad: Okruh polynomů modulo $(x^2 - 1)$ nad tělesem Z_2

(značení - $Z_2 / x^2 - 1$)

Prvky tohoto okruhu jsou $0,\ 1,\ x\ ,\ x + 1$.

Okruhy polynomů modulo $x^n - 1$

Ilustrační příklad: Okruh polynomů modulo $(x^2 - 1)$ nad tělesem Z_2

Prvky tohoto okruhu jsou $0,\ 1,\ x\ ,\ x + 1\ .$

Operace nad nimi nadefinujeme takto:

+	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

Cyklické kódy - příklad

- Ilustrační příklad: kód celkové kontroly parity s délkou $n = 4$ (cykličnost je zřejmá, sudost/lichost počtu jedniček se cyklickými posuvy nemění).
- Množina kódových značek:

  {0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111}
- V dalším provedeme následující:
  - každou značku vyjádříme polynomem
  - ukážeme, že každý „značkový polynom“ je násobkem jistého „speciálního mnohočlenu“ $g(x)$

Cyklické kódy - příklad

v	***v(x)***	***v(x) = u(x) ∗ g(x)***	***u(x)***
0000	0	$0 \cdot (1 + x)$	000
1100	$1 + x$	$1 \cdot (1 + x)$	100
1010	$1 + x^2$	$(1 + x) \cdot (1 + x)$	110
1001	$1 + x^3$	$(1 + x + x^2) \cdot (1 + x)$	111
0110	$x + x^2$	$x \cdot (1 + x)$	010
0101	$x + x^3$	$(x + x^2) \cdot (1 + x)$	011
0011	$x^2 + x^3$	$x^2 \cdot (1 + x)$	001
1111	$1 + x + x^2 + x^3$	$(1 + x^2) \cdot (1 + x)$	101

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

Cyklické kódy - obecně

- V každém cyklickém kódu splňujícím podmínku $0 < k < n$ existuje polynom $g(x)$ *(generující mnohočlen)* stupně $n - k$.
- Všechny mnohočleny reprezentující kódové značky jsou násobky generujícího polynomu v okruhu polynomů $\mathrm{Z}_p / \, x^n - 1$.
- Generující mnohočlen je nenulový mnohočlen nejnižšího stupně ze všech „značkových“ polynomů.
- U binárních kódů nad tělesem Z_2 je generující mnohočlen určen jednoznačně, u kódů na obecným Z_p má vlastnosti generujícího mnohočlenu více mnohočlenů, ale liší se jen násobnou konstantou. Je-li $g(x)$ gen. mn., je jím i $k \cdot g(x)$, $k \neq 0$, $k \in \mathrm{Z}_p$

Cyklické kódy - obecně

- Vlastnosti generujícího mnohočlenu $g(x)$:
  - množina značkových polynomů je tvořena všemi násobky generujícího mnohočlenu $g(x)$ v okruhu polynomů $\mathrm{Z}_p / x^n - 1$

$$K = \{q(x) * g(x) \mid q(x) \in \mathrm{Z}_p / x^n - 1\}$$

  - polynomy $g(x),\ x \cdot g(x),\ x^2 \cdot g(x), \ldots\ldots, x^{k-1} \cdot g(x)$ tvoří bázi kódu K
  - generující mnohočlen je *nerozložitelný* (viz LA)
  - generující mnohočlen je *primitivní* , tj.
    - $g(x)$ je dělitelem polynomu $x^{\mathrm{n}} - 1$ (dělí jej beze zbytku)
    - neexistuje $m < n$ takové, že $g(x)$ dělí beze zbytku $x^m - 1$

Cyklické kódy - obecně

- Z vlastností generujícího mnohočlenu $g(x)$ je zřejmé, že ne každý polynom může být generujícím mnohočlenem.
- Ověření vlastností mnohočlenu je algoritmicky zvládnuté, i když výpočetně složité.
- Jsou publikovány tabulky s polynomy, které mají vlastnosti generujících mnohočlenů.
- Ukazuje se, že požadavky na primitivnost a nerozložitelnost nejsou nepřekročitelné, v praxi se používají i polynomy ve tvaru $(x+1)$ - násobek nerozložitelného polynomu (v jistém smyslu to může zabezpečovací vlastnosti kódu vylepšit).

  Generující mnohočlen specifikovaný standardem IEEE 802.3 není primitivní:

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

Cyklické kódy - obecně

- Generující matice cyklického kódu

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{b}_0 \\ \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \vdots \\ \boldsymbol{b}_{k-1} \end{bmatrix} = \begin{bmatrix} g(x) \\ x \cdot g(x) \\ x^2 \cdot g(x) \\ \vdots \\ \vdots \\ x^{k-1} \cdot g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ & & & \ddots & \ddots & \ddots & \ddots & \ddots & & \\ 0 & 0 & \cdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{bmatrix}$$

reprezentace bázových prvků polynomy

reprezentace bázových prvků vektory

- Takto konstruované cyklické kódy jsou nesystematické (zřejmé z tvaru matice $\boldsymbol{G}$).

Cyklické kódy - obecně

- Kódování informační části

$$\boldsymbol{v} = \varphi(u) = u_0 \cdot \boldsymbol{b}_0 + u_1 \cdot \boldsymbol{b}_1 + \cdots + u_{k-1} \cdot \boldsymbol{b}_{k-1}\,, \text{ tedy}$$

$$v(x) = u_0 \cdot g(x) + u_1 \cdot x\, g(x) + \cdots + u_{k-1} \cdot x^{k-1}\, g(x) =$$
$$= (u_0 + u_1 \cdot x + \cdots + u_{k-1} \cdot x^{k-1}) \cdot g(x) = u(x) \cdot g(x)$$

- U cyklických kódů přebírá úlohu generující matice generující mnohočlen $g(x)$.
- Informační části o k prvcích přiřadíme *informační mnohočlen* $u(x)$:

$$\boldsymbol{u} = [u_0\, u_1 \ldots u_i \ldots u_{k-1}]^{\boldsymbol{T}} \quad \approx \quad u(x) = u_0 + u_1 \cdot x + \cdots + u_i \cdot x^i + \cdots + u_{k-1} \cdot x^{k-1}$$

Cyklické kódy - obecně

- Kódování informační části

$$\boldsymbol{v} = \varphi(u) = u_0 \cdot \boldsymbol{b}_0 + u_1 \cdot \boldsymbol{b}_1 + \cdots + u_{k-1} \cdot \boldsymbol{b}_{k-1}\,,\ \text{tedy}$$

$$v(x) = u_0 \cdot g(x) + u_1 \cdot x\, g(x) + \cdots + u_{k-1} \cdot x^{k-1}\, g(x) =$$
$$= (u_0 + u_1 \cdot x + \cdots + u_{k-1} \cdot x^{k-1}) \cdot g(x) = u(x) \cdot g(x)$$

- U cyklických kódů přebírá úlohu generující matice generující mnohočlen $g(x)$.
- Informační části o *k* prvcích přiřadíme *informační mnohočlen* $u(x)$:

$$\boldsymbol{u} = [u_0\, u_1 \ldots u_i \ldots u_{k-1}]^{\boldsymbol{T}} \quad \approx \quad u(x) = u_0 + u_1 \cdot x + \cdots + u_i \cdot x^i + \cdots + u_{k-1} \cdot x^{k-1}$$

- Informační mnohočlen pak zakódujeme: $v(x) = u(x) \cdot g(x)$.

Cyklické kódy – pokračování příkladu

- Ilustrační příklad: kód celkové kontroly parity s délkou $n = 4$
- Generující mnohočlen $g(x) = 1 + x$.

  stupeň $g(x)$ = $n - k = 1$, $n = 4$ $\Rightarrow k = 3$
- Vytvoříme generující matici $\boldsymbol{G}$ (rozměr k/n, tedy 3/4):

$$\boldsymbol{G} = \begin{bmatrix} 1+x \\ x\cdot(1+x) \\ x^2\cdot(1+x) \end{bmatrix} = \begin{matrix} x^0 x^1 x^2 x^3 \\ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \end{matrix}$$

- „Vytvořující rovnice“: $v_0 = u_0\,,\ v_1 = u_0 + u_1\,,\ v_2 = u_1 + u_2\,,\ v_3 = u_2$

Cyklické kódy – pokračování příkladu

- Zakódujeme informační část $\boldsymbol{u} = [u_0\, u_1\, u_2\,]^T = [1\ 0\ 1\,]^T$
- Kódování pomocí generující matice:

$$v_0 = u_0\,,\ \ v_1 = u_0 + u_1\,,\ \ v_2 = u_1 + u_2\,,\ \ v_3 = u_2$$

tedy

$$v_0 = 1\,,\ \ v_1 = 1\,,\ \ v_2 = 1\,,\ v_3 = 1 \qquad \boldsymbol{v} = [v_0\, v_1\, v_2\, v_3\,]^T = [1\ 1\ 1\ 1\,]^T$$

- Kódování pomocí generujícího mnohočlenu:

$$u(x) = u_0 + u_1 \cdot x\ + u_2 \cdot x^2 = 1 + x^2$$

$$v(x) = u(x) \cdot g(x) = (1 + x^2) \cdot (1 + x) = 1 + x^2 + x + x^3 = 1 + x + x^2 + x^3$$

$$\boldsymbol{v} = [v_0\, v_1\, v_2\, v_3\,]^T = [1\ 1\ 1\ 1\,]^T$$

Cyklické kódy - obecně

- Kontrola přijaté značky – u cyklických kódů přebírá úlohu kontrolní matice *kontrolní mnohočlen* $h(x)$.
- Kontrolní mnohočlen $h(x)$ je jednoznačně určen generujícím mnohočlenem $g(x)$:

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

  Toto dělení vždy vyjde beze zbytku.
- Každý značkový polynom $v(x) \in K$ vyhovuje podmínce $h(x) * v(x) = 0$

  operátor $*$ představuje operaci násobení polynomů v okruhu $\mathrm{Z}_p / x^n - 1$
- Kód K pak tvoří všechny polynomy splňující tuto podmínku:

$$K = \{v(x) \mid v(x) \in \mathrm{Z}_p / x^n - 1 \ \wedge \ h(x) * v(x) = 0\}$$

Cyklické kódy - obecně

- Kontrolní matici $\boldsymbol{H}$ lze sestavit z koeficientů kontrolního mnohočlenu $h(x)$:

$$\boldsymbol{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & h_k & \cdots & h_2 & h_1 & h_0 \\ 0 & 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & 0 \\ & & & \iddots & \iddots & \iddots & \iddots & \iddots & & & \\ & & \iddots & \iddots & \iddots & \iddots & \iddots & & & & \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 & 0 \\ h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$

Cyklické kódy – pokračování příkladu

- Ilustrační příklad: kód celkové kontroly parity s délkou *n* = 4
- Generující mnohočlen $g(x) = 1 + x$ a generující matice $\boldsymbol{G} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
- Výpočet kontrolního mnohočlenu:

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

$$-\underline{(x^4 + x^3)}$$

$$x^3 + 1$$

$$-\underline{(x^3 + x^2)}$$

$$x^2 + 1$$

$$-\underline{(x^2 + x)}$$

$$x + 1$$

$$-\underline{(x + 1)}$$

$$0$$

$$h(x) = h_3\, x^3 + h_2 x^2 + h_1 x + h_0$$

$$h_3 = 1 \qquad h_1 = 1$$

$$h_2 = 1 \qquad h_0 = 1$$

Cyklické kódy – pokračování příkladu

- Kontrolní mnohočlen : $h(x) = 1 + x + x^2 + x^3$
- Kontrolní matice : $\boldsymbol{H} = [\, h_0\ h_1\ h_2\ h_3 \,] = [\, 1\ 1\ 1\ 1 \,]$
- Kontrolní matice a generující matice obsahují prvky bází dvou navzájem ortogonálních podprostorů ⇒ skalární součin (libovolného) řádku matice $\boldsymbol{H}$ s libovolným řádkem matice $\boldsymbol{G}$ je nulový, tedy

$$\boldsymbol{H} \cdot \boldsymbol{G}^{\boldsymbol{T}} = \boldsymbol{0}$$

$\boldsymbol{0}$ představuje nulovou matici typu $(n-k)/k$

- Obecný závěr: v této (nesystematické) podobě nejsou cyklické kódy prakticky použitelné (nekomfortní dekódování a extrakce informační části) ⇒ dále se budeme zabývat ekvivalentními systematickými cyklickými kódy.