# 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 $G \cap \{v \in \mathbb{R}^n \,|\, \|v - g\| < \varepsilon\} = \{g\}$. □