Lineární algebra nad $\mathbb{Z}_m$ (dokončení), lineární kódy

Minule:

soustavy lineárních rovnic nad $\mathbb{Z}_p$, p prvočíslo, stejně jako nad $\mathbb{R}$.
Dále nad $\mathbb{Z}_p$ stejně jako nad $\mathbb{R}$:

1. Vektorový (lineární) prostor, dimense, báze, souřadnice vzhledem k bázi.
   Například: $(\mathbb{Z}_p)^n$ vektorový prostor dimense n nad $\mathbb{Z}_p$.
2. Vektorový (lineární) podprostor, dimense, báze, souřadnice vzhledem k bázi.
   Například:

   $$\{\alpha \cdot (2,1,3,4,7) + \beta \cdot (0,2,7,5,4) \mid \alpha, \beta \in \mathbb{Z}_{13}\}$$

   vektorový podprostor $(\mathbb{Z}_{13})^5$ dimense 2.
   Báze: $g_1 = (2,1,3,4,7)$, $g_2 = (0,2,7,5,4)$.
   Souřadnice $(12,10,6,8,50)$ vzhl. k bázi: $(6,2)$.
   Protože $(12,10,6,8,50) = 6 \cdot (2,1,3,4,7) + 2 \cdot (0,2,7,5,4)$.

3. Ortogonální doplněk vektorového podprostoru.
Například: ortogonální doplněk k

$$\{\alpha \cdot (2,1,3,4,7) + \beta \cdot (0,2,7,5,4) \mid \alpha, \beta \in \mathbb{Z}_{13}\}$$

má dimensi 3 ($= 5 - 2$) a jeho báze je (jakýkoli) fundamentální systém soustavy

$$\begin{pmatrix} 2 & 1 & 3 & 4 & 7 \\ 0 & 2 & 7 & 5 & 4 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = 0$$

nad $\mathbb{Z}_{13}$.
Protože: prvky ortogonálního doplňku jsou vektory kolmé na všechny vektory původního prostoru.

Nad $\mathbb{Z}_m$, když m není prvočíslo:

1. Aritmetika matic: sčítání a násobení stejně jako nad $\mathbb{R}$.
2. GEM se chová podivně: cokoli, založené na GEM nebudeme používat. Tj. řešení soustav, hodnost matice, ...
3. Determinant čtvercové matice stejně jako nad $\mathbb{R}$ (rekursivní definice).

Věta (inverse matice nad obecným $\mathbb{Z}_m$)

Čtvercová matice $\mathbb{A}$ nad $\mathbb{Z}_m$ má inversi právě tehdy, když $\det \mathbb{A}$ *má inversi v $\mathbb{Z}_m$.*
Pak

$$\mathbb{A}^{-1} = (\det \mathbb{A})^{-1} \cdot \mathbb{D}^{\top}$$

kde $\mathbb{D}$ je matice algebraických doplňků[a] *matice $\mathbb{A}$.*

[a] Položka d_{ij} matice $\mathbb{D}$ je alg. doplněk prvku a_{ij}. Je to číslo $(-1)^{i+j} \cdot \det A_{ij}$, kde A_{ij} vznikla z matice $\mathbb{A}$ vynecháním i-tého řádku a j-tého sloupce.

Příklad

Pokud existuje, nalezněte inversi k matici

$$\mathbb{A} = \begin{pmatrix} 2 & 3 & 5 \\ 5 & 11 & 2 \\ 1 & 2 & 2 \end{pmatrix}$$

nad $\mathbb{Z}_{26}$.
Postup:

1. 26 není prvočíslo: nemůžeme použít GEM.
2. $\det \mathbb{A} = 7$ v $\mathbb{Z}_{26}$ (nemůžeme použít GEM).
3. 7^{-1} v $\mathbb{Z}_{26}$ existuje (sice $7^{-1} = 15$). Proto existuje i inverse k matici $\mathbb{A}$.

Příklad (pokrač.)

4. Spočteme matici $\mathbb{D}$ algebraických doplňků:

$$\mathbb{D} = \begin{pmatrix} 18 & 18 & 25 \\ 4 & 25 & 25 \\ 3 & 21 & 7 \end{pmatrix}$$

5. Inverse:

$$\mathbb{A}^{-1} = 15 \cdot \begin{pmatrix} 18 & 18 & 25 \\ 4 & 25 & 25 \\ 3 & 21 & 7 \end{pmatrix}^{\top} = \begin{pmatrix} 10 & 8 & 19 \\ 10 & 11 & 3 \\ 11 & 11 & 1 \end{pmatrix}$$

Příklad (Rovina v $\mathbb{R}^3$ jako lineární kód)

Rovina $x + y - z = 0$ je lineární podprostor V dimense 2 v $\mathbb{R}^3$.

1. Volbou báze V lze generovat prvky V.
   1. V má bázi (např.): $g_1 = (1, 2, 3)$, $g_2 = (0, 1, 1)$.
   2. Tudíž $v \in V$ iff existují $a_1, a_2 \in \mathbb{R}$ tak, že $a_1 \cdot g_1 + a_2 \cdot g_2 = v$. (Protože báze určuje systém souřadnic.)
   3. Neboli: volbou a_1, a_2 lze vygenerovat $v \in V$ takto:

$$v = (a_1, a_2) \cdot \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \end{pmatrix}}_{\text{generující matice } \mathbb{G}}$$

Příklad (Rovina v $\mathbb{R}^3$ jako lineární kód, pokrač.)

Rovina $x + y - z = 0$ je lineární podprostor V dimense 2 v $\mathbb{R}^3$.

1. Volbou ortogonálního doplňku V lze testovat, zda vektory leží ve V.
   1. V má ortogonální doplněk (např.): $h_1 = (1, 1, -1)$.
   2. Tudíž $v \in V$ iff $h_1 \cdot v = 0$. (Protože ortogonální doplněk tu je normálový vektor.)
   3. Neboli: syndrom s vektoru $v = (v_1, v_2, v_3)$

$$s = \underbrace{\begin{pmatrix} 1 & 1 & -1 \end{pmatrix}}_{\text{kontrolní matice } \mathbb{H}} \cdot \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$$

určuje míru příslušnosti do V.

Tyto úvahy zobecníme

1. Vektorový prostor $\mathbb{R}^3$ nahradíme vektorovým prostorem $(\mathbb{Z}_p)^n$, p prvočíslo.
2. Rovinu v $\mathbb{R}^3$ nahradíme vektorovým podprostorem V v $(\mathbb{Z}_p)^n$ dimense k.

Předcházející geometrická interpretace však zůstává stejná!

Příklad (ISBN — International Standard Book Number)

Deset cifer: použity symboly z množiny $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}$, chápáno jako $\mathbb{Z}_{11}$.
Příklad:

$$80-7203-438-3$$

kde jednotlivé skupiny znamenají:

1. 80 jazyk knihy (čeština)
2. 7203 nakladatelství (Argo)
3. 438 číslo knihy, přidělené nakladatelstvím
4. 3 kontrolní bit

Obecně: $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$, kde $\sum_{i=1}^{10} ix_i = 0$ v $\mathbb{Z}_{11}$.

Příklad (ISBN, pokrač.)

Kdy je řetězec $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$ kódem ISBN?
Právě když jeho syndrom

$$\underbrace{(1,2,3,4,5,6,7,8,9,X)}_{\text{kontrolní matice } \mathbb{H} \text{ kódu ISBN}} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \end{pmatrix}$$

je nula (počítáno v $\mathbb{Z}_{11}$).

Příklad (ISBN, pokrač.)

Jak vytvořit kód ISBN?
Info o knize = 9 bitů. Jak spočítat kontrolní bit?

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) \cdot \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 9 \end{pmatrix}}_{\text{generující matice } \mathbb{G} \text{ kódu ISBN}}$$

$$= (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}) \text{ v } \mathbb{Z}_{11}.$$

Příklad (ISBN, pokrač., geometrický pohled)

1. Kódy ISBN = prvky vektorového podprostoru V ve vektorovém prostoru $(\mathbb{Z}_{11})^{10}$.
   Báze prostoru V = řádky matice $\mathbb{G}$.
   Dimense $V = 9$.
2. Info o knize = souřadnice $v \in V$ vzhledem k bázi.
3. Test při příjmu = syndrom $\mathbb{H}v$.
   Řádky $\mathbb{H}$ = báze ortogonálního doplňku k V.

Kód ISBN = lineární 11-kód délky 10 a dimense 9.
Je schopen detekovat jednu chybu a prohození dvou pozic.[a]

---

[a] To jsou běžné písařské chyby. ISBN je starý kód, začíná být nahrazován ISBN 13.

Lineární p-kód délky n a dimense k

Chceme zabezpečit data před poškozením.
V podprostor $(\mathbb{Z}_p)^n$ dimense k.
Terminologie:

1. $v \in V$ je kódové slovo (ta budeme posílat).
2. Báze $g_1, \dots, g_k$ prostoru V jako řádky matice $\mathbb{G}$: generující matice.
3. $v \in V$ iff $v = \sum_{i=1}^{k} \alpha_i \cdot g_i$.
   Souřadnice v vzhledem ke $\mathbb{G}$: $(\alpha_1, \dots, \alpha_k)$ jsou informační bity.
4. Báze ortogonálního doplňku k V, zapsaná jako řádky matice $\mathbb{H}$: kontrolní matice.
5. $v \in V$ iff $\mathbb{H}v = 0$ iff syndrom slova v je 0 (test při příjmu).

Příklad (Lineární 2-kód délky 7 a dimense 4)

V podprostor $(\mathbb{Z}_2)^7$ dimense 4 s generující maticí

$$\mathbb{G} = \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Posílání zprávy:

1. 4 info bity $=$ souřadnice vzhledem ke $\mathbb{G}$.
2. $7 - 4 = 3$ redundantní bity $=$ dimense ortogonálního doplňku.
3. Například: info $= (0, 1, 1, 1)$. Pošleme
   $v = (0, 1, 1, 1) \cdot \mathbb{G} = (0, 1, 1, 1, 1, 0, 0)$.

Příklad (pokrač.)

Spočteme kontrolní matici (= báze ortogonálního doplňku):

$$\mathbb{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Ideální kód, pokud došlo k nejvýše jedné chybě. Přijímání zprávy:

1. Přijmeme w a předpokládáme, že došlo k nejvýše jedné chybě. Tj. $w = v + e$ (v je kódové slovo a e je error pattern, e obsahuje nejvýše jednu jedničku).
2. Spočteme syndrom s slova w: $s = \mathbb{H}w = \mathbb{H}e$. Jestliže $s = 0$, při přenosu nedošlo k chybě. Jestliže s je i-tý sloupec $\mathbb{H}$, došlo k chybě na i-tém místě, opravíme.
3. Izolujeme info bity.

Vztah matice $\mathbb{G}$ s maticí $\mathbb{H}$

V prostor dimense k, řádky matice $\mathbb{G}$ = báze V, $\mathrm{rank}(\mathbb{G}) = k$.

$V^\perp$ ortogonální doplněk prostoru V, dimense $(n-k)$. Řádky matice $\mathbb{H}$ = báze $V^\perp$, $\mathrm{rank}(\mathbb{H}) = n-k$.

Tj. $\mathbb{G} \cdot \mathbb{H}^\top = 0$.

1. Známe $\mathbb{G}$: řádky matice $\mathbb{H}$ jsou fundamentální systém rovnice $\mathbb{G}x = 0$.
2. Známe $\mathbb{H}$: řádky matice $\mathbb{G}$ jsou fundamentální systém rovnice $\mathbb{H}x = 0$.
3. Je-li $\mathbb{G} = (\mathbb{E}|\mathbb{B})$ (tj., když V je systematický kód), pak $\mathbb{H} = (-\mathbb{B}^\top|\mathbb{E}')$.

Další informace a historie:

1. Richard Wesley Hamming (1915–1998): Bellovy laboratoře, ∼1946, technika pro opravu chyb na děrných štítcích, http://www-gap.dcs.st-and.ac.uk/∼history/Biographies/Hamming.html
2. J. Adámek, *Foundations of Coding*, John Wiley & Sons, New York, 1991
3. D. J. C. MacKay, *Information Theory, Inference and Learning Algorithms*, Cambridge Univ. Press, 2003