Cvičení 4. - Tělesa, ISBN - kódy

Pojmy z přednášky

Struktury s jednou operací – Grupoid
- Pologrupa
- Monoid
- Grupa

Struktury se dvěma operacemi – Okruh $(R, +, \cdot)$
$(R, +)$ - komutativní grupa
$(R, \cdot)$ - pologrupa + distributivní zákony

- Těleso $(F, +, \cdot)$
komutativní okruh, kde $(F, \cdot)$ je grupa
- Konečné těleso řádu n $GF(n)$

Věta 3.6. Je-li p prvočíslo $(\mathbb{Z}_p, +, \cdot)$ je tělesem.
okruh zbytkových tříd modulo p

Věta: Konečné těleso $GF(n)$ existuje $\Leftrightarrow$ n je mocnina prvočísla.

Tělesa řádu mocnina prvočísla konstruujeme faktorové okruhy okruhů polynomů $(Z_2[x] / \langle p(x) \rangle, +, \cdot)$

① Tabulky operací pro $(Z_2, +, \cdot)$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

1. Sestavte těleso řádu 4.

$(Z_4, +, \cdot)$ ← není těleso

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(Z_4, +)$ komut. grupa ✓

a	0	1	2	3
a^{-1}	0	3	2	1

· – je komutativní

$(Z_4 \setminus \{0\}, \cdot)$ není grupa

$(Z_4 \setminus \{0\}, \cdot)$ není uzavřená vzhl. k „·",

a	1	2	3
a^{-1}	1	?	3

k 2 neexistuje inverze

$2 \cdot 2 = 0$ ← existují dělitelé 0

Protože $4 = 2^2$ ← mocnina prvočísla, podle věty 3.6 těleso řádu 4 existuje.

P_i: $F_2[x]/(x^2+x+1)$

Nosná množina $GF(4) = F_2[x]/(x^2+x+1)$

$F_q[x]$ – polynomy s koeficienty ze Z_q s operacemi + a ·. Okruh

$F_q[x]/f(x)$ – zbytky polynomů $F_q[x]$ po dělení polynomem $f(x)$

- Dělení polynomů se zbytkem $g(x) = q(x) \cdot f(x) + r(x)$
  $st(r(x)) < st(g(x))$
- kongruence polynomů $g(x) \equiv h(x) \pmod{f(x)}$ jestliže
  $g(x) - h(x)$ je dělitelné $f(x)$

$F_q[x]/f(x)$ je množina polynomů stupně $< st(f(x))$

s operacemi $+_a$ • modulo $f(x)$:

Je-li $a(x), b(x) \in F_q[x]/f(x)$ pak

„+" $a(x)+b(x) \pmod{f(x)}$ odpovídá $a(x)+b(x) \in F_q(x)$
protože $st(a(x)+b(x)) < st(f(x))$

„·" $a(x)\cdot b(x) \pmod{f(x)}$ výsledkem je jednoznačně určený polynom, který je zbytkem polynomu $a(x)\cdot b(x)$ po dělení $f(x)$, kdy $st\, a(x)\cdot b(x) < st\, f(x)$

Jaké zbytky můžeme dostat po dělení polynomů $F_2[x]$ polynomem x^2+x+1?

$\underbrace{0, 1, x, x+1}_{4 \text{ možné zbytky}}$ ← všechny možné zbytky

Obecně v $F_q[x]$ po dělení polynomem $f(x)$ stupně n dostaneme q^n zbytků stupně $\leq n-1$

Proto $|F_2[x]/(x^2+x+1)| = 4$

Jak budou vypadat tabulky pro $+_a$ • modulo $f(x)=x^2+x+1$

+	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

$(F_2(x)/(x^2+x+1), +)$ - Grupa ✓
asociativní, komutativní
každý prvek je opačný sám k sobě

Po přejmenování $a=x$, $b=x+1$

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

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

$(F_2(x)/(x^2+x+1)\setminus\{0\}, \cdot)$ - Grupa

•	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Nalezení zbytku

Počítání s polynomy → počítání modulo x^2+x+1

dělení

$x\cdot(x+1) = x^2+x$

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

$-(x^2+x+1)$

$-1 = 1$

$x^2+x \equiv x^2+x+x^2+x+1 = 2x^2+2x+1$

$= 1 \pmod{x^2+x+1}$

$x\cdot x = x^2$

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

$-(x^2+x+1)$

$-x-1 = x+1$

$x^2 \equiv x^2+x^2+x+1$

$= 2x^2+x+1 = x+1 \pmod{x^2+x+1}$

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

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

$-(x^2+x+1)$

$-x = x$

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

$= x^2+1 \equiv x^2+1+x^2+x+1 = x \pmod{x^2+x+1}$

Př. ISBN-10 a) - detekuje jakoukoliv 1 chybu (viz přednáška)

b) - detekuje transpozici symbolů

Ukažte, že tento kód je schopen detekovat transpozici (b)

$\bar{X} = x_1 x_2 \dots x_{10}$ $\quad \sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$

$\bar{y} = y_1 y_2 \dots y_{10}$ ← slovo s chybou pro $j \neq k$ je $y_j = x_k$ a $y_k = x_j$ (transpozice)

$$\sum_{i=1}^{10} i y_i = \sum_{i=1}^{10} i x_i - j x_j - k x_k + j\cdot x_k + k x_j$$

$$= \sum_{i=1}^{10} i x_i + x_k(j-k) - x_j(j-k) =$$

$$= \underbrace{\sum_{i=1}^{10} i x_i}_{\equiv 0 \pmod{11}} + (j-k)(x_k - x_j) \not\equiv 0 \pmod{11}$$

$\overbrace{j-k}^{a} \neq 0$ jinak $j=k$ - není transp.

$\underbrace{x_k - x_j}_{b} \neq 0$ jinak $x_k = x_j$ - stejné symboly, není transp.

$a\cdot b = 0$ pro $a, b \neq 0$

nelze v tělese, kde neexistují děl. 0

a $\mathbb{Z}_{11}$ je těleso.

Poznámka: ISBN-10 nelze použít k opravování chyb.

Pouze v případě, že chybí symbol na dané pozici, pak jsme schopni ho doplnit.

Příklad: Je-li ISBN-10 kód $0-201-1?-502-7$
určete chybějící symbol. $[x = 3]$

$1\cdot 0 + 2\cdot 2 + 3\cdot 0 + 4\cdot 1 + 5\cdot 1 + 6x + 7\cdot 5 + 8\cdot 0 + 9\cdot 2 + 10\cdot 7 \equiv 0 \pmod{11}$

$2 + 6x + 2 + 7 + 4 \equiv 0 \pmod{11}$

$6x + 4 \equiv 0 \pmod{11}$

$6x \equiv 7 \pmod{11}$

$6x \equiv 18 \pmod{11}$

$x \equiv 3 \pmod{11}$

$x = 3$

nebo přes inverzi

$6x \equiv 7 \pmod{11} \;/\cdot 2$

$12x \equiv 14 \pmod{11}$

$x \equiv 3 \pmod{11}$

Příklad: (i) Jaká je min. vzdálenost ISBN-10 kódu? 2

(ii) Jaké procento knih se dá očekávat, že budou mít v ISBN-čísle symbol X?

(iii) Jaká je velikost ISBN-10 kódu

(i) Vzdálenost je 2. Již jsme ukázali, že detekuje jednu chybu $\Rightarrow$ Vzdál. je nejméně 2.
Vzdál není 3. Lehce najdeme 2 čísla, která splňují kontrolní schema ISBN-10 kódu a liší se na dvou pozicích, například:

$$\underbrace{150\,000\,000}_{\bar{x}} \equiv 0 \pmod{11} \quad \text{a} \quad dist(\bar{x}, \bar{y}) = 2$$
$$\underbrace{530\,000\,000}_{\bar{y}} \equiv 0 \pmod{11}$$

(ii) Je-li každá možná 9-tice čísel $x_1, x_2, \ldots, x_9$ stejně pravděpodobná, pak každá 11-tá desetice má na 10-tém místě symbol X.
Proto 1/11 slov ISBN-10 kódu má symbol X.

(iii) Poslední cifra umí vždy zajistit, aby součet v kontr. schematu byl $\equiv 0 \pmod{11}$. Prvních 9 cifer může být libovolných. Lze sestavit 10^9 (miliardu) různých kódových slov.

Příklad: ISBN-13 kód

(i) Kolik chyb dokáže detekovat ISBN-13 kód

Předpokl. že $\bar{x} = x_1 \cdots x_{13}$ je platné slovo ISBN-13 kódu a došlo v něm k jedné chybě. Slovo s chybou ozn. $\bar{y} = y_1 \cdots y_{13}$ a platí, že $y_j \neq x_j$, jinak $y_i = x_i \ \forall i \neq j$.

Pro kontrolní součet platí $\sum_{i=1}^{13} w_i x_i \equiv 0 \pmod{10}$, $w_i = 1$ když i je liché, $w_i = 3$ když i je sudé

Pak • pro j-liché

$$\sum_{i=1}^{13} w_i y_i = \sum_{i=1}^{13} w_i x_i - x_j + y_j \equiv 0 - x_j + y_j \pmod{10}$$

$$y_j - x_j \equiv 0 \pmod{10}$$

$$y_j \equiv x_j \pmod{10} \Leftrightarrow y_j = x_j$$

spor

• pro j-sudé

$$\sum_{i=1}^{13} w_i y_i = \sum_{i=1}^{13} w_i x_i - 3x_j + 3y_j \equiv 0 - 3x_j + 3y_j \pmod{10}$$

$$3y_j \equiv 3x_j \pmod{10}$$

lze krátit číslo nesoudělné s modulem

$$y_j \equiv x_j \pmod{10} \Leftrightarrow y_j = x_j$$

spor

Tj. ISBN-13 detekuje jednu chybu.

(ii) Jaká je min vzdálenost ISBN-13 kódu.

Protože detekuje 1 chybu, vzdálenost je alespoň 2.

Že min vzdálenost není větší, ukážeme nalezením dvou platných kódových slov ve vzdálenosti 2.

$\bar{x} = 1300\ldots0 \Rightarrow 1 \cdot 1 + 3 \cdot 3 + 0 \cdot + 0 = 10 \equiv 0 \pmod{10}$

$\bar{y} = 8400\ldots0 \Rightarrow 1 \cdot 8 + 3 \cdot 4 + 0 \ldots + 0 = 20 \equiv 0 \pmod{10}$

$dist(\bar{x}, \bar{y}) = 2 \Rightarrow dist(ISBN\text{-}13) \leq 2$

Minimální vzdál. je 2.

(iii) Ukažte, že ISBN 13 kód detekuje transpozici dvou sousedních cifer (musí být sousední?)

Ozn $\bar{x} = x_1 \dots x_{13}$ kódové slovo ve kterém dojde k prohození dvou sousedních symbolů a vznikne slovo $\bar{y} = y_1 \dots y_{13}$ takové, že $(y_j = x_{j+1}$ a $y_{j+1} = x_j)$.

Pak z konstr. schema pro ISBN-13 dostaneme (dosadíme)

- pro j - liché

$$\sum_{i=1}^{13} w_i y_i = \sum_{i=1}^{13} w_i x_i - x_j - 3x_{j+1} + y_j + 3y_{j+1} \equiv 3y_{j+1} - x_j + y_j - 3x_{j+1} \pmod{10}$$

$$2y_{j+1} - 2y_j \equiv 0 \pmod{10}$$

$$y_{j+1} - y_j \equiv 0 \pmod{5}$$

$$y_{j+1} \equiv y_j \pmod{5}.$$

To nastane jen když y_{j+1} se liší o 5 od y_j, nebo $y_j = y_{j+1}$ což není transpozice. Tj. pokud dojde k transpozici sousedních symbolů, kód ji detekuje. (Podobně detekuje transpozici symbolů mezi lichou a sudou pozicí kódu. Transpozice symbolů na sudých (resp. lichých) pozicích nebude postřehnuta.

- pro j - sudé

$$\sum_{i=1}^{13} w_i y_i = \sum_{i=1}^{13} w_i x_i - 3x_j - x_{j+1} + 3y_j + y_{j+1} \equiv 3y_j - x_{j+1} + y_{j+1} - 3x_j \pmod{10}$$

$$2y_j - 2y_{j+1} \equiv 0 \pmod{10}$$

$$2(y_j - y_{j+1}) \equiv 0 \pmod{10}$$

$$y_j \equiv y_{j+1} \pmod{5} \iff 5 \mid (y_j - y_{j+1})$$

(5 dělí)

Příklad: V čem je horší oproti ISBN-10 kód, který je tvořen slovy $x_1, x_2, \ldots, x_9, x_{10}$, kde $\sum_{i=1}^{10} x_i \equiv 0 \pmod{11}$ a $x_i \in [0, 9]$? Ukažte, že tento kód detekuje jakoukoli jednu chybu.

Sami DU

Vektorové prostory a podprostory.

Definice Množinu $V(n, q)$ pro nějaké přirozené číslo n a vhodné přirozené číslo q společně s tělesem $GF(q)$ a společně s operacemi sčítání vektorů a násobení vektorů skalárem nazveme *vektorový prostor* nad tělesem $GF(q)$.

Definice Mějme množinu vektorů $M = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_r\}$ prostoru $V(n, q)$. Jestliže M je lineárně nezávislá generující množina nějakého podprostoru C, tak M nazýváme *báze* podprostoru C.

Viz přednáška a částečně další cvičení.