

# Algoritmy na mřížích

Pavel Příhoda

3. listopadu 2021



# Obsah

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Úvod</b>                                | <b>2</b> |
| 1.1      | Algebraická struktura mříží . . . . .      | 2        |
| 1.2      | Rozložení mříže v $\mathbb{R}^n$ . . . . . | 2        |

# 1 Úvod

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

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

## 1.1 Algebraická struktura mříží

- $L$  je komutativní grupa (podgrupa grupy  $(\mathbb{R}^n, +)$ )
- $L$  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  $\mathbb{R}^n$ ).** Necht  $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ ,  $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ . 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  $\|u\| := \sqrt{u \cdot u} = (\sum_{i=1}^n u_i^2)^{\frac{1}{2}}$ .

## 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

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

**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.*  $\Rightarrow \checkmark$

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