Lin. kód

podprostor v $\mathbb{Z}_p^n$

① popis přes bázi

→ kódování $\mathbb{G}$ (generující matice)

② podprostor lze popsat jako prostor lin. rovnic

$\bar{w} \in K$ iff $\bar{w}$ řeší $\mathbb{H} \cdot \bar{x}^T = \bar{o}^T$

Proč $\begin{pmatrix} \bar{c} \end{pmatrix} \begin{pmatrix} w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

iff $\bar{c}_i \cdot \bar{w} = 0 \quad \forall i$

řádky v $\mathbb{H}$ skalární součin

iff $c_i \perp \bar{w} \quad \forall i \ \forall \bar{w} \in K$

iff $\mathbb{H} = \begin{pmatrix} \bar{c}_1 \\ \bar{c}_{n-k} \end{pmatrix}$ ← v řádcích bázi ortogonálního doplňku k podpr. K

tzv. kontrolní matice pro kód K tj. $K^\perp$

→ řádků je $n-k$ ~ informace

↑ délka slova

Převést $\mathbb{G}$ na $\mathbb{H}$ či naopak

v řádcích $\mathbb{G}$ je báze prostoru řešení $\mathbb{H} \cdot \bar{x}^T = \bar{o}^T$

v řádcích $\mathbb{H}$ je — " — $\mathbb{G} \cdot x^T = \bar{o}^T$

Př. Sestavit k nad $\mathbb{Z}_5$ s $G = \begin{pmatrix} 3 & 3 & 3 & 2 & 4 \\ 0 & 2 & 0 & 0 & 4 \\ 2 & 0 & 1 & 1 & 3 \end{pmatrix}$

Najít H

$$G\bar{x}^T = \bar{o}^T$$

$$\left(G \middle| \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} \right) \underset{\text{gaussova eliminace}}{\sim} \left(\begin{matrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 4 \end{matrix} \middle| \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} \right)$$

$\uparrow \uparrow$

3 rovnice o 5 neznámých volím 2 jako parametr a ... dopočítám

chci jen bázické vektory a ty získám lineárně nezávislou volbou parametrů např. $t = 0$, $s = 0$

$t = 0$, $s = 1$

$\bar{c}_1 = (-2\ 0\ -2\ 1\ 0)$

$\bar{c}_2\ (-2\ -2\ -4\ 0\ 1)$ ← řádky kontrolní matice H

v $\mathbb{Z}_5$

$$H = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \quad = \begin{pmatrix} 3 & 0 & 3 & 1 & 0 \\ 3 & 3 & 1 & 0 & 1 \end{pmatrix}$$

Odvodili jsme vzorec

pro $G_s = (E_k\ B)$ je $H = (-B^T\ E_{n-k})$

Kontrola správnosti:

Pošle $\bar{w} \longrightarrow$ přijmu $\bar{v}$

Předpokládám nejvýše 1 chybu (málo chyb)

$H \cdot v = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = s^T$ tzv. syndrom slova $\bar{v}$

když $\bar{s} = \bar{o}$ v je bez chyby

$\bar{s} \neq \bar{o}$ je tam chyba

Opravování:

Když je právě jedna chyba

$$\bar{r} = \vec{w} + (0\,0\,0\,0\,0\,a\,0\,0)$$

(a na i-tém místě)

chybové slovo $\bar{e}$

Jak se to projeví v syndromu:

$$\bar{s} = H \cdot \bar{r}^T = H(\bar{w} + \bar{e}) = H \cdot \vec{w} + H \cdot \bar{e} =$$

$$\vec{0}^T + H \cdot \begin{pmatrix} 0 \\ 0 \\ a \\ 0 \end{pmatrix}_{\leftarrow i} = a \cdot S_i \quad \text{(i-tý sloupec $\neq \#$)}$$

Určíme-li S_i a a jednoznačně, tak můžeme opravit

$$\vec{w} = \vec{r} - (0\,0\,0\,0\,a\,0\,0)$$

(a na i-tém místě)

Příklad: Zkontrolujte příp. opravte slovo r.
Nejdříve zjistíme, zda $r_1 \in \Pi_5$

$$\bar{r}_1 = (4\,0\,1\,1\,4)$$

$$H \cdot \bar{r}^T = \begin{pmatrix} 3 & 0 & 3 & 1 & 0 \\ 3 & 3 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 0 \\ 1 \\ 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow \text{chyba}$$

NE NE NE NE

Zkusíme opravit

$$= a \cdot S_i \qquad \neq a \begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

$$\neq a \cdot \begin{pmatrix} 3 \\ 3 \end{pmatrix} \qquad = a \begin{pmatrix} 3 \\ 1 \end{pmatrix} - 2\,S_3 \quad \text{jen 3. sloupec a jen 2×}$$

musím odečíst 2 ve 3. pozici

$w_1 = r_1 - (00200) = (40414)$

$r_2 = (40030)$

$H \cdot w_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix} = 5 \begin{cases} 4 \cdot s_2 \\ 2 \cdot s_5 \end{cases}$

	↓				↓
3	0	3	1	0	
3	3	1	0	1	

$\rightarrow w_2 = r_2 - (04000)$

$\rightarrow w_3 = r_2 - (00002)$

Jsou 2 možnosti opravy. Nevíme, které z nich byly poslány

$r_3 = (10004)$

$H \cdot r = = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ jediná šance, že 3 sloupce $a * \begin{pmatrix} 3 \\ 1 \end{pmatrix}$ $\begin{matrix} a=1 \\ a=2 \end{matrix}$ není možné řešení $\Rightarrow$ jsou tam alespoň 2 chyby

<u>Tvrzení</u> jsou-li použité 2 sloupce v matici H libovolně nezávislé, pak lze vždy jednu chybu opravit a 2 chyby lze odhalit, přičemž mají nenulový syndrom

Příkladem je Hammingův kód

nad $\mathbb{Z}_2$ $H = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}$ se skládá

1 – 7 bitově. Různé sloupce nad $\mathbb{Z}_2$ jsou lineárně nezávislé

$S_i \neq a \cdot S_j \quad i \neq j$

$a \in \{0, 1\}$

Tento kód jedna chyba opraví a 2 pozná.

Když S rozšíříme jako binární rozvoj k, tak chyba je na k-té pozici.

Počítání modulo polynom

Věta o dělení se zbytkem pro celá čísla

⇒ konstrukce nad n ⇒ zbytkové třídy nad n neboli jsme $(\mathbb{Z}_n, +, \cdot)$ ... komutativní okruh s jedničkou když $\mathbb{Z}$ prvočíslo jsou moduly tělesa protože nenulové má inverz.

$\mathbb{Z}_p[x]$ {polynom proměnné x nad $\mathbb{Z}_p$} =

$\{ a_n x^n + \dots + a_1 x_1 + a_0 ; \; a_i \in \mathbb{Z}_p \}$

Věta o dělení se zbytkem.

Pro libovolné $a(x), b(x) \neq 0$ v $\mathbb{Z}_p[x]$ existují jednoznačně $q(x), z(x)$ v $\mathbb{Z}_p[x]$ že 1) $a(x) = q(x) \cdot b(x) + z(x)$
2) platí $z < b$

Př: $\mathbb{Z}_5[x]$ $a(x) : b(x)$

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

$:2 = \cdot 2^{-1}$ v algoritmu dělení nahrazeno inverzním k vedoucímu koeficientu.

v $\mathbb{Z}_{n}[x]$ $n+p$ nelze dělit polynomy jejichž vedoucí koef. nemá inverz v $\mathbb{Z}_n$

$\therefore 2^{-1}$ v $\mathbb{Z}_7 = 3$ $3 \cdot 3 = 9 = 4$

$-(3x^3 + 1x^2)$

$x^2 + x$

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

$-x = 4x$ = zbytek

Lze definovat relaci dělí beze zbytku
$a(x) \mid b(x)$ iff $b(x) = q(x) \cdot a(x)$

Přes Vždy lze dělit konstantou $\neq 0$

$b(x) = k \cdot (k^{-1} b(x))$ $k \in \mathbb{Z}_p \setminus \{0\}$

→ lze $a(x) \mid b(x)$, $b(x) \mid a(x)$ přitom $a(x) \neq b(x)$

Tedy se liší jen o konstantní násobek
(tzv. asociované polynomy)

② $\gcd(a(x), b(x)) = d(x)$ to je že

1) $d(x)$ dělí oba
2) $d(x)$ dělitelný každým společným dělitelem

Pozn. Je tolik největších společných dělitelů
kolik je nenulových konstant a jsou
spolu asociované.

Hledání gcd = Euklidův algoritmus
(protože stačí jen to dělení se zbytkem)

Najděte největší spol. dělitel $a(x)$, $b(x)$

$a(x) = 3x^3 + 2x^2 + x$ v $\mathbb{Z}_5[x]$
$b(x) = 2x^2 + 4x$

přidat příklad

1) $a(x) = (4x + 3) \cdot b(x) + 4x$
$b(x) = (3x + 1) \cdot 4x + 0$

$\gcd = 4x$, ale i $k \cdot 4x$ pro $k \in \mathbb{Z}_5 \setminus \{0\}$

$\cdot 4^{-1} = 4 \in \mathbb{Z}_5$

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

$-2x^2$

$4x$

$-4x$

0

Bezoutova věta

$$\gcd(a(x), b(x)) = k(x) \cdot a(x) + l(x)\, b(x)$$

pro $k(x), l(x) \in \mathbb{Z}_p[x]$

Př. $\gcd = 4x = a(x) - (4x+3)\, b(x) =$

$= \underbrace{1}_{k(x)} \cdot a(x) + \underbrace{(x+2)}_{l(x)} b(x)$

Řešení polynomiálních rovnic

$a(x) \cdot \varphi(x) = b(x)\, k(x) = c(x)$ a, b, c zadaná

má řešení iff $\gcd(a(x), b(x)) \mid c(x)$

dělí

pak $(r, s) = (r_p, s_p) + k(x) \cdot (r_0, s_0)$

rozšíř. Euklid partikulární řeš. homogenní rov.

Př. v $\mathbb{Z}_7[x]$ řešte

$$\underbrace{(2x^3+2x^2+x)}_{a(x)}\cdot r(x)+\underbrace{(2x^2+4x)}_{b(x)}\cdot s(x)=2x^2$$

$$4x = 1\cdot a(x) + (x-12)\,b(x)$$

$$2x = 3x(4x) = \underbrace{3x}_{\text{NP}}\, a(x) + \overbrace{\underbrace{(3x^2+3)}_{3\cdot(x+2)}}^{\text{NP}}\, b(x)$$

Nesoudělné řešení homogenní rovnice

$$(3x^3+2x^2+x)\,r(x)+(2x^2+4x)\,s(x)=0 \qquad /:\text{gcd}$$

$$\underbrace{(2x^2+3x+4\cdot 1)}_{s_0}\,r(x)+\underbrace{(3x+1\cdot 1)}_{-r_0}\cdot s(x)=0 \qquad :4=4^{-1}=\cdot 4$$

$$r(x) = 3x + b(x)\cdot(2x+4)$$

$$s(x) = (3x^2+x)+b(x)(2x^2+3x+4)$$

$$b(x)\in\mathbb{Z}_7[x]$$

Def: Kongruence modulo polynom

$a(x) \equiv b(x) \pmod{q(x)}$

iff $q(x) \mid (b(x) - a(x))$

když $a(x)$ i $b(x)$ mají stejný zbytek po dělení $q(x)$

Platí $\equiv (\mathrm{mod}\ q(x))$ je ekvivalence a je respektována "+" a "·"

Rozbije $\mathbb{Z}_p[x]$ na zbytkové třídy, "+","·" lze definovat na třídách přes reprezentanty

Vezmeme faktorový okruh modulo polynom $q(x)$

Značí se $\mathbb{Z}_p/_{q(x)}$ = { třída, polynom $a(x) \in \mathbb{Z}_p[x]$ a stupeň $< q$ }

zbytková třída mod $q(x)$

Když st $= k$

$a(x) = a_{k-1}x^{k-1} + \ldots + a_1 x + a_0$; $a_i \in \mathbb{Z}_p$

p^k možností (zbytková třída)

Řešení lin. rovnice v $\mathbb{Z}_p[x]/_{q[x]} = A$

$a(x) \cdot r(x) = c(x)$ v A

$a(x) \cdot r(x) + q(x) \cdot s(x) = c(x)$ v $\mathbb{Z}_p[x]$

má řešení když

dělí

$gcd(a(x), q(x)) \mid c(x)$

$r(x) = r_p + b(x) \cdot r_0$

– různá řešení budou pro $b(x) \in \mathbb{Z}_p[x]$

že $st(b(x) \cdot r_0) < st\, q$

spec. $a(x)^{-1}$ v $\mathbb{Z}_p[x]/q(x)$

existuje když $a(x)$ je nesoudělné s $q(x)$

Příklad $A = \mathbb{Z}_3[x]/x^2+1$

$|A| = p^k = 3^2 = 9$

$A = \{ ax + b,\ a,b \in \mathbb{Z}_3 \}$

$+ \cdot$ mod x^2+1 mod $\mathbb{Z}_3$

$(2x) + x + 2 = 3x + 2 = 2$

0

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

4

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

-2 zbytek

Buď $(2x^2 + x) : (x^2+1) = 2$

$\underline{-2x - 2}$

$x + 1$

Najít $(2x+1)^{-1} = r(x)$

$\text{alg}_{\mathbb{Z}}\ (2x+1)\cdot r(x) = 1 \quad \nearrow A$

$(2x+1)\,s(x) + (x^2+1)\,t(x) = 1 \quad \nearrow \mathbb{Z}[x]$

Stačí Euklidův algoritmus. Inverze jednotek je tak, že jsou jedna. Stačí mají partikulární řešení

① $(x^2+1) = (2x+2)(2x+1) + (-1)$

② $\qquad\qquad\qquad\qquad\quad + \quad 0$

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

$\qquad\ \ w \qquad\qquad\ \ r(x)$

$\qquad\ s(x)$

inverze $(2x+1)^{-1} = 2x+2$

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

$-x-2x$

$x+1 \qquad \cdot 2^{-1} = \cdot 2 \quad \nearrow \mathbb{Z}_3$

$-x-2$

$-1 \cdot 2$