Algoritmy na mřížích

Pavel Příhoda

3. listopadu 2021

Obsah

1 Úvod

Definice 1.1. Mříž v n-dimenzionálním prostoru je množina $L \subseteq \mathbb{R}^n$ taková, že $\exists b_1, b_2, \ldots, b_d \in \mathbb{R}^n, \mathrm{LN}\,(\text{nad } \mathbb{R})$ tak, že $L = \mathbb{Z}b_1 + Zb_2 + \cdots + \mathbb{Z}b_d = \{z_1b_1 + z_2b_2 + \cdots + z_db_d | z_1, \ldots z_d \in \mathbb{Z}\}$.

Poznámka 1.2. $\{b_1, b_2, \ldots, b_d\}$ se nazývá *báze* L. Není určená jednoznačně. $d = \dim < L >$, d je hodnost (rank) určená množinou L, $0 \leq d \leq n$.

1.1 Algebraická struktura mříží

- L je komutativní grupa (podgrupa grupy $(R^n, +)$)
- L je konečně generovaná (báze je množina generátorů)
- L je beztorzní ($\forall z \in \mathbb{Z}\ \forall \underline{l} \in L : z \cdot \underline{l} = 0 \implies z = 0 \vee \underline{l} = 0$)

Věta 1.3. *Každá beztorzní konečně generovaná komutativní grupa je volná.*

Důsledek 1.4. $(L, +) \simeq (\mathbb{Z}^d, +)$

Definice 1.5 (Euklidovská norma v $\mathbb{R}^n$). Nechť $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$, $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$. Potom standradní skalární součin $\cdot$ definujeme jako $u \cdot v = \sum_{i=1}^n u_i v_i = u^T v$. *Euklidovskou normu* definujeme jako $\|u\| := \sqrt{u \cdot u} = \left(\sum_{i=1}^n u_i v_i\right)^{\frac{1}{2}}$.

1.2 Rozložení mříže v $\mathbb{R}^n$

Definice 1.6 (Diskrétní podgrupy $(\mathbb{R}^n, +)$). Podgrupa $G \subseteq (\mathbb{R}^n, +)$ je *diskrétní*, pokud

$$\forall g \in G\ \exists \varepsilon > 0 : G \cap \{v \in \mathbb{R}^n \,|\, \|v - g\| < \varepsilon\} = \{0\}.$$

Pozorování 1.7. $G \subseteq (\mathbb{R}^n, +)$ je diskrétní $\iff \exists \varepsilon > 0 : G \cap \{v \in \mathbb{R}^n \,|\, \|v\| < \varepsilon\} = \{0\}$

Důkaz. $\Rightarrow$ ✓
$\Leftarrow$ vezmi $\varepsilon > 0$ tak, aby platila pravá strana tvrzení. Zvol $g \in G$ libovolné. Potom pro každé $v \in G$ splňující $\|v - g\| < \varepsilon$ platí $v = g$, neboť $v - g \in G$ a tedy z předpokladu $v - g = 0$.
Celkem tedy $G \cap \{v \in \mathbb{R}^n \,|\, \|v - g\| < \varepsilon\} = \{g\}$. □

Důsledek 1.8. *Je-li $G \subseteq (\mathbb{R}^n, +)$ diskrétní, pak $\forall M \in \mathbb{R}^+\ |\{g \in G | \|g\| < M\}| < \infty$.*

Důkaz. $B_M := \{v \in \mathbb{R}^n \,|\, \|v\| < M\}$, $B_\varepsilon := \{v \in \mathbb{R}^n \,|\, \|v\| < \varepsilon\}$, kde $\varepsilon > 0$ splňuje $B_\varepsilon \cap G = \{0\}$. $X := G \cap B_M$, $B_{\frac{\varepsilon}{2}} := \{v \in \mathbb{R}^n \,|\, \|v\| < \frac{\varepsilon}{2}\}$. Potom $\forall g_1, g_2 \in G : g_1 \neq g_2 \implies (g_1 + B_{\frac{\varepsilon}{2}}) \cap (g_2 + B_{\frac{\varepsilon}{2}}) = \emptyset$, neboť $\|g_1 - g_2\| \geq \varepsilon$.

$$\dot{\bigcup_{x \in X}} x + B_{\frac{\varepsilon}{2}} \subseteq B_{M+\varepsilon}$$

$$|X| \cdot \mathrm{vol}(B_{\frac{\varepsilon}{2}}) \leq \mathrm{vol}(B_{M+\varepsilon})$$

$$|X| \leq \frac{\mathrm{vol}(B_{M+\varepsilon})}{\mathrm{vol}(B_{\frac{\varepsilon}{2}})} < \infty$$

□

Tvrzení 1.9. *Každá n-dimenzionální mříž je diskrétní podgrupa* $(\mathbb{R}^n, +)$.

Důkaz. Indukcí dle hodnosti mříže $L(d)$. (Případ $d = 0$ platí, ale vynecháme jej.)
$\boxed{d=1}$ tj. $\exists_1 \in \mathbb{R}^n$, $b_1 \neq 0$, $L = \mathbb{Z}b_1$ $0 \neq b \in L \iff l = zb_1,\ z \in \mathbb{Z}\setminus\{0\}$.
$\|l\| = |z| \cdot \|b_1\| \geq \|b_1\| \implies \varepsilon = \|b_1\|$ projde.
$\boxed{d>1}$ $\{b_1, \ldots, b_d\}$ báze L. Definujme $L_0 = \mathbb{Z}b_1 + \mathbb{Z}b_2 + \cdots + \mathbb{Z}b_{d-1}$. To odpovídá bázi $\{b_1, \ldots, b_{d-1}\}$, potom z indukčního předpokladu $\exists \varepsilon_0 > 0$ takové, že $\forall l \in L_0 \setminus \{0\}$ $\|l\| \geq \varepsilon_0$. Platí, že $\mathbb{R}^n = \langle L_0 \rangle \oplus \langle L_0 \rangle^\perp$. Z toho plyne $\forall v \in \mathbb{R}^n$ $\exists v_0, v^\perp \in \mathbb{R}^n$ $v = v_0 + v^\perp$, $v_0 \in \langle L_0 \rangle$, $v^\perp \in \langle L_0 \rangle^\perp$.

$$0 \neq l = z_1 b_1 + z_2 b_2 + \cdots + z_d b_d,\ z_1, \ldots, z_d \in \mathbb{Z}$$

1. $z_d = 0 \implies l \in L_0 \setminus \{0\} \overset{\text{I.P.}}{\implies} \|l\| \geq \varepsilon_0$ a důkaz je hotov, nebo
2. $z_d \neq 0$ … $l = l_0 + l^\perp \implies \|l\| \geq \|l^\perp\| = \|z_d b_d^\perp\|$
   $b_d \notin L_0$, neboť $b_1, \ldots, b_d$ jsou LN $\implies b_d = \underset{\in L_0}{b_{d_0}} + \underset{\neq \emptyset}{b_d^\perp} \implies \|l\| \geq |z_d| \cdot \|b_d^\perp\| \geq \|b_d^\perp\| > 0$.
   Tedy platí, že $\|l\| \geq \min\{\varepsilon_0, \|b_d^\perp\|\}$

□

2 Výpočetní problémy na mřížích

SVP - shortest vector problem

Definice 2.1 (První postupné minimum). Nechť $0 \neq L \subseteq (\mathbb{R}^n, +)$ je n-dimenzionální mříž. Definujeme *první postupné minimum* $\lambda_1(L) := \min\{\|v\| : 0 \neq v \in L\}$. Toto minimum existuje, neboť $\forall l : 0 \neq l \in L$, $\{v \in L \setminus \{0\} : \|v\| \leq \|l\|\}$ je konečná.

Definice 2.2 (Nejkratší vektor L). Nechť $0 \neq L \subseteq (\mathbb{R}^n, +)$ je n-dimenzionální mříž. v je *nejkratší vektor* L, pokud $\|v\| = \lambda_1(L)$

Poznámka 2.3. v je nejkratší vektor $L \iff -v$ je nejkratší vektor L.

Poznámka 2.4. $L = \mathbb{Z}^2 \subseteq (\mathbb{R}^2, +)$ má tyto nejkratší vektory: $\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\-1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}-1\\0\end{pmatrix}$.

Definice 2.5 (Formulace SVP).
Vstup: Mříž zadaná bází.
Výstup: Nejkratší vektor L (stačí jeden libovolný).

Věta 2.6 (M. Ajtai, 1998). SVP *je* NP*-hard (*NP*-těžký).*

Definice 2.7 (SVP$_\gamma$). (aproximační verze SVP)
Definujeme aproximační faktor $\gamma : \mathbb{N} \to \mathbb{R}^+$.
Vstup SVP$_\gamma$: n-dimenzionální mříž zadaná bází.
Výstup: $0 \neq v \in L$ takový, že $\forall 0 \neq v \in L : \gamma(n) \cdot \|u\| \geq \|v\|$.

Věta 2.8 (A. K. Lenstra, H. W. Lenstra, L. G. Lowász, 1982).

$$\text{SVP}_{2^{\frac{n-1}{2}}}$$

je řešitelný v polynomiálním čase.

Definice 2.9 (Gap SVP$_\gamma$). (rozhodovací verze SVP$_\gamma$)
$L \subseteq (\mathbb{R}^n, +)$ mříž, úplná (hodnost $= n$), víme, že $\lambda_1(L) \leq 1$ nebo $\lambda_1(L) \geq \gamma(n)$. Máme rozhodnout, který případ nastává.

Learning with errors: Odvozuje se od BDD_γ (bounded distance decoding)

Definice 2.10 (BDD_γ - bounded distance decoding). $L \subseteq (\mathbb{R}^n, +), v \in \mathbb{R}^n$. Víme: $dist(v, L) < \frac{\lambda_1(L)}{2\gamma(n)}$. Chceme najít vektor $l \in L$, který tuto nerovnost dokazuje, tedy splňuje

$$\|v - l\| < \frac{\lambda_1(L)}{2\gamma(n)}$$

.

Poznámka 2.11. $l_1 \neq l_2 \in L$, $\|l_1 - l_2\| \geq \lambda_1(L)$
Pak $|\{u \in \mathbb{R}^n : \|u - v\| < \frac{\lambda_1(L)}{2} \cap L\}| \leq 1$

Definice 2.12 (i-té postupné minimum). $L \subseteq (\mathbb{R}^n, +)$ mříž hodnosti d. Pro $i \in \{1, \ldots, d\}$ definujeme *i-té postupné minimum* $\lambda_i(L) = \min\{r \in \mathbb{R} : L\text{obsahuje i LN vektorů normy } \leq r\}$

Definice 2.13 (SIVP_γ - short independent vectors problem). Dána $L \subseteq (\mathbb{R}^n, +)$ úplná. Chceme nalézt $S = \{s_1, \ldots, s_n\} \subseteq L$ lineárně nezávislé tak, aby $\|s_i\| \leq \gamma(n) \cdot \lambda_n(L)$.

Definice 2.14 ($\text{SIS}_{n,q,s,m}$ - short integer soultion). Nechť $q \in \mathbb{N}$. Volíme náhodně $a_1, a_2, \ldots, a_m \in \mathbb{Z}_q^n$. $A := (a_1|a_2|\cdots|a_m)$, $n \times m$ nad $\mathbb{Z}_q$. Chceme najít $0 \neq t \in \mathbb{Z}^m$ $\|z\| \leq \beta, Az \equiv 0 \pmod q$

Poznámka 2.15. $L = \{n \in \mathbb{Z}^m : An \equiv 0 \pmod q\}$ je celočíselná mříž obsahující $q : \mathbb{Z}^m$ (q-ární mříž)

Příklad 2.16. $2^m > q^n (m > n \cdot \log(q))$. Vezmeme $f_A : \{0,1\}^m \to \mathbb{Z}_q^n$ $f_A(n) := An \mod q$
$\exists u_1 \neq u_2 \in \{0,1\}^m : f_A(u_1) = f_A(u_2)$
$z = u_1 - u_2 \in \{0,1\}^m, O < \|z\| \leq \sqrt{m}$, $Az \equiv 0 \pmod q$.
Potom z řeší $\text{SIS}_{n,q,\sqrt{m},n}$.

Věta 2.17 (M. Ajatai, 1996). *Nechť $m = \text{poly}(n), q \geq \beta\,\text{poly}(n)$. Pokud existuje algoritmus řešící $SIS_{n,q,\beta,n}$ s nezanedbatelnou pravděpodobností, pak existuje srovnatelně efektivní algoritmus, který řeší $SIVP_\gamma$ s nezanedbatelnou pravděpodobností pro všechny instance $n-$dimenzionálních mříží, kde $\gamma = \text{poly}(n) \cdot \beta$.*

Příklad 2.18. Nechť $2^m > q^n$, $\beta \geq \sqrt{m}$. Díváme se na $\{f_A : A \in M_{n,m}(t_q)\}$ jako na množinu hashovacích funkcí, která má q^n prvků. Hledáme v ní náhodnou kolizi (speciální případ $\text{SIS}_{n,q,\beta,m}$). Důkaz obtížnosti SIVP_γ pro odpovídající γ povede k důkazu obtížností problému hledání kolizí.

3 Lineární algebra nad $\mathbb{Z}$

Definice 3.1 (volná grupa). konečně generovaná komutativní grupa G je *volná*, pokud $\exists b_1, b_2, \ldots, b_d \in G$ takové, že $\forall g \in G$ $\exists! z_1, z_2, \ldots, z_d \in \mathbb{Z}$ tak, aby $g = z_1 b_1 + z_2 b_2 + \cdots + z_d b_d$. Množina $\{b_1, b_2, \ldots, b_d\}$ se nazývá *volná báze G*.

Poznámka 3.2. $G = O$ volná grupa s volnou bází $\emptyset$
$L \subseteq (\mathbb{R}^n, +)$ mříž. Potom báze mříže je volná báze grupy $(L, +)$
$(\mathbb{Z}^n, +)$ Potom volná báze např. $\{e_1, e_2, \ldots, e_n\}, e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

Tvrzení 3.3. *Konečně generovaná volná grupa je izomorfní $(\mathbb{Z}^n, +)$ pro nějaké $n \in \mathbb{N}$.*

Důkaz. G s volnou bází is $\{b_1,+\ldots,b_d\}$ $\varphi:\mathbb{Z}^d\to G$ $\begin{pmatrix}z_1\\ \vdots\\ z_d\end{pmatrix}\to\sum_{i=1}^d z_ib_i$ je izomorfizmus grup. □

Tvrzení 3.4. $(\mathbb{Z}^{d_1},+)\simeq(\mathbb{Z}^{d_2},+)\Rightarrow d_1=d_2$

Důkaz. $\varphi:\mathbb{Z}^{d_1}\to\mathbb{Z}^{d_2}$
$\varphi/2\mathbb{Z}^{d_i}:2\mathbb{Z}^{d_1}\to\mathbb{Z}^{d_2}$
tyto dvě věci implikují: $\mathbb{Z}^{d_1}/2\mathbb{Z}^{d_2}\simeq\mathbb{Z}^{d_2}/2\mathbb{Z}^{d_2}\implies 2^{d_1}=2^{d_2}\implies d_1=d_2$. □

Důsledek 3.5. *$\{b_1,\ldots,b_d\},\{b'_1,\ldots,b'_d\}$ volné báze komutativní volné grupy $G\Rightarrow d=d'$. ($G\simeq(\mathbb{Z}^d,+)\simeq(\mathbb{Z}^{d'},+)$)*

Definice 3.6 (rank grupy). Rankem volné komutativní grupy G rozumíme počet prvků nějaké její volné báze.

Tvrzení 3.7. *$\forall\varphi:(\mathbb{Z}^n,+)\to(\mathbb{Z}^m,+)$ hom. $\exists!A\in M_{m,n}(\mathbb{Z})$ tak, že $\varphi(u)=A\cdot u\forall u\in\mathbb{Z}^n$.*

Důkaz. Pro $i=1,\ldots,n$: $\varphi(e_i)=:a_i\in\mathbb{Z}^m$. Dále $A:=(a_1|a_2|\ldots|a_n)$. Potom $Au=A\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}=$

$\sum_{i=1}^n u_ia_i=\sum_{i=1}^n u_i\varphi(e_i)=\varphi(\sum_{i=1}^n u_ie_i)=\varphi(\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix})=\varphi(n)$.
Jednoznačnost: $\varphi(u)=A\cdot u\implies\varphi(e_i)=Ae_i\implies\varphi(e_i)$ musí být i-tý sloupec matice A. □

3.1 Souřadnice

G konečně generovaná volná komutativní grupa. $B=\{b_1,\ldots,b_d\}$ volná báze G.
Pro $g\in G$ je $[g]_B=\begin{pmatrix}z_1\\ \vdots\\ z_d\end{pmatrix}\in\mathbb{Z}^d$, kde $g=\sum_{i=1}^d z_ib_i$, souřadnice g vzhledem k bázi B.

Definice 3.8 (Matice homomorfismu). Nechť $0\neq G,H$ jsou konečně generované volné komutativní grupy, B_G volná báze G, B_H volná báze H.
$\varphi:G\to H$ homomorfismus $[\varphi]_{B_H}^{B_G}$ je matice $|B_H|\times|B_G|$ nad $\mathbb{Z}$ splňující $[\varphi]_{B_H}^{B_G}\cdot[g]_{B_G}=[\varphi(g)]_{B_H}$ pro každé $g\in G$

Sestrojí se tak, že $[\varphi]_{B_H}^{B_G}=([\varphi(b_1)]_{B_H}|[\varphi(b_2)]_{B_H}|\ldots|[\varphi(b_d)]_{B_H})$, $B_G=\{b_1,\ldots,b_d\}$

Tvrzení 3.9. *$\varphi:G\to H,\psi:H\to K$, G,H,K volné komutativní grupy,*
B_G,B_H,B_K jejich volné báze
$[\psi\circ\varphi]_{B_K}^{B_G}=[\psi]_{B_K}^{B_H}\cdot[\psi]_{B_H}^{B_G}$

Důkaz. Stejný důkaz jako v lineární algebře □