Algoritmy na mřížích

Pavel Příhoda

25. prosince 2021

Obsah

1 Úvod

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

Poznámka 1.2. Množina $\{b_1, b_2, \ldots, b_d\}$ se nazývá *báze* L. Není určená jednoznačně. $d := \dim < L >$ 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. $(L, +) \simeq (\mathbb{Z}^d, +)$ *pro* $d = \dim < L >$.

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 standardní 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

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

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

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

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

Důkaz. Položme $B_M := \{v \in \mathbb{R}^n \mid \|v\| < M\}$, $B_\varepsilon := \{v \in \mathbb{R}^n \mid \|v\| < \varepsilon\}$, kde $\varepsilon > 0$ splňuje $B_\varepsilon \cap G = \{0\}$. Položme dále $X := G \cap B_M$, $B_{\frac{\varepsilon}{2}} := \{v \in \mathbb{R}^n \mid \|v\| < \frac{\varepsilon}{2}\}$.
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 $\|g_1 - g_2\| \geq \varepsilon$. Odtud plyne

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

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

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

□

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.)
$\boxed{d=1}$ $\exists 0 \neq b_1 \in \mathbb{R}^n$: $L = \mathbb{Z}b_1$. Pak $0 \neq l \in L \iff l = zb_1,\ z \in \mathbb{Z}\setminus\{0\}$.
Pro normu l pak platí $\|l\| = |z| \cdot \|b_1\| \geq \|b_1\| \implies \varepsilon = \|b_1\|$ projde.
$\boxed{d>1}$ Nechť $\{b_1, \ldots, b_d\}$ je báze L. Definujme $L_0 := \mathbb{Z}b_1 + \mathbb{Z}b_2 + \cdots + \mathbb{Z}b_{d-1}$. Pak $\{b_1, \ldots, b_{d-1}\}$ je báze L_0 a z indukčního předpokladu $\exists \varepsilon_0 > 0$ takové, že $\forall l \in L_0 \setminus \{0\} :\ \|l\| \geq \varepsilon_0$. Platí, že $\mathbb{R}^n = \langle L_0 \rangle \oplus \langle L_0 \rangle^\perp$ a proto $\forall v \in \mathbb{R}^n\ \exists v_0, v^\perp \in \mathbb{R}^n$ splňující $v = v_0 + v^\perp,\ v_0 \in \langle L_0 \rangle,\ v^\perp \in \langle L_0 \rangle^\perp$.
Ať pro $l \in L$ platí

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

Pak buď

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. $z_d \neq 0$: pak $l = l_0 + l^\perp,\ l_0 \in L_0,\ l^\perp \in \langle L_0 \rangle^\perp \implies \|l\| = \|l_0 + l^\perp\| \geq \|l^\perp\| = \|z_d b_d^\perp\|$.
   $b_d \notin L_0$, neboť $b_1, \ldots, b_d$ jsou LN $\implies b_d = \underset{\in L_0}{b_{d_0}} + \underset{\neq 0}{b_d^\perp} \implies \|l\| \geq |z_d| \cdot \|b_d^\perp\| \geq \|b_d^\perp\| > 0$.

   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 $\forall 0 \neq l \in L$ je množina $\{v \in L \setminus \{0\} : \|v\| \leq \|l\|\}$ 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 $\forall 0 \neq u \in L : \gamma(n) \cdot \|u\| \geq \|v\|$.

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

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

je řešitelný v polynomiálním čase.

Definice 2.9 (Gap SVP$_\gamma$). (Rozhodovací verze SVP$_\gamma$)
Dána $L \subseteq (\mathbb{R}^n, +)$ 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$_\gamma$ (bounded distance decoding)

Definice 2.10 (BDD$_\gamma$ - bounded distance decoding).
Dány $L \subseteq (\mathbb{R}^n, +)$, $v \in \mathbb{R}^n$. 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. $\forall l_1, l_2 \in L$, $l_1 \neq l_2$ platí $\|l_1 - l_2\| \geq \lambda_1(L)$, neboť $l_1 - l_2 \in L$.
Proto $\forall v \in \mathbb{R}^n : \ |\{u \in \mathbb{R}^n : \|u - v\| < \frac{\lambda_1(L)}{2} \cap L\}| \leq 1$

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* $\lambda_i(L) := \min\{r \in \mathbb{R} : L$ obsahuje i LN vektorů normy $\leq r\}$

Definice 2.13 (SIVP$_\gamma$ - 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 (SIS$_{n,q,\beta,m}$ - short integer solution).
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 $0 \neq z \in \mathbb{Z}^m$ takové, aby $\|z\| \leq \beta$ a $Az \equiv 0 \pmod q$.

Poznámka 2.15. $L = \{u \in \mathbb{Z}^m : Au \equiv 0 \pmod q\}$ je celočíselná mříž obsahující
$q \cdot \mathbb{Z}^m = \{(qz_1 \ldots qz_m)^T | \ z_1, \ldots z_m \in \mathbb{Z}\}$ (q-ární mříž).

Příklad 2.16. Nechť $2^m > q^n$ (tzn. $m > n \log_2(q)$).
Vezmeme $f_A : \{0,1\}^m \to \mathbb{Z}_q^n$ definované předpisem $f_A(u) := Au \pmod q$.
Protože f_A není prosté, $\exists u_1, u_2 \in \{0,1\}^m, u_1 \neq u_2 : f_A(u_1) = f_A(u_2)$. Položme $z = u_1 - u_2$.
Pak $z \in \{-1, 0, 1\}^m$, $0 < \|z\| \leq \sqrt{m}$, $Az \equiv 0 \pmod q$.
Potom z řeší SIS$_{n,q,\sqrt{m},n}$.

Věta 2.17 (M. Ajatai, 1996). *Nechť $m = \text{poly}(n)$ (nějaký polynom v 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 $\{f_A : A \in M_{n,m}(\mathbb{Z}_q)\}$ jako na množinu hashovacích funkcí, která má q^n prvků. Hledáme v ní náhodnou kolizi (speciální případ SIS$_{n,q,\beta,m}$).
Důkaz obtížnosti SIVP$_\gamma$ 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 $\forall g \in G \quad \exists! z_1, z_2, \ldots, z_d \in \mathbb{Z}$ 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.

1. $G = \{0\}$ volná grupa s volnou bází $\emptyset$.
2. $L \subseteq (\mathbb{R}^n, +)$ mříž. Potom báze mříže je volná báze grupy $(L, +)$.

3. Volná báze grupy $(\mathbb{Z}^n,+)$ je 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. Nechť G je konečne generovaná volná grupa s volnou bází $\{b_1,\ldots,b_d\}$. Uvážíme zobrazení $\varphi:\mathbb{Z}^d\to G$ definované předpisem $\varphi(z)=\sum_{i=1}^d z_ib_i\ \forall z=\begin{pmatrix}z_1\\\vdots\\z_d\end{pmatrix}\in\mathbb{Z}^d$. Z linearity předpisu je φ homomorfismus, který je zřejmě navíc prostý. Z definice má každé $g\in G$ vzor $\implies\varphi$ je na $\implies\varphi$ je izomorfizmus grup. □

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

Důkaz. $\varphi:\mathbb{Z}^{d_1}\xrightarrow{\simeq}\mathbb{Z}^{d_2}$
$\varphi/2\mathbb{Z}^{d_1}:2\mathbb{Z}^{d_1}\xrightarrow{\simeq}2\mathbb{Z}^{d_2}$
Tyto dvě věci implikují (z 1. věty o isomorfisme): $\mathbb{Z}^{d_1}/2\mathbb{Z}^{d_1}\simeq\mathbb{Z}^{d_2}/2\mathbb{Z}^{d_2}$
$\implies 2^{d_1}=|\mathbb{Z}^{d_1}/2\mathbb{Z}^{d_1}|=|\mathbb{Z}^{d_2}/2\mathbb{Z}^{d_2}|=2^{d_2}\implies d_1=d_2.$ □

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

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

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

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 $Au=A\begin{pmatrix}u_1\\\vdots\\u_n\end{pmatrix}=$

$\sum_{i=1}^n a_iu_i=\sum_{i=1}^n\varphi(e_i)u_i=\varphi(\sum_{i=1}^n u_ie_i)=\varphi(\begin{pmatrix}u_1\\\vdots\\u_n\end{pmatrix})=\varphi(n).$

Jednoznačnost: $\varphi(u)=Au\ \forall u\in\mathbb{Z}^n\implies\varphi(e_i)=Ae_i\ \forall i\in\{1,\ldots,n\}\implies\varphi(e_i)$ musí být i-tý sloupec matice A. □

3.1 Souřadnice

Nechť $\{0\}\neq G$ je konečně generovaná volná komutativní grupa a $B=\{b_1,\ldots,b_d\}$ je 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 a $\varphi:G\to H$ 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 $g\in G$.

Konstrukce $[\varphi]_{B_H}^{B_G}$: Pro $B_G=\{b_1,\ldots,b_d\}$ je $[\varphi]_{B_H}^{B_G}=([\varphi(b_1)]_{B_H}|[\varphi(b_2)]_{B_H}|\ldots|[\varphi(b_d)]_{B_H})$.

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

Důkaz. Stejný důkaz jako v lineární algebře. □

Opakování

- Každá konečně generovaná volná komutativní grupa G je isomorfní $(\mathbb{Z}^n, +)$, kde $n \in \mathbb{N}_0$ je *rank grupy G*.
- Homomorfismus $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$ koresponduje s maticovým násobením: $\exists! A \in M_{m,n}(\mathbb{Z}) : \varphi(u) = Au \ \forall u \in \mathbb{Z}$. Potom tedy A je matice φ vzhledem ke kanonickým bazím.
- $M_n(\mathbb{Z})$ značí množinu všech čtvercových matic $n \times n$ nad $\mathbb{Z}$. E značí jednotkovou matici.
- adj(A) značí adjungovanou matici (`https://cs.wikipedia.org/wiki/Adjungovan%C3%A1_matice`)
- K značí kanonickou bázi.

3.2 Unimodulární matice

Definice 3.10. $A \in M_n(\mathbb{Z})$ je *unimodulární*, pokud $\det(A) = \pm 1$. $GL(n, \mathbb{Z})$ je *množina všech unimodulárních matic* řádu n.

Lemma 3.11. *$A \in M_n(\mathbb{Z})$ je unimodulární $\iff$ A je regulární a $A^{-1} \in M_n(\mathbb{Z})$.*

Důkaz.

$\Leftarrow$: Mějme regulární $A \in M_n(\mathbb{Z})$ takovou, že $A^{-1} \in M_n(\mathbb{Z})$. Potom $A \cdot A^{-1} = E \implies \det(A) \cdot \det(A^{-1}) = 1$. Ale jelikož $A, A^{-1} \in M_n(\mathbb{Z})$, tak $\det(A)$, $\det(A^{-1}) \in \mathbb{Z}$ a tedy $\det(A) = \pm 1 = \det(A^{-1})$.

$\Rightarrow$: Z definice unimodulární matice je $\det(A) = \pm 1$, což implikuje regularitu A a existenci A^{-1}. Pak platí $A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A)$. Navíc adj$(A) \in M_n(\mathbb{Z})$, protože všechny subdeterminanty A jsou celočíselné, a proto $A^{-1} \in M_n(\mathbb{Z})$.

□

Tvrzení 3.12. *Homomorfismus $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$ je isomorfismus $\iff$ $A = [\varphi]_K^K$ je unimodulární.*

Důkaz.

$\Rightarrow$: Mějme $\psi = \varphi^{-1}$. Označme $B = [\psi]_K^K$. Potom $AB = [\varphi]_K^K [\psi]_K^K = [\varphi \circ \psi]_K^K = [id]_K^K = E \implies B = A^{-1}$, tedy A je regulární. Dále $B = [\psi]_K^K = (\psi(e_1)|\psi(e_2)|\dots|\psi(e_n)) \in M_n(\mathbb{Z})$, protože $\psi : \mathbb{Z}^n \to \mathbb{Z}^n$.

$\Leftarrow$: Nechť $A = [\varphi]_K^K$ je unimodulární. Pak z Lemmatu 3.11 je A regulární a $B := A^{-1} \in M_n(\mathbb{Z})$. Mějme zobrazení $\psi : \mathbb{Z}^n \to \mathbb{Z}^n$ definované vztahem $\psi(u) = Bu$ pro $u \in \mathbb{Z}^n$. Potom

$$\varphi \circ \psi(u) = ABu = AA^{-1}u = u = BAu = \psi \circ \varphi(u),$$

tedy $\psi = \varphi^{-1}$.

□

Poznámka 3.13. Vezmeme mříž s hezkou bází a tu potom schováme → dostaneme kryptosystém.

3.3 Hermitův tvar regulární celočíselné matice

Definice 3.14. $A \in M_n(\mathbb{Z})$ regulární je v *Hermitově normálním tvaru (HNF)*, pokud:

- A je horní trojúhelníková
- na diagonále A jsou kladná čísla
- $\forall i \in \{1,\dots,n\}\ \forall j \in \{i+1,\dots,n\}:\ a_{i,j} \in \{0,\dots,a_{i,i}-1\}$

Poznámka 3.15. Tedy matice A je v HNF, pokud je horní trojúhelníková, má na diagonále kladná čísla a všechny prvky vpravo od diagonály jsou menší než prvek na diagonále na stejném řádku.

Věta 3.16. $\forall A \in M_n(\mathbb{Z})$ *regulární* $\exists! B,U \in M_n(\mathbb{Z}) : B$ *je v HNF,* $U \in GL(n,\mathbb{Z}),\ B = AU$.

Důkaz.

existence: Algoritmem - na sloupce A opakovaně aplikujeme úpravy, které nemění absolutní hodnotu determinantu:

- permutace sloupců
- přenásobení sloupce -1
- přičtení celočíselné lineární kombinace ostatních sloupců k jinému sloupci

Potom tedy $AU_1U_2\cdots U_t = B$ je HNF a $U = U_1U_2\cdots U_t \in GL(n,\mathbb{Z})$.

Algoritmus:

1. $B := A$
2. $i := n$ *//*i *=index upravovaného řádku; na rozdíl od Gaussovy eliminace postupujeme od pravého dolního rohu doleva nahoru*
3. dokud $b_{i,1}, b_{i,2}, \dots, b_{i,i-1}$ nejsou všechny rovny 0:
   i. permutujeme prvních i sloupců B tak, aby po spermutování platilo: $\|b_{i,i}\| = \min\{\|b_{i,j}\| : 1 \le j \le i, b_{i,j} \neq 0\}$
   ii. pokud $b_{i,i} < 0$, tak vynásobíme $i-$tý sloupec -1
   iii. pro $j \in \{1,\dots,i-1\}$ označíme $q = \lfloor \frac{b_{i,j}}{b_{i,i}} \rfloor$ a od $j-$tého sloupce odečteme $q-$násobek $i-$tého sloupce. *//dělení se zbytkem:* $b_{i,j} \to b_{i,j} \mod b_{i,i}$
4. pokud $b_{i,i} < 0$, tak vynásobíme $i-$tý sloupec -1
5. *//čísla vpravo od* $b_{i,i}$ *taky vydělíme se zbytkem*
   pro $j \in \{i+1,\dots,n\}$
   i. $q := \lfloor \frac{b_{i,j}}{b_{i,i}} \rfloor$
   ii. od $j-$tého sloupce odečteme $q-$násobek $i-$tého sloupce
6. pokud $i > 1$, tak od i odečteme 1 a pokračujeme znovu od kroku 2.
7. **return** B

Poznámka 3.17. Při výpočtu B může dojít k velké expanzi koeficientů matice.

($n = 20$, matice s koeficienty $0,\dots 10 \to$ koeficienty B mohou být velikosti 10^{1500})

Algoritmus se v praxi nevyužívá.

jednoznačnost: Mějme $B = AU$ a $C = AV$ takové, že $B,C,U,V \in M_n(\mathbb{Z})$, B,C jsou v HNF a $U,V \in GL(n,\mathbb{Z})$.

Spojením definic matic B a C dostaneme $C = BU^{-1}V$. Označme $W = U^{-1}V \in GL(n,\mathbb{Z})$. Víme, že $W = B^{-1}C$ a tedy je W horní trojúhelníková (protože B,C jsou horní trojuhelníkové) a na diagonále má $\frac{c_{i,i}}{b_{i,i}} \in \mathbb{Z}$ a protože C je v HNF, máme $c_{i,i} > 0$, a tedy i $w_{i,i} > 0$. Jelikož $W = U^{-1}V$, tak $\det(W) = 1$ a tedy $w_{1,1} = w_{2,2} = \cdots = w_{n,n} = 1$. Tedy $b_{i,i} = c_{i,i}\ \forall i$.

Dále $C = BW$. Chceme dokázat $W = E$. Sporem: nechť v $i-$tém sloupci nad diagonálou existuje nenulový prvek (označme ho z). Označme j index řádku, ve kterém leží z. Dále označme $C = (c_1|c_2|\ldots|c_n) = (b_1|b_2|\ldots|b_n)W = BW$. Potom $c_i = b_i + zb_j +$nějaká celočíselná LK $b_1,\ldots,b_{j-1}$. Tedy $c_{j,i} = b_{j,i} + zb_{j,j}$. Ale $c_{j,i} \in \{0,\ldots,c_{j,j}-1\}$ a $b_{j,i} \in \{0,\ldots,b_{j,j}-1\} \implies$ spor, protože $c_{j,i}$ je moc velké. Tedy všechny prvky nad diagonálou matice W jsou nulové.

□

3.4 HNF obecné matice

Definice 3.18. $A \in M_n(\mathbb{Z})$ je v *HNF*, pokud $\exists r \in \{0,\ldots,n\}$ a $f : \{r+1,\ldots,n\} \to \{1,\ldots,m\}$ ostře rostoucí takové, že:

- prvních r sloupců A je nulových
- $\forall j \in \{r+1,\ldots,n\}:\ a_{f(j),j} \geq 1$ *//"pivot"*
- $\forall j \in \{r+1,\ldots,n\}\ \forall f(j) < i \leq m:\ a_{i,j} = 0$ *//pod pivotem jsou nuly*
- $\forall k < j \in \{r+1,\ldots,n\}:\ 0 \leq a_{f(k),j} < a_{f(k),k}$

Věta 3.19. *$\forall A \in M_{m,n}(\mathbb{Z})\ \exists B \in M_{m,n}(\mathbb{Z})\ \exists U \in GL(n,\mathbb{Z})$, kde B je HNF a $B = AU$. Navíc matice B je určená jednoznačně.*

Důkaz. Vynecháme. □

Tvrzení 3.20. *Nechť $A,B \in M_{m,n}(\mathbb{Z})$. Nechť $\exists U \in GL(n,\mathbb{Z}) : A = BU$. Pak sloupce matice A generují v $\mathbb{Z}^n$ stejnou podgrupu jako sloupce matice B.*

Důkaz. Máme $A = (a_1|a_2|\ldots|a_n) = (b_1|b_2|\ldots|b_n)U$. Každé a_i je tedy celočíselná LK $b_1,\ldots,b_n$. Tedy $\langle a_1,a_2,\ldots,a_n\rangle_{\mathbb{Z}^n} \subseteq \langle b_1,b_2,\ldots,b_n\rangle_{\mathbb{Z}^n}$. Jelikož ale také $B = AU^{-1}$, tak i $\langle b_1,b_2,\ldots,b_n\rangle_{\mathbb{Z}^n} \subseteq \langle a_1,a_2,\ldots,a_n\rangle_{\mathbb{Z}^n}$. □

Důsledek 3.21. *Každá konečně generovaná podgrupa $(\mathbb{Z}^n,+)$ je volná komutativní grupa.*

Důkaz. Mějme $G = \langle g_1,g_2,\ldots,g_n\rangle \subseteq (\mathbb{Z}^n,+)$. Položme $A := (g_1|g_2|\ldots|g_n) \in M_{m,n}(\mathbb{Z})$. Dle Věty 3.19 $\exists B \in M_{m,n}(\mathbb{Z})$ v HNF $\exists U \in GL(n,\mathbb{Z}):\ B = AU$. Nenulové sloupce B generují G a jsou lineárně nezávislé $\Rightarrow$ tvoří volnou bázi G.
//a taky jsme tím dokázali, že je to mříž □

Opakování

Minule: $A,B \in M_{m,n}(\mathbb{Z})$, $B = AU$, $U \in GL(n,\mathbb{Z}) \implies$ sloupce matic A,B generují stejnou podgrupu $(\mathbb{Z}^m,+)$

Poznámka 3.22. Každá podgrupa konečně generované komutativní grupy je konečně generovaná.

Příklad 3.23. $A = \begin{pmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 1 & 1 \end{pmatrix}$. Určete volnou bázi grupy $G = \{u \in \mathbb{Z}^4 \mid Au \equiv 0 \pmod 5\}$.

Řešení: Vyřeším soustavu $Au = 0$ nad $\mathbb{Z}_5$:

$\begin{pmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 3 \\ 0 & 1 & -1 & -2 \end{pmatrix}$. Vektory $u_1 = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}$, $u_2 = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \end{pmatrix}$ tvoří bázi řešení soustavy,

tudíž $\forall u \in G:\ u \bmod 5 \in \mathbb{Z}u_1 + \mathbb{Z}u_2$, a tedy $\begin{pmatrix} 5 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 5 \end{pmatrix}$, u_1, u_2 generují G.

(Detailněji: $\exists z_1, z_2:\ z_1u_1 + z_2u_2 \equiv u \pmod 5$, ekvivalentně $z_1u_1 + z_2u_2 - u = \begin{pmatrix} 5a_1 \\ 5a_2 \\ 5a_3 \\ 5a_4 \end{pmatrix}$

$\implies u = z_1u_1 + z_2u_2 + a_1 \begin{pmatrix} 5 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 5 \\ 0 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 0 \\ 5 \\ 0 \end{pmatrix} + a_4 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 5 \end{pmatrix}$)

Označíme B matici tvořenou nalezenými generujícími vektory volné grupy G, a ekvivalentními úpravami ji převedeme do HNF: $B = \begin{pmatrix} 5 & 0 & 0 & 0 & 2 & 0 \\ 0 & 5 & 0 & 0 & 1 & 2 \\ 0 & 0 & 5 & 0 & 1 & 0 \\ 0 & 0 & 0 & 5 & 0 & 1 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 0 & 0 & 5 & 0 & 2 & 0 \\ 0 & 0 & 0 & 5 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

Nenulové sloupcové vektory $z_1 = \begin{pmatrix} 5 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $z_2 = \begin{pmatrix} 0 \\ 5 \\ 0 \\ 0 \end{pmatrix}$, $z_3 = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \end{pmatrix}$, $z_4 = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}$ normalizované matice pak tvoří volnou bázi G.

3.5 Soustavy lineárních diofantických rovnic

Dána $A \in M_{m,n}(\mathbb{Z})$ určující $R = \{u \in \mathbb{Z} \mid Au = 0\}$ podgrupu $\mathbb{Z}^n$. Hledáme volnou bázi R.
Víme, že $\exists U \in GL(n, \mathbb{Z})$, AU je v HNF, přičemž $A(u_1|u_2|\ldots|u_n)$ má prvních r sloupců nulových, tedy $u_1, u_2, \ldots, u_r \in R$.
Protože U je regulární, $u_1, u_2, \ldots, u_r$ jsou LN (nad $\mathbb{Q}$), a pro $u \in R$ platí

$Au = 0 \implies (AU)(U^{-1}u) = 0 \implies U^{-1}u \in \begin{pmatrix} * \\ \vdots \\ * \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ (r nenulových prvků, pak nuly)

$\implies \exists \begin{pmatrix} z_1 \\ \vdots \\ z_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}^n,\ u = U \begin{pmatrix} z_1 \\ \vdots \\ z_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} = z_1u_1 + z_2u_2 + \cdots + z_ru_r$, tedy $\{u_1, \ldots u_r\}$ generují R.

Příklad 3.24. Určete celočíselné řešení rovnice $2x+3y+5z=0$.
Řešení: AU je v HNF, $EU=U$. Eliminujeme:

$$\left(\begin{array}{ccc|ccc}2&3&5&1&0&0\\1&0&0&0&1&0\\0&1&0&0&0&1\end{array}\right)\sim\left(\begin{array}{ccc|ccc}2&3&5&1&0&0\\1&0&0&0&1&0\\0&1&0&0&0&1\end{array}\right)\sim\left(\begin{array}{ccc|ccc}5&3&2&0&0&1\\0&0&1&0&1&0\\1&0&0&1&0&0\end{array}\right)\sim\left(\begin{array}{ccc|ccc}1&1&2&-2&-1&1\\-2&-1&1&0&1&0\\0&1&0&1&0&0\end{array}\right)\sim\left(\begin{array}{ccc|ccc}1&2&1&-2&1&-1\\0&0&1&0&0&1\\1&0&0&1&0&0\end{array}\right)\sim\left(\begin{array}{ccc|ccc}0&0&1&-1&3&-1\\-1&-2&1&-1&-2&1\\1&0&0&1&0&0\end{array}\right),$$

tudíž $U:=\begin{pmatrix}-1&3&-1\\-1&-2&1\\1&0&0\end{pmatrix}$ a $R=\{\begin{pmatrix}-z_1+3z_2\\-z_1-2z_2\\z_1\end{pmatrix}\mid z_1,z_2\in\mathbb{Z}\}$.

3.6 Jednoznačnost HNF

Tvrzení 3.25. *Nechť $A\in M_{m,n}(\mathbb{Z})$, $U,U'\in\mathrm{GL}(n,\mathbb{Z})$. Nechť matice $AU=B$, $AU'=B'$ jsou obě v HNF. Pak $B=B'$.*

Důkaz. Nechť G je podgrupa $\mathbb{Z}^m$ generovaná sloupci A. Sloupce B, sloupce B' rovněž generují G, protože $U,U'\in\mathrm{GL}(n,\mathbb{Z})$.
Protože B,B' jsou obě v HNF, existují $r,r'\in\mathbb{N}$ taková, že matice B má prvních r sloupců nulových a matice B' má prvních r' sloupců nulových. Protože $r=n-\mathrm{rank}\ G$, $r'=n-\mathrm{rank}\ G$, máme $r=r'$.
Dále položme $L_1:=\left\{\begin{pmatrix}z_1\\0\\\vdots\\0\end{pmatrix}\middle|z_1\in\mathbb{Z}\right\}$, $L_2:=\left\{\begin{pmatrix}z_1\\z_2\\0\\\vdots\\0\end{pmatrix}\middle|z_1,z_2\in\mathbb{Z}\right\}$ atd., t.j. L_i obsahuje všechny vektory, které mají na prvních i souřadnicích celé čísla z_1 až z_i a na zvyšných souřadnicích samé nuly, a dále označme $G_i:=G\cap L_i\ \forall i\in\{1,\dots m\}$. Nechť $f(r+i)$ je index posledního nenulového prvku v $(r+i)$-tém sloupci matice B (tedy $b_{w,r+i}=0\ \forall w\in\{f(r+i)+1,m\}$), a analogicky zadefinujeme $f'(r'+i)$ pro matici B'. Pak tedy platí
$f(r+i)=\min\{j\in\{1,\dots,m\}\mid\mathrm{rank}\ G_j=i\}=f'(r+i)\ \forall i\in\{1,\dots\mathrm{rank}\ G\}$, odkud plyne
$b_{f(r+i),r+i}=b'_{f(r+i),r+i}$, protože z definice jsou oba kladné.
Podívám se na poslední nenulový řádek matice A a vidíme, že $b_{f(n),n}$ je NSD prvků v posledním nenulovém řádku A. Zároveň vidíme, že $b_{f(n),n}|b'_{f(n),n}$ a zároveň $b'_{f(n),n}|b_{f(n),n}$.
Položme $W:=U^{-1}U$, pak platí $B=B'W$, z čeho např. vidíme, že b'_i ($(r+i)$-tý sloupec B') je prvkem G a b'_i je celočíselná lineární kombinace sloupců B. Ale kterých?
$b'_i=b_i+$ LK sloupců vlevo od b_i
$\vdots$
$b_{f(r+i),r+i}=b'_{f(r+i),r+i}$ (na pivotech jsou stejné prvky)
Pro $r<j<k\le n$ je $b_{f(j),k}\in\{0,\dots,b_{f(j),j}-1\}$. To vynutí, že LK sloupců vlevo od b_i je triviální. □

3.7 Smithova normální forma

Definice 3.26 (Smithův normální tvar). $A\in M_n(\mathbb{Z})$ je ve *Smithově normálním tvaru* (SNF), pokud je diagonální $A=\mathrm{diag}(a_1,a_2,\dots,a_n)$, $a_1,\dots,a_n\in\mathbb{N}_0$ a $\forall i\in\{1,\dots,n-1\}:\ a_{i+1}|a_i$.

Věta 3.27. $\forall A\in M_n(\mathbb{Z})\ \exists U,V\in\mathrm{GL}(n,\mathbb{Z})$ *takové, že UAV je ve Smithově normálním tvaru.*

Definice 3.28. Součin UAV je určený jednoznačně a nazývá se Smithova normální forma A.

K důkazu existence: Na řádky/sloupce aplikujeme tyto úpravy

- permutace řádků, permutace sloupců
- řádek/sloupec přenásobíme (-1)
- k sloupci přičíst celočíselnou LK ostatních sloupců
- k řádku přičíst celočíselnou LK ostatních řádků

...snažíme se A převést do SNF

Věta 3.29. *Nechť G je konečně generovaná volná komutativní grupa, H podgrupa G. Nechť $\{b_1,\dots,b_d\}$ je volná báze G. Pak $\exists z_1,z_2,\dots,z_d\in\mathbb{Z}$ tak, že $\{z_1b_1,z_2b_2,\dots,z_db_d\}\setminus\{0\}$ je volná báze H.*

Důkaz. Víme, že $G\simeq(\mathbb{Z}^d,+)$, BÚNO $G=\mathbb{Z}^d$ a H je konečně generovaná volná komutativní grupa ranku $l\le d$. Nechť $\{h_1,h_2,\dots,h_l\}$ je volná báze H. Položme $A:=(h_1|h_2|\dots|h_l|0|\dots|0)$, pak dle Věty 3.27 $\exists U,V\in\mathrm{GL}(d,\mathbb{Z}):\ UAV=\mathrm{diag}(z_1,\dots,z_d)$.
Pozorování: H je podgrupa $\mathbb{Z}^d$ generovaná sloupci A, a taky je generovaná sloupci AV (protože $U\in\mathrm{GL}(n,\mathbb{Z})$).
Definujme zobrazení $\phi_U:\mathbb{Z}^d\to\mathbb{Z}^d$ předpisem $\phi_U(v):=Uv$. Toto zobrazení je automorfismus (neboť $U\in\mathrm{GL}(n,\mathbb{Z})$) a $\phi_U(H)$ je volná komutativní grupa s volnou bází $\{z_1e_1,z_2e_2,\dots,z_de_d\}\setminus\{0\}$, kde e_i je i-tý vektor kanonické báze. Označme $b_i:=\phi_U^{-1}(e_i)=U^{-1}e_i$, pak $\{b_1,\dots,b_d\}$ je volná báze $(\mathbb{Z}^d,+)$, a $\{z_1b_1,\dots,z_db_d\}\setminus\{0\}$ je volná báze $\varphi_U^{-1}(\varphi_U(H))=H$. □

3.8 Determinant mříže

Značení: $\{b_1,\dots b_m\}\in\mathbb{R}^n$ báze mříže $L=\mathbb{Z}b_1+\dots+\mathbb{Z}b_m$.
n … *dimenze* mříže L
m … *hodnost* mříže L
$m\le n$
úplná mříž … $m=n$
celočíselná mříž … $L\subseteq\mathbb{Z}^n$

Tvrzení 3.30. *Nechť $B=\{b_1,b_2,\dots b_m\}$, $B'=\{b'_1,b'_2,\dots b'_m\}$ jsou LN množiny v $\mathbb{R}^n$. Pak B a B' jsou báze stejné mříže $\iff$ $\exists U\in\mathrm{GL}(n,\mathbb{Z}):\ (b_1|\ \dots|b_m)=(b'_1|\dots|b'_m)U$.*

Důkaz.

$\Rightarrow$: Nechť $L=\mathbb{Z}b_1+\dots+\mathbb{Z}b_m=\mathbb{Z}b'_1+\dots+\mathbb{Z}b'_m$. Pro každé i vyjádříme $b_i=\sum_{j=1}^m u_{j,i}b'_j$, kde $u_{j,i}\in\mathbb{Z}$. Položme $U:=(u_{i,j})_{i,j}$. Pak platí $(b_1|\ \dots|b_m)=(b'_1|\dots|b'_m)U$.

Analogicky vyjádříme $b'_i=\sum_{j=1}^m v_{j,i}b_j$, kde $v_{j,i}\in\mathbb{Z}$. Položíme $V:=(v_{i,j})_{i,j}$,
pak $(b'_1|\ \dots|b'_m)=(b_1|\dots|b_m)V$.

Nyní $(b_1|\dots|b_m)=(b'_1|\ \dots|b'_m)U=(b_1|\dots|b_m)VU\implies(b_1|\dots|b_m)(VU-E)=0$, a protože $b_1,\dots b_m$ jsou LN a $VU-E$ je čtvercová řádu m, platí $VU=E$, neboli $V=U^{-1}$, a protože $V\in M_n(\mathbb{Z})$, máme $U\in\mathrm{GL}(n,\mathbb{Z})$.

$\Leftarrow$: Máme $(b_1|\ \dots|b_m)=(b'_1|\dots|b'_m)U$. Protože $U\in M_n(\mathbb{Z})$, je každé b_i celočíselnou LK vektorů $b'_1,\dots,b'_m\implies\mathbb{Z}b_1+\dots+\mathbb{Z}b_m\subseteq\mathbb{Z}b'_1+\dots+\mathbb{Z}b'_m$.

Naopak, protože $U\in\mathrm{GL}(n,\mathbb{Z})\implies V=U^{-1}\in M_n(\mathbb{Z})$, máme $(b'_1|\ \dots|b'_m)=(b_1|\dots|b_m)V$ a tedy $\mathbb{Z}b'_1+\dots+\mathbb{Z}b'_m\subseteq\mathbb{Z}b_1+\dots+\mathbb{Z}b_m$.

□

Definice 3.31. Pro úplnou mříž $L \subseteq \mathbb{R}^n$ s bází $B = \{b_1, \dots b_n\}$ definujeme *determinant mříže* L jako $d(L) := |\det(b_1|\dots|b_n)|$.

Poznámka 3.32. Nechť $B = \{b_1, \dots b_n\}$, $B' = \{b'_1, \dots b'_n\}$ jsou dvě báze mříže $L \subseteq \mathbb{R}^n$. Dle tvrzení $\exists U \in \mathrm{GL}(n\mathbb{Z}) : \ (b_1| \ \dots|b_n) = (b'_1|\dots|b'_n)U$, tedy $|\det(b_1|\dots|b_n)| = |\det(b'_1|\dots|b'_n)|$
$\implies d(L)$ nezávisí na volbě báze.

Definice 3.33. Pro obecnou mříž $L \subseteq \mathbb{R}^n$ s bází $\{b_1, \dots b_m\}$ položíme $M = (b_1|\dots|b_m)$. Pak definujeme $d(L) := \sqrt{\det(M^T M)}$.

3.9 Fundamentální rovnoběžnostěn

Definice 3.34. Pro $B = \{b_1, \dots b_m\} \in \mathbb{R}^n$ LN definujeme *fundamentální rovnoběžnostěn B* jako $\mathcal{F}(B) := \{\sum_{i=1}^m r_i b_i | \ r_1, \dots, r_m \in [0,1)\}$.

Lemma 3.35. *Nechť $B = \{b_1, \dots b_m\} \in \mathbb{R}^n$ je LN, $L = \mathbb{Z}b_1 + \dots + \mathbb{Z}b_m$. Pak*

$$< B >_{\mathbb{R}} = \dot{\bigcup_{l \in L}} l + \mathcal{F}(B), \ \textit{kde } l + \mathcal{F}(B) = \{l + v | \ v \in \mathcal{F}(B)\}.$$

Speciálně, je-li L úplná, pak

$$\mathbb{R}^n = \dot{\bigcup_{l \in L}} l + \mathcal{F}(B).$$

Důkaz. Nechť $v \in < B >_{\mathbb{R}}$, tedy $v = r_1 b_1 + \dots + r_m b_m$, $r_i \in \mathbb{R}$. Položme $z_i := \lfloor r_i \rfloor \in \mathbb{Z}$
a $l' := z_1 b_1 + \dots + z_m b_m \in L$. Pak $v = l' + v - l' = l' + \sum_{i=1}^m (r_i - z_i) b_i \in l' + \mathcal{F}(B)$, protože
$r_i - z_i \in [0,1)$, a tedy

$$< B >_{\mathbb{R}} = \bigcup_{l \in L} l + \mathcal{F}(B).$$

Dále ať $l_1, l_2 \in L$, $l_1 \neq l_2$. Chceme ukázat, že platí $(l_1 + \mathcal{F}(B)) \cap (l_2 + \mathcal{F}(B)) = \emptyset$. Sporem:
Ať $f_1, f_2 \in \mathcal{F}(B)$ splňují $l_1 + f_1 = l_2 + f_2$. Pak $l_1 - l_2 = f_2 - f_1$. Všimneme si, že $l_1 - l_2$ je celočíselná LK vektorů $b_1, \dots, b_m$, a $f_2 - f_1 = \sum_{i=1}^m (r_i - s_i) b_i$ pro $r_i, s_i \in [0,1)$, tedy $r_i - s_i \in (-1,1)$, a z lineární nezávislosti vektorů $b_1, \dots, b_m$ pak plyne $r_i - s_i = 0 \ \forall i \implies l_1 = l_2$, spor. □

Poznámka 3.36. Je-li $L \in \mathbb{R}^n$ úplná, pak $d(L) = \mathrm{vol}(\mathcal{F}(B))$, kde B je nějaká báze L.

Tvrzení 3.37. *Nechť $L \in \mathbb{R}^n$ je mříž s hodností m, $B = \{b_1, \dots b_m\} \subseteq L$ je LN.*
Pak B je báze $L \iff \mathcal{F}(B) \cap L = \{0\}$.

Důkaz.

$\Rightarrow$: Protože je B bází L, je dle Lemmatu 3.35 $< B >_{\mathbb{R}} = \dot{\bigcup}_{l \in L} l + \mathcal{F}(B)$, a proto je 0 jediný prvek v $0 + \mathcal{F}(B) = \mathcal{F}(B)$.

$\Leftarrow$: Pro $l \in L \ \exists r_1, \dots r_m \in \mathbb{R}$, $l = \sum_{i=1}^m r_i b_i$. Položme pro všechna $i \in \{1, \dots m\}$ $z_i := \lfloor r_i \rfloor \in \mathbb{Z}$ a $l' := \sum_{i=1}^m z_i b_i \in L$. Potom

$$L \ni l - l' = \sum_{i=1}^m (r_i - z_i) b_i \in \mathcal{F}(B), \text{ protože } r_i - z_i \in [0,1),$$

a jelikož $L \cap \mathcal{F}(B) = \{0\}$, tak $l = l' \in \mathbb{Z}b_1 + \dots + \mathbb{Z}b_m$.

□

3.10 Minkowského odhad

Připomenutí: Pro $L \subseteq \mathbb{R}^n$ definujeme *první postupné minimum* $\lambda_1(L) := \min\{\|v\| \mid 0 \neq v \in L\}$.

Věta 3.38 (Minkowski). *Nechť $L \subseteq \mathbb{R}^n$ je úplná mříž. Pak $\lambda_1(L) \leq \sqrt{n}\,\sqrt[n]{d(L)}$.*

Budeme k tomu směřovat.

Definice 3.39.

1. *Objem* v $\mathbb{R}^n$: Pro $S = [a_1, b_1] \times \cdots \times [a_n, b_n]$ definujeme $\mathrm{vol}(S) := (b_1 - a_1) \cdot \ldots \cdot (b_n - a_n)$.
   Pro obecnou $S \subseteq \mathbb{R}^n$ definujeme $\lambda^*(S) = \inf\{\sum_{i=1}^{\infty} \mathrm{vol}(X_i) \mid X_i \text{ jsou kvádry, } S \subseteq \bigcup_{i=1}^{\infty} X_i\}$.
2. Nechť $A \subseteq \mathbb{R}^n$. Pokud $\forall S \subseteq \mathbb{R}^n : \ \lambda^*(S) = \lambda^*(A \cap S) + \lambda^*(A \setminus S)$, pak A je *měřitelná* a definujeme $\mathrm{vol}(A) := \lambda^*(A)$.

Věta 3.40 (Blichfeldt). *Nechť $L \in \mathbb{R}^n$ je úplná mříž, $S \subseteq \mathbb{R}^n$ je měřitelná,* $\mathrm{vol}(S) > d(L)$. *Pak $\exists s_1, s_2 \in S, s_1 \neq s_2 : \ s_1 - s_2 \in L$.*

Důkaz. Zvolme B bázi L. Protože je L úplná, je dle Lemmatu 3.35 $\mathbb{R}^n = \dot{\bigcup}_{l \in L}\, l + \mathcal{F}(B)$. Pak můžeme psát $S = \dot{\bigcup}_{l \in L}\, ((l + \mathcal{F}(B)) \cap S)$.
Pro $l \in L$ je množina $l + \mathcal{F}(B)$ je měřitelná, a proto je měřitelná taky $(l + \mathcal{F}(B)) \cap S$, protože průnik měřitelných množin je měritelný. Jest $\mathrm{vol}(l + \mathcal{F}(B)) = \mathrm{vol}(\mathcal{F}(B)) = d(L)\ \forall l \in L$, a jelikož je disjunktné spočetné sjednocení měřitelných množin měřitelné a jeho objem je součet objemů jeho částí, platí $\mathrm{vol}(S) = \sum_{l \in L} \mathrm{vol}((l + \mathcal{F}(B)) \cap S)$.
Dále $\forall l \in L$ položme

$$X_l := ((l + \mathcal{F}(B)) \cap S) - l = \{x - l \mid x \in (l + \mathcal{F}(B)) \cap S\} \subseteq \mathcal{F}(B).$$

Pak X_l jsou měřitelné a $\mathrm{vol}(X_l) = \mathrm{vol}((l + \mathcal{F}(B)) \cap S)$.
Dále pokračujeme sporem: pokud platí, že $\{X_l \mid l \in L\}$ je systém po dvou disjunktních množin, pak

$$\dot{\bigcup_{l \in L}} X_l \subseteq \mathcal{F}(B),\ \mathrm{vol}(\dot{\bigcup_{l \in L}} X_l) = \sum_{l \in L} \mathrm{vol}(X_l) = \sum_{l \in L} \mathrm{vol}((l + \mathcal{F}(B)) \cap S) = \mathrm{vol}(S).$$

Z předpokladu ovšem $\mathrm{vol}(S) > d(L)$, a tedy

$$\mathrm{vol}(\dot{\bigcup_{l \in L}} X_l) = \mathrm{vol}(S) > d(L) = \mathrm{vol}(\mathcal{F}(B)),$$

spor. Tudíž $\exists l_1, l_2 \in L,\ l_1 \neq l_2 : \ X_{l_1} \cap X_{l_2} \neq \emptyset$. Zvolme $z \in X_{l_1} \cap X_{l_2}$ a položme $s_1 := l_1 + z$, $s_2 := l_2 + z$. Pak $s_1, s_2 \in S$, dále $l_1 \neq l_2 \implies s_1 \neq s_2$ a platí $s_1 - s_2 = l_1 + z - l_2 - z = l_1 - l_2 \in L$. □

Opakování

Nechť $L \subseteq \mathbb{R}^n$ je úplná mříž, $S \subseteq \mathbb{R}^n$ je měřitelná, $\mathrm{vol}(S) > d(L)$.
Pak $\exists s_1, s_2 \in S, s_1 \neq s_2 : \ s_1 - s_2 \in L$.

Věta 3.41 (Minkowského věta o mřížovém bodě). *Nechť $L \subseteq \mathbb{R}^n$ je úplná mříž. Nechť $S \in \mathbb{R}^n$ je*

- *měřitelná a* $\mathrm{vol}(S) > 2^n d(L)$,
- *středově souměrná (t.j.* $\forall S \in S: \ -s \in S$*),*
- *konvexní (t.j.* $\forall s_1, s_2 \in S \ \forall \lambda \in [0,1]: \ \lambda s_1 + (1-\lambda)s_2 \in S$*).*

Pak S obsahuje nenulový prvek L.

Důkaz. Položme $\tilde{S} := \{\frac{1}{2}s \mid s \in S\}$. Pak $\tilde{S}$ je měřitelná a $\mathrm{vol}(\tilde{S}) = \frac{1}{2^n}\mathrm{vol}(S) > d(L)$. Z Blichfeldtovy věty 3.40 pak plyne, že $\exists \tilde{s_1}, \tilde{s_2} \in \tilde{S}, \ \tilde{s_1} \neq \tilde{s_2}: \ \tilde{s_1} - \tilde{s_2} \in L$. Označme $s_1 := 2\tilde{s_1}, \ s_2 := 2\tilde{s_2}$, pak $s_1, s_2 \in S$ a platí

$$L \ni \tilde{s_1} - \tilde{s_2} = \frac{1}{2}s_1 + \frac{1}{2}(-s_2) \in S,$$

neboť dle předpokladu je S konvexní, a tudíž je $\tilde{s_1} - \tilde{s_2}$ hledaným nenulovým prvkem L. □

Věta 3.42 (Minkowski). *Nechť $L \subseteq \mathbb{R}^n$ je úplná mříž. Pak $\lambda_1(L) \leq \sqrt{n}\sqrt[n]{d(L)}$.*

Důkaz. Aplikujeme větu o mřížovém bodě 3.41 na $S = \{v \in \mathbb{R}^n \mid \|v\| \leq \sqrt{n}\sqrt[n]{d(L)}\}$. Ověříme předpoklady věty:

- S je uzavřená $\implies$ měřitelná,
- S je středově souměrná a konvexní, protože je to koule.

Položme $K := \{(x_1 \ \dots \ x_n)^T \mid |x_i| < \sqrt[n]{d(L)} \ \forall i\}$. Je-li $v \in K$, pak

$$\|v\| \leq \sqrt{n \cdot (\sqrt[n]{d(L)})^2} = \sqrt{n}\sqrt[n]{d(L)} \implies K \subseteq S.$$

Platí $\mathrm{vol}(K) = 2^n(\sqrt[n]{d(L)})^n = 2^n d(L)$, z čeho pak plyne $\mathrm{vol}(K) = 2^n d(L) \leq \mathrm{vol}(S)$. Ve skutečnosti dokonce platí $\mathrm{vol}(K) < \mathrm{vol}(S)$ (pozn.: nebylo vysvětleno proč) a tedy $2^n d(L) < \mathrm{vol}(S)$ a můžeme použít větu o mřížovém bodě, z které plyne tvrzení. □

Připomenutí: Pro $L \subseteq \mathbb{R}^n$ úplná, $i \in \{1, \dots, n\}$ definujeme
$\lambda_i(L) := \min\{r \in \mathbb{R}^+ \mid L \cap \{v \mid \|v\| \leq r\}$ obsahuje i LN vektorů$\}$.

Věta 3.43 (Minkowski). *Nechť $L \subseteq \mathbb{R}^n$ je úplná mříž. Pak $(\lambda_1(L) \cdot \ldots \cdot \lambda_n(L))^{\frac{1}{n}} \leq \sqrt{n}\sqrt[n]{d(L)}$.*

Lemma 3.44. *Nechť $L \subseteq \mathbb{R}^n$ je úplná mříž. Pak $\exists x_1, \ldots x_n \in L: \ \|x_i\| = \lambda_i(L) \ \forall i \in \{1, \dots, n\}$.*

Důkaz. Zvolíme x_1 nenulový vektor L s nejmenší normou, pak $\|x_1\| = \lambda_1(L)$. Když už máme vektory $x_1, \dots, x_i$, za x_{i+1} vezmeme vektor z $L \setminus < x_1, \dots, x_i >_{\mathbb{R}}$ s nejmenší normou.
Zjevně $\|x_i\| \geq \lambda_i(L)$. Pokud $\|x_i\| > \lambda_i(L)$, pak $M = \{v \in L \mid \|v\| < \|x_i\|\}$ obsahuje i LN vektorů. Proto $M \setminus < x_1, \dots, x_{i-1} >_{\mathbb{R}} \neq \emptyset$ a i-tý vektor by musel mít normu $< \|x_i\|$, spor. □

Důkaz. (Věta 3.43) Z předchozího lemmatu 3.44 plyne, že $\exists x_1, \dots, x_n \in L$ LN (báze $\mathbb{R}^n$) splňující $\|x_i\| = \lambda_i(L) \ \forall i \in \{1, \dots, n\}$. Gram-Schmidtovou ortogonalizací získáme z této báze ortogonální bázi $\{x_1^*, \dots, x_n^*\}$ prostoru $\mathbb{R}^n$ (konkrétně: položíme $x_1^* := x_1$, a následně
$x_j^* := x_j - \sum_{i=1}^{j-1} \mu_{j,i} x_i^*, \ \mu_{j,i} := \frac{x_j^T x_i^*}{x_i^{*T} x_i^*}$). Dále položíme $T := \{v \in \mathbb{R}^n \mid \sum_{i=1}^n (\frac{v^T x_i^*}{\lambda_i(L)\|x_i^*\|})^2 < 1\}$ a
$b_i := \frac{x_i^*}{\|x_i^*\|}$, pak $\{b_1, \dots, b_n\}$ je ON báze $\mathbb{R}^n$.
Zvolme $v \in \mathbb{R}^n$, pak $v = \sum_{i=1}^n r_i b_i$ pro nějaká $r_i \in \mathbb{R}$. Pak

$$v \in T \iff \sum_{i=1}^n \left(\frac{(\sum_{j=1}^n r_j b_j)^T b_i}{\lambda_i(L)} \right)^2 = \sum_{i=1}^n \frac{r_i^2}{\lambda_i(L)^2} < 1.$$

Vidíme, že T je středově souměrná a že je měřitelná a konvexní, jelikož z předchozího vztahu plyne, že T je elipsoid v $\mathbb{R}^n$. Plán: ukážeme, že $T \cap L = \{0\}$, pak Minkowského věty o mřížovém bodě 3.41 musí platit $\mathrm{vol}(T) \leq 2^n d(L)$.
Pro $v \in L \setminus \{0\}$ existuje $k \in \{1, \ldots, n\} : \ \|v\| \geq \lambda_k(L)$. Zvolme největší vyhovující k, pak máme $x_1, \ldots, x_k$ LN splňující $\|x_i\| = \lambda_i(L)$, a platí, že $v \in < x_1, \ldots, x_k >_{\mathbb{R}} = < x_1^*, \ldots, x_k^* >_{\mathbb{R}}$, neboť:

- Pokud $k = n$, pak $x_1, \ldots, x_n$ je báze $\mathbb{R}^n$, a
- jestli pro $k < n$ platí $v \notin < x_1, \ldots, x_k >_{\mathbb{R}}$, položíme $M := \{u \in L \mid \|u\| \leq \|v\|\}$. Pak M obsahuje vektory $x_1, x_2, \ldots, x_k, v$ a tudíž $\lambda_{k+1}(L) \leq \|v\|$ - spor s volbou k.

Pro toto k pak platí:

$$\sum_{i=1}^{n} \left(\frac{v^T x_i^*}{\lambda_i(L) \|x_i^*\|} \right)^2 \geq \sum_{i=1}^{k} \left(\frac{v^T x_i^*}{\lambda_i(L) \|x_i^*\|} \right)^2 \geq \frac{1}{\lambda_k(L)^2} \sum_{i=1}^{k} \left(\frac{v^T x_i^*}{\|x_i^*\|} \right)^2 = \frac{1}{\lambda_k(L)^2} \|v\|^2 \geq 1,$$

t.j. $v \notin T$, a tedy $\mathrm{vol}(T) \leq 2^n d(L)$.
Uvažme dále zobrazení $\phi : \mathbb{R}^n \to \mathbb{R}^n$ definováno předpisem $(r_1 \ \ldots \ r_n)^T \mapsto \sum_{i=1}^{n} \lambda_i(L) r_i b_i$. Platí $\phi((r_1 \ \ldots \ r_n)^T) \in T \iff \sum_{i=1}^{n} r_i^2 < 1$, a teda $\phi^{-1}(T) = \{v \in \mathbb{R}^n \mid \|v\| < 1\}$. Vezmeme jednotkovou krychli $K = [0,1] \times \ldots \times [0,1]$, pak $\phi(K) = [0, \lambda_1(L)] b_1 \times \ldots \times [0, \lambda_n(L)] b_n$ a platí $\mathrm{vol}(K) = 1$ a $\mathrm{vol}(\phi(K)) = \lambda_1(L) \cdot \ldots \cdot \lambda_n(L)$. Navíc pro S měřitelnou je $\mathrm{vol}(\phi(S)) = \lambda_1(L) \cdot \ldots \cdot \lambda_n(L) \cdot \mathrm{vol}(S)$, a tudíž

$$\mathrm{vol}(T) = \mathrm{vol}(B) \cdot \prod_{i=1}^{n} \lambda_i(L), \text{ kde } B = \{v \in \mathbb{R}^n \mid \|v\| < 1\}.$$

Nakonec

$$\left\{ (x_1 \ \ldots \ x_n)^T \mid |x_i| < \frac{1}{\sqrt{n}} \ \forall i \right\} \subseteq B$$

a tedy $\mathrm{vol}(B) \geq \left(\frac{2}{\sqrt{n}}\right)^n$. Spojením předchozích tak dostáváme

$$2^n d(L) \geq \mathrm{vol}(T) = \mathrm{vol}(B) \cdot \prod_{i=1}^{n} \lambda_i(L) \geq \left(\frac{2}{\sqrt{n}} \right)^n \cdot \prod_{i=1}^{n} \lambda_i(L) \implies \sqrt[n]{\prod_{i=1}^{n} \lambda_i(L)} \leq \sqrt{n} \sqrt[n]{d(L)}.$$

□

3.11 Gram-Schmidtova ortogonalizace

Nechť $b_1, b_2, \ldots, b_k$ jsou LN vektory v $\mathbb{R}^n$. Gram-Schmidtova ortogonalizace nalezne $b_1^*, b_2^*, \ldots, b_k^* \in \mathbb{R}^n$ splňující

1. $b_i^* \cdot b_j^* = 0 \ \forall 1 \leq i \neq j \leq k$,
2. $b_i^* = b_i - x_i, \ x_i \in < b_1, \ldots, b_{i-1} >_{\mathbb{R}}$ pro $i = 1, \ldots, k \ (i = 1 \implies b_1 = b_1^*)$

Poznámka 3.45.

- $< b_1, \ldots, b_i >_{\mathbb{R}} = < b_1^*, \ldots, b_i^* >_{\mathbb{R}} \ \forall 1 \leq i \leq k$,
- $b_i^* + x_i = b_i, \ x_i \in < b_1^*, \ldots, b_{i-1}^* >_{\mathbb{R}}, \ b_i^* \perp x_i$, t.j. b_i^* je kolmá projekce b_i do $< b_1, \ldots, b_{i-1} >^{\perp}$ a platí $\|b_i^*\|^2 + \|x_i\|^2 = \|b_i\|^2 \implies \|b_i^*\|^2 \leq \|b_i\|^2$.

Lemma 3.46. *$L \subseteq (\mathbb{R}^n, +)$ mříž s bází $b_1, b_2, \ldots, b_k$. Pak $\lambda_1(L) \geq \min\{\|b_1^*\|, \ldots, \|b_k^*\|\}$*

Důkaz. Chceme $\forall 0 \neq v \in L: \ \|v\| \geq \{\|b_1^*\|, \ldots, \|b_k^*\|\}$. Zvolme takové v, pak $v = \sum_{i=1}^{k} z_i b_i$, pro nějaké $z_1, \ldots, z_k \in \mathbb{Z}$. Zvolme $l \in \{1, \ldots, k\}$, tak, aby $z_l \neq 0$ a $z_{l+1} = \cdots = z_k = 0$. Pak $v = z_l b_l^* + \sum_{i=1}^{l-1} r_i b_i^*$ pro vhodná $r_1, \ldots, r_{l-1} \in \mathbb{R}$, a platí

$$\|v\|^2 = z_l^2 \|b_l^*\|^2 + \sum_{i=1}^{l-1} r_i^2 \|b_i^*\|^2 \geq \|b_l^*\|^2,$$

a tudíž $\|v\| \geq \|b_l^*\| \geq \min\{\|b_1^*, \ldots, b_k^*\}$. □

Značení 3.47. $b_i^* = b_i - \sum_{j=1}^{i-1} u_{i,j} b_j^*, \ u_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}$.
Chceme vyjádření $x_i = \sum_{j=1}^{i-1} r_j b_j, \ r_1, \ldots, r_{i-1} \in \mathbb{R}, \ (b_i - x_i) \cdot b_t = 0 \ \forall t = 1, 2, \ldots, i-1$.
Jest

$$0 = (b_i - \sum_{j=1}^{i-1} r_j b_j) \cdot b_t \iff \sum_{j=1}^{i-1} (b_t \cdot b_j) r_j = b_i b_t \ \forall t = 1, \ldots, i-1$$

$$\iff \begin{pmatrix} b_1 \cdot b_1 & \ldots & b_1 \cdot b_j & \ldots & b_1 \cdot b_{i-1} \\ \vdots & \ddots & \vdots & & \vdots \\ b_t \cdot b_1 & \ldots & b_t \cdot b_j & \ldots & b_t \cdot b_{i-1} \\ \vdots & & \vdots & \ddots & \vdots \\ b_{i-1} \cdot b_1 & \ldots & b_{i-1} \cdot b_j & \ldots & b_{i-1} \cdot b_{i-1} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{i-1} \end{pmatrix} = \begin{pmatrix} b_i \cdot b_1 \\ b_i \cdot b_2 \\ \vdots \\ b_i \cdot b_{i-1} \end{pmatrix}.$$

Tato matice se nazývá *Gramova matice* vektorů $b_1, \ldots, b_{i-1}$. Značíme ji $G_{b_1, \ldots, b_{i-1}}$.
Koeficienty $r_1, \ldots, r_{i-1}$ získáme řešením soustavy lineárních rovnic s maticí $G_{b_1, \ldots, b_{i-1}}$ a pravou stranou $(b_i \cdot b_1 \ \ldots \ b_i \cdot b_{i-1})^T$.

Tvrzení 3.48 (Hadamardova nerovnost). *Nechť $b_1, b_2, \ldots, b_k \in \mathbb{R}^n$ jsou lineárně nezávislé, pak $\det G_{b_1, \ldots, b_{i-1}} = \|b_1^*\|^2 \|b_2^*\|^2 \cdots \|b_k^*\|^2 \leq \|b_1\|^2 \|b_2\|^2 \cdots \|b_k\|^2$.*

Důkaz. Položme $A := (b_1 | b_2 | \cdots | b_k) \in M_{n,k}(\mathbb{R})$, $B := (b_1^* | b_2^* | \cdots | b_k^*) \in M_{n,k}(\mathbb{R})$. Pak $A^T A = G_{b_1, \ldots, b_{i-1}}$, neboť na pozici (t, j) je prvek $b_t \cdot b_j$. Podobně $B^T B = G_{b_1^*, \ldots, b_{i-1}^*} = \operatorname{diag}(\|b_1^*\|^2, \|b_2^*\|^2, \ldots \|b_k^*\|^2)$.
Vyjádříme-li pro všechna $i \in \{1, \ldots, k\}$ $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$, pak $A = BU$ pro

$$U := \begin{pmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \ldots & \mu_{k,1} \\ 0 & 1 & \mu_{3,2} & \ldots & \mu_{k,2} \\ 0 & 0 & 1 & \ldots & \mu_{k,3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Dále $\det G_{b_1, \ldots, b_{i-k}} = \det A^T A = \det U^T (B^T B) U = \det(U^T) \cdot \det(B^T B) \cdot \det(U) = \|b_1^*\|^2 \|b_2^*\|^2 \cdots \|b_k^*\|^2$, a nakonec z $\|b_i^*\| \leq \|b_i\| \ \forall i \in \{1, \ldots, k\}$ plyne $\|b_1^*\|^2 \|b_2^*\|^2 \cdots \|b_k^*\|^2 \leq \|b_1\|^2 \|b_2\|^2 \cdots \|b_k\|^2$. □

Připomenutí 3.49. Pro obecnou mříž $L = \mathbb{Z} b_1 + \cdots \mathbb{Z} b_k \subseteq \mathbb{R}^n$ definujeme $d(L) := \sqrt{\det A^T A}$, kde $A = (b_1 | b_2 | \cdots | b_k)$. Pak $d(L) = \sqrt{\det A^T A} = \|b_1^*\| \cdot \|b_2^*\| \cdot \ldots \cdot \|b_k^*\|$, tedy $d(L)$ lze chápat jako k-rozměrný objem množiny $F = \{\sum_{i=1}^{k} r_i b_i \mid r_i \in [0, 1)\}$ v $\mathbb{R}^n$.

3.12 Gaussova redukce úplné dvourozměrné mříže

Definice 3.50. Nechť $L \subseteq (\mathbb{R}^2, +)$ úplná mříž. Báze (b_1, b_2) mříže L se nazývá *nejkratší báze* L, pokud

1. $\forall v \in L \setminus \{0\} : \ \|v\| \geq \|b_1\|$,
2. $\forall v \in L \setminus <b_1>_{\mathbb{R}} : \ \|v\| \geq \|b_2\|$.

Příklad 3.51. Položme $L = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_5 + \mathbb{Z}f$, kde

$$e_1 = \begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}, \ e_2 = \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}, \ldots, \ e_5 = \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}, \ f = \begin{pmatrix}1/2\\1/2\\1/2\\1/2\\1/2\end{pmatrix}.$$

Množina $\{e_1, e_2, e_3, e_4, f\}$ tvoří bázi L a platí $e_5 = 2f - e_1 = e_2 - e_3 - e_4$. Ukážeme, že L nemá nejkratší bázi, tedy bázi $\{b_1, b_2, \ldots, b_5\}$, kde b_1 je nejkratší vektor $L \setminus \{0\}$, b_2 je nejkratší vektor $L \setminus <b_1>_{\mathbb{R}}$,$\ldots b_i$ je nejkratší vektor $L \setminus <b_1, \ldots, b_{i-1}>_{\mathbb{R}}$.
Je-li $v \in L \setminus \{0\}$, pak buď $v \in \mathbb{Z}^5 \implies \|v\| \geq 1$, nebo $v \in f + \mathbb{Z}^5 \implies \|v\| \geq \sqrt{5 \cdot 1/4} > 1$. Volme tedy postupně

$$\begin{aligned}
&b_1 \in \{\pm e_1, \ldots, \pm e_5\} \text{ takové, že } \|b_1\| = 1,\\
&b_2 \in \{\pm e_1, \ldots, \pm e_5\} \setminus \{\pm b_1\} \text{ takové, že } \|b_2\| = 1,\\
&b_3 \in \{\pm e_1, \ldots, \pm e_5\} \setminus \{\pm b_1, \pm b_2\} \text{ takové, že } \|b_3\| = 1,\\
&b_4 \in \{\pm e_1, \ldots, \pm e_5\} \setminus \{\pm b_1, \pm b_2, \pm b_3\} \text{ takové, že } \|b_4\| = 1,\\
&b_5 \in \{\pm e_1, \ldots, \pm e_5\} \setminus \{\pm b_1, \pm b_2, \pm b_3, \pm b_4\} \text{ takové, že } \|b_5\| = 1.
\end{aligned}$$

Avšak $f \notin \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_5 = \mathbb{Z}^5$, a tudíž nejkratší báze L by musela obsahovat alespoň 6 vektorů, spor.

Definice 3.52 (Algoritmus - Gaussova redukce mříže).
Vstup: (b_1, b_2) báze $L \subseteq \mathbb{Z}^2$
Výstup: nejkratší báze L

1. **repeat**

   i **if** $\|b_2\| < \|b_1\|$:
   vyměň hodnoty proměnných b_1 a b_2

   ii $x := \lfloor \mu_{2,1} \rceil = \lfloor \frac{b_2 \cdot b_1}{b_1 \cdot b_1} \rceil$ *//celočíselné zaokrouhlení* $\mu_{2,1}$

   iii $b_2 := b_2 - xb_1$

   until $x = 0$

2. **return** (b_1, b_2)

Poznámka 3.53. Položme $b_2' := b_2 - xb_1$ pro $x = \lfloor \mu_{2,1} \rceil$. Pak $b_2' := L \cap (b_2 + <b_1>_{\mathbb{R}})$ je bod L na přímce $b_2 + <b_1>_{\mathbb{R}}$ nejbližší k $b_2^* =$ ortogonální projekce b_2 na $<b_1>^{\perp}$.

Poznámka 3.54 (Zaokrouhlení). Pokud $\mu_{2,1} \in 1/2 \pm \mathbb{Z}$, lze $\mu_{2,1}$ zaokrouhlit nahoru i dolů. Ale pokud $\mu_{2,1} = \pm 1/2$, zaokrouhlíme vždy na nulu! (jinak může nastat endless loop)

4 LLL-redukovaná báze mříže

Definice 4.1. $b_1, \ldots, b_n \in \mathbb{R}^n$ je *LLL-redukovaná*, pokud

- (R1) $|\mu_{i,j}| \leq 1/2 \ \forall 1 \leq j < i \leq b$
- (R2) $\|b_i^*\|^2 \geq (3/4 - \mu_{i,i-1}^2 \|b_{i-1}^*\|^2 \ \forall 1 < i \leq n$

Kde $b_1^*, \ldots, b_n^*$ je G-S ortogonalizace $b_1, \ldots, b_n$, $\mu_{i,j}$ jsou koeficienty z G-S ortogonalizace $b_1, \ldots, b_n$, $b_1^* = b_1$, $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$, kde $\mu_{i,j} = \frac{b_i \cdot b_j^*}{\|b_j^*\|}$

Poznámka 4.2 (A. K. Lenstra, H. W. Lenstra, L. G. Lovász (1982)). Factory polynomials with rational coefficients $f \in \mathbb{Z}[x]$ primitivní:

- $p \in \mathrm{P}$
- faktorizace $f \mod p$ v $\mathbb{Z}_p[x]$
- Henselova "zdvihnutím"TODO rozklad $f \mod p^k$ v $\mathbb{Z}_{p^k}[x]$
- Kombinae faktorů až $2^{\deg f - 1}$ kombinací

Nahradit kombinací faktorů hledáním dostatečně krátkého vektoru v mříži.

Poznámka 4.3. Dále si rozebereme podmínku (R2)
$b_i^* \perp b_{i-1}^*$
$\|b_i^* + \mu_{i,j} b_{i-1}^*\| = \|b_i^*\|^2 + \mu_{i,i-1}^2 \|b_{i-1}^*\|$
(R2) $\|b_i^* + \mu_{i,i-1} b_{i-1}\|^2 \geq 3/4 \|b_{i-1}\|^2$

b_i^* je kolmá projekce b_i do $\langle b_1, \ldots, b_{i-1} \rangle^\perp$
$b_i = b_i^* + \sum L$ mříž s bází $b_1, \ldots, b_n$ b_1, b_n je LLL-redukovaná.
$L = \mathbb{Z} b_1 + \cdots + \mathbb{Z} b_n$, $1 \leq i \leq n$
$L' := \mathbb{Z} b_{i-1}^* + \mathbb{Z}(b_i^* + \mu_{i,i-1} b_{i-1}^*$ je kolmá projekce $\mathbb{Z} b_1 + \cdots + \mathbb{Z} b_n$ do $\langle b_1, \ldots, b_{i-1} \rangle^\perp$

TODO There are missing parts.

Lemma 4.4 (25.1 Ve skriptech). *Nechť $b_1, \ldots b_n$ je LLL-redukovaná báze $\mathbb{R}^n$. Pak $\|b_i\|^2 \leq 2^{j-1} \|b_j^*\| \ \forall 1 \leq i \leq j \leq n$*

Důkaz. (R1) + (R2) $\implies \|b_i^*\|^2 \geq \frac{1}{2} \|b_{i-1}^*\|^2$, indukcí $\|b_i^*\|^2 \geq \frac{1}{2^l} \|b_{i-l}\|^2 \ 0 \leq l < i$

$$\|b_i\|^2 = \|b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|b_j^*\| \overset{(R1)}{\leq} \|b_i^*\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} \|b_{i-j}^*\|^2$$

$$\leq \|b_i^*\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} 2^j \|b_i^*\|^2 = (1 + \underbrace{\frac{1}{4} \sum_{j=1}^{i-1})}_{2^{i-2}} \|b_i^*\|^2 = (2^{i-2} + \frac{1}{2}) \|b_i^*\|^2 \leq 2^{i-1} \|b_i^*\|^2$$

$\forall i \geq 1 \ 2^{i-2} + \frac{1}{2} \leq 2^{i-1} \iff 2^{i-1} + 1 \leq 2^i$.

Máme $\|b_i\|^2 \leq 2^{i-1} \|b_i^*\|^2$ a zároveň $\|b_i\|^2 \leq 2^{j-i} \|b_j^*\|^2$. Celkem tedy $\|b_i\|^2 \leq 2^{i-1} 2^{j-i} \|b_j^*\|^2 = 2^{j-1} \|b_j^*\|^2$. □

Tvrzení 4.5 (25.2). *Nechť $b_1,\dots,b_n$ je LLL-redukovná báze mříže $L \subseteq (\mathbb{R}^N,+)$. Pak $d(L) \leq \|b_1\|\cdots\|b_n\| \leq 2^{\frac{n(n-1)}{4}} d(L)$, $\|b_1\| \leq 2^{\frac{n(n-1)}{4}} \sqrt[n]{d(L)}$.*

Důkaz. $d(L)^2 = \|b_1^*\|^2\cdots\|b_n^*\|^2$ (platí pro každo bázi), $\|b_i\| \geq \|b_i^*\| \implies d(L) \leq \|b_i\|\cdots\|b_n\|$
Lemma 25.1 pro $i=j$: $\|b_i\|^2 \leq 2^{i-1}\|b_i^*\|^2$ $i=1,\dots,n$
$\implies \|b_1\|^2\cdots\|b_n\|^2 \leq 2^{\sum_{i=1}^n i-1}\|b_1^*\|^2\cdots\|b_n^*\|^2 = 2^{\frac{n(n-1)}{2}} d(L)^2$
$\implies \|b_1\|^2\cdots\|b_n\|^2 \leq 2^{\frac{n(n-1)}{4}} d(L)$
Lemma 25.1 $\implies$ ||| TODO konec důkazu □

Tvrzení 4.6 (25.3). *$b_1,\dots,b_n$ LLL-redukovaná báze mříže $L \subseteq (\mathbb{R}^n,+)$. $\forall 0 \neq v \in L : \|b_1\| \leq 2^{\frac{n-1}{2}}\|v\|$*

Důkaz. $v = z_1b_1 + \cdots + z_nb_n$, $z_1,\dots,z_n \in \mathbb{Z}$
$v \neq 0 : \exists k$ $z_k \neq 0$, $z_{k+1} = z_{k+2} = \cdots = z_n = 0$
$v = \sum_{i=1}^k z_ib_i = \sum_{i-1}^k z_i(b_i^* + \sum_{j=1}^{i-1}\mu_{i,j}b_j^*) = z_kb_k^* + \sum_{j=1}^{k-1} r_jb_j^*$
$\|v\|^2 = \underbrace{z_k^2}_{z_k^2\geq 1}\|b_k^*\|^2 + \sum_{j=1}^{k-1} r_j^2\|b_j^*\|^2 \geq \|b_k^*\|^2 \overset{25.1}{\geq} \frac{1}{2^{k-1}}\|b_1\|^2$
$2^{n-1}\|v\|^2 \geq 2^{k-1}\|v\|^2 \geq 2^{k-1}\|v\|^2 \geq \|b_1\|^2 \implies 2^{\frac{n-1}{2}}\|v\| \geq \|b_1\|$
$r_j \in \mathbb{R}$

□

Definice 4.7 (LLL algoritmus). (základní verze)
VSTUP: $b_1,\dots,b_n$ báze $L \subseteq (\mathbb{Z}^n,+)$
VÝSTUP: LLL-redukovaná báze L

1. G-S ortogonalizace $b_1,\dots,b_n$. Spočteme $b_1^*,\dots,b_n^*$ a $\mu_{i,j}$ pro $1 \leq j \leq i \leq n$
2. for i=2 to n do:
   - for j=i-1 downto 1 do:
     - $x := \lfloor \mu_{i,j} \rceil$ //celočíselné zaokrouhlení
     - $b_i := b_i - xb_j$
     - $\mu_{i,j} := \mu_{i,j} - x$ // $\mu_{i,j} \in \langle -1/2, 1/2\rangle$
     - for l=1 to j-1 do: $\mu_{i,l} := \mu_{i,l} - x\mu_{j,l}$
3. for i=2 to n do:
   - if $\|b_i^*\|^2 < (3/4 - \mu_{i,i-1}^2)\|b_{i-1}^*\|$ then
     - prohoď hodnoty v b_i a b_{i-1}
     - GOTO 1
4. return $b_1,\dots,b_n$

Poznámka 4.8. V průběhu algoritmu v proměnných $b_1,\dots,b_n$ je vždy báze L.
$b_1,\dots,b_n$ báze L, $i \neq j$, $z \in \mathbb{Z}$
$b_1,\dots,b_{i-1},b_i - xb_j,b_{i+2},\dots,b_n$ také báze L.

Po skončení kroku 2 jsou v proměnných $b_1^*,\dots,b_n^*,\mu_{i,j}$ data z G-S ortogonalizace báze v proměnných $b_1,\dots,b_n$ $\implies$ po skončení kroku 2 báze v proměnných $b_1,\dots,b_n$ splňuje (R1). Pokud nevyskočíme z kroku 3, je splněna podmína (R2)

Tvrzení 4.9. *Nechť $b_1, \ldots, b_n$; $c_1, \ldots, c_n$ jsou dvě báze $\mathbb{R}^n$, $x \in \mathbb{R}$*
$1 \leq j < i \leq n$, $c_l = b_l \ \forall l \neq i$ a zároveň $c_i = b_i - xb_j$
$b_1^*, \ldots, b_n^*$ G-S ortogonalizace $b_1, \ldots, b_n$
$c_1^*, \ldots, c_n^*$ G-S ortogonalizace $c_1, \ldots, c_n$
Pak $b_l^* = c_l^* \ \forall l \in \{1, \ldots, n\}$

Důkaz. c_l^* je ortogonální projekce c_l do $\langle c_1, \ldots, c_{l-1} \rangle^\perp$
b_l^* je ortogonální projekce b_l do $\langle b_1, \ldots, b_{l-1} \rangle^\perp$
Celkem $\implies c_l^* = b_l^* \ \forall l \neq i$
$c_i = b_i - \underbrace{xb_j}_{\in \langle b_1, \ldots, b_{i-1} \rangle}$ ortogonální projekce c_i do $\langle b_1, \ldots, b_{i-1} \rangle^\perp = b_i^* + 0 \implies c_i^* = b_i^*$. □