LINEÁRNÍ ALGEBRA NAD $\mathbb{Z}_p$

09

$\mathbb{Z}_p$ je podobné $\mathbb{R}$ → $\mathbb{Z}_p$ je těleso jako $\mathbb{R}$ je těleso → fungují obdobně ($\neq \mathbb{Z}_n$ NE!)

ALE pouze když pracuji s prvočísly

SOUSTAVY LINEÁRNÍCH ROVNIC V $\mathbb{Z}_p$

Pozn.: 1 lin. rov. o 1 neznámé

$$ax = b \quad v \ \mathbb{Z}_n$$

může NEmít řešení, či mít více řešení

více rovnic o více neznámých nad $\mathbb{Z}_n$, kde $n \neq p$ (n není prvočíslo), nebudeme řešit.

Druhý důvod: nad $\mathbb{Z}_n$, kde $n \neq p$, nefungují obecně Gaussova eliminace

(PŘ) v $\mathbb{Z}_5$ řešte

$$\begin{aligned} 4x + y + 2z + 2w &= 4 \\ 3x + y \quad\quad + 3w &= 3 \\ 4x + 2y + z + 3w &= 4 \end{aligned}$$

Řešení Gaussovou eliminací – v $\mathbb{Z}_5$

$$\left(\begin{array}{cccc|c} 4 & 1 & 2 & 2 & 4 \\ 3 & 1 & 0 & 3 & 3 \\ 4 & 2 & 1 & 3 & 4 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 4 & 3 & 3 & 1 \\ 0 & -1 & 1 & -1 & 0 \\ 0 & 1 & -1 & 1 & 0 \end{array}\right) \begin{array}{ll} 4^{-1}\check{r}_1 = 4.\check{r}_1 & (2) \\ \check{r}_2 - 3\check{r}_1 & (3) \\ \check{r}3 - \check{r}1 & (1) \end{array}$$

$$\sim \left(\begin{array}{cccc|c} \cdot & & & & \\ \cdot & & \nearrow & & \\ \cdot & & & & \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \check{r}_3 + \check{r}_2$$

$$\sim \left(\begin{array}{cccc|c} 1 & 0 & 2 & 4 & 1 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ & & \uparrow_k & \uparrow_s & \end{array}\right) \begin{array}{l} \check{r}_1 - \check{r}_2 \quad (3) \\ -\check{r}_2 \quad (2) \\ \check{r}_3 + \check{r}_2 \quad (1) \end{array}$$

$$(x, y, z, w) = (1-2k-4s,\ k-s,\ k,\ s) \qquad k, s \in \mathbb{Z}_5$$

$\rightarrow$ bude $5^2 = 25$ řešení

$$= \underbrace{(1,0,0,0)} + k(3,1,0) + s\underbrace{(1,4,0,1)}$$

(minusy přeneseny na +)

x_p = partikul. řeš.

podprostor řešení homog. rovn.

$\bar{x}_0 = k \cdot \bar{b}_1 + s\bar{b}_2$

Obecně: lineární soustava nad $\mathbb{Z}_p$ může mít – žádné
– jedno
– p^k } řešení

$\bar{x} = \bar{x}_p + \bar{x}_0$

Každé řešení homog. soustavy tvoří podprostor v $\mathbb{Z}_p^n$.

MATICOVÝ POČET

bez dělat nad $\mathbb{Z}_n$ vždy

Regulární matice nad $\mathbb{Z}_n$ = čtvercová matice, jejíchž determinant má inverzi v $\mathbb{Z}_n$.

Budou $A^{-1} = (\det A)^{-1} \cdot D^T$

A^{-1} ⇗ inverzní matice

D^T ↑ transponovaná matice doplňků

$D = \left((-1)^{i+j} \cdot \det A_{i,j}\right)$

$A_{i,j}$ ↑ podčtverc. mat.

v $\mathbb{Z}_p$ funguje GEM

$$(A|E) \sim \dots (E|A^{-1})$$

LINEÁRNÍ PROSTORY, PODPROSTORY

Uspořádaná n-tice nad $\mathbb{Z}_p$

$$\mathbb{Z}_p^n = \{(x_1, \dots x_n),\ x_i \in \mathbb{Z}_p\}$$

$+, \alpha.$ ← mají splňovat „běžné vlastnosti", aby to byl lineární prostor

$\alpha \in \mathbb{Z}_p$ ↑ skalární násobky

doplníme ještě skalárním součinem

$\vec{u} \odot \vec{v} = u_1 v_1 + \dots u_n v_n$

→ lze měřit úhly

$\vec{u} \perp \vec{v}$ iff $\vec{u} \odot \vec{v} = 0$

LINEÁRNÍ KÓDY

kódování → k informačním znakům přidám kontrolní, aby šlo ověřit, zda při přenosu nedošlo k chybě, event. aby šlo chybu opravit

lineární kódování → přidám znaky tak, aby slovo bylo z lin. podprostoru

(DEF) **Lineární kód délky n s k info-znaky** nad $\mathbb{Z}_p$ je podprostor v $\mathbb{Z}_p^n$ dimenze k

Jsou 2 možnosti jak popsat podprostory

① přes bázi → použije se ke kódování

② přes homog. soustava rovnic → použije se ke kontrole, zda je bezchybný

Kód K

ad ①

kódování = přiřazení informací $\bar{a} = (a_1, \dots, a_k)$

kódové slovo $\bar{w} = (w_1, \dots w_n) \in K$

je dáno volbou báze

info jsou souřadnice $\bar{w}$ vůči bázi $\bar{b}_1, \dots, \bar{b}_k$ $\quad \bar{a} \to \bar{w} = a_1\bar{b}_1 + \dots + a_k\bar{b}_k$

$$= \bar{a} \begin{pmatrix} \bar{b}_1 \\ \bar{b}_2 \\ \vdots \\ \bar{b}_k \end{pmatrix}$$

$$\boxed{\bar{w} = \bar{a} \cdot G_1}$$

G_1 → kan. generující matice

(v řádcích má bázi kódu K) $\bar{w} = \bar{a} \cdot G_1$

Systematické kódování = informace ukládané na začátku kódového slova

$\bar{a} \to \bar{w} = (\underbrace{a_1, \dots a_k}_{\text{info}}, \underbrace{b_1, \dots b_{n-k}}_{\text{kontrolní znaky}})$

Potřebuje $G_{1s} = (E\ B)$

Dekódování = najít souřadnice $\bar{w}$ vůči bázi v G_1. U system. kód. snadné.

(PŘ) lineární kód nad Z_5 má $G_1 = \begin{pmatrix} 3 & 3 & 3 & 2 & 4 \\ 0 & 2 & 0 & 0 & 4 \\ 2 & 0 & 1 & 1 & 3 \end{pmatrix}$

1) ? délka kódových slov
~~2)~~ ? počet informací
~~3)~~ ? počet kódových slov

~~4)~~ = 5 → jak jsou dlouhá slova, tak jsou dlouhé řádky
použiji předpoklad $G_1 = \begin{pmatrix} \bar{b}_1 \\ \bar{b}_2 \\ \bar{b}_3 \end{pmatrix}$

~~2)~~ = 3

~~3)~~ $= 5^3 = 125$ $\quad K = \{ \bar{w} = \alpha_1 \bar{b}_1 + \alpha_2 \bar{b}_2 + \alpha_3 \bar{b}_3,\ \alpha_i \in Z_5 \}$

2) Zakódujte info ~~$\bar{a} = (1, 1$~~ ~~$\bar{a} = (1, 1$~~

$$\bar{a} = (1\ 2\ 3)$$

$$\bar{w} = \bar{a} \cdot G_7 = (1\ 2\ 3) \cdot \begin{pmatrix} & \\ & G_7 \\ & \end{pmatrix} = (4\ 2\ 1\ 0\ 1)$$

3) Najdi systemat. generující matici G_{7s} a znovu zakódovat $\bar{a} = (1\ 2\ 3)$

$$G_7 = \begin{pmatrix} 2 & 0 & 1 & 1 & 3 \\ 0 & 2 & 0 & 0 & 4 \\ 0 & 3 & 4 & 3 & 2 \end{pmatrix} \begin{matrix} \cdot \bar{x}_3 \\ \\ \cdot \bar{x}_1 + \bar{x}_3 \end{matrix} \quad \begin{matrix} ② \ /\cdot 2^{-1} \\ /\cdot 2^{-1} \sim \dots \sim \\ ① \end{matrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix} = G_{7s}$$

$$\bar{u} = \bar{a} \cdot G_{7s} = (1\ 2\ 3) \cdot \begin{pmatrix} & \\ & G_{7s} \\ & \end{pmatrix} = (1\ 2\ 3\ 3\ 3)$$

Pozn.: GEM převádí jednu bázi na jinou bázi lineárního podprostoru tj. G_7, G_{7s} generují stejný kód