

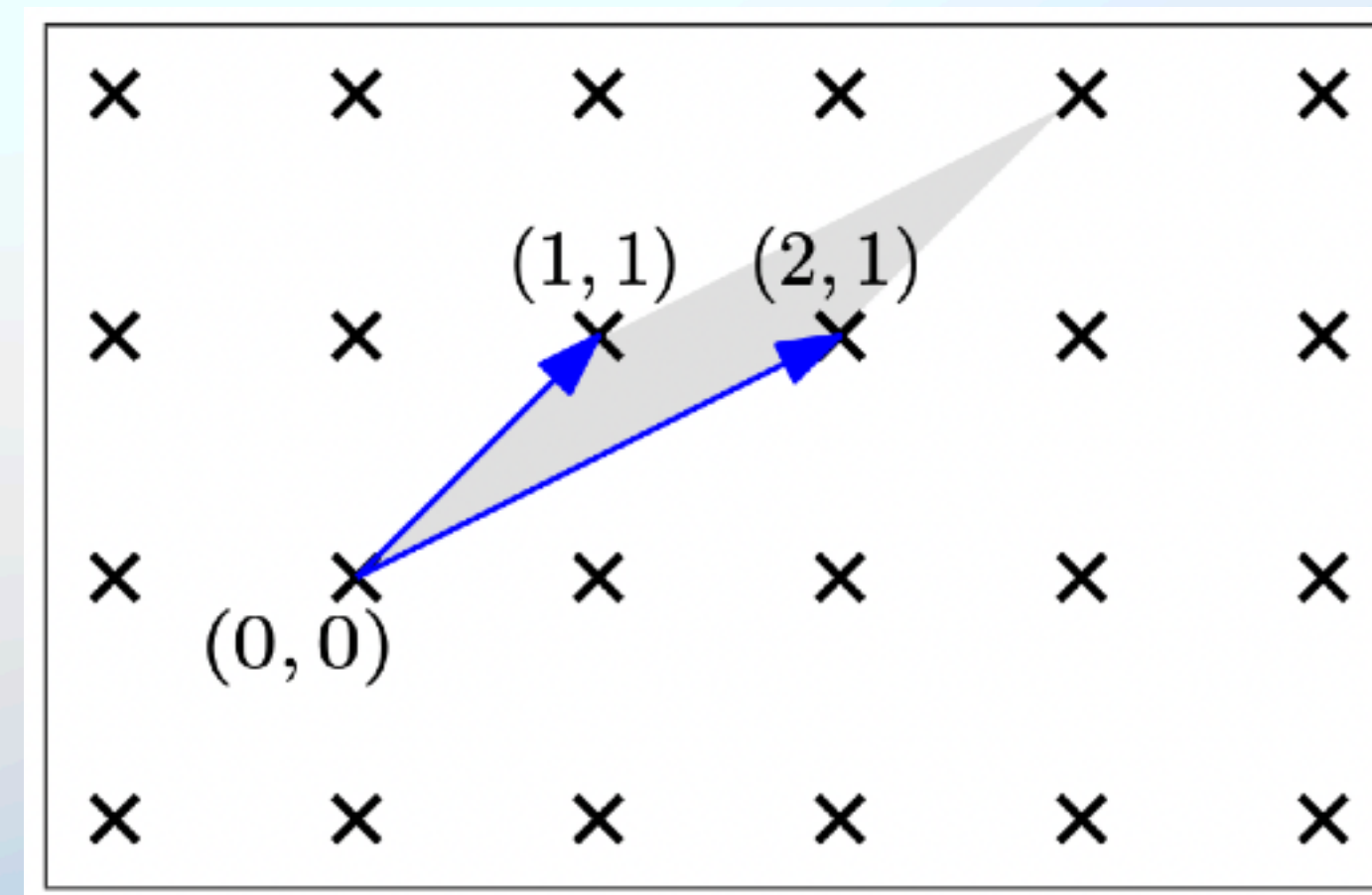
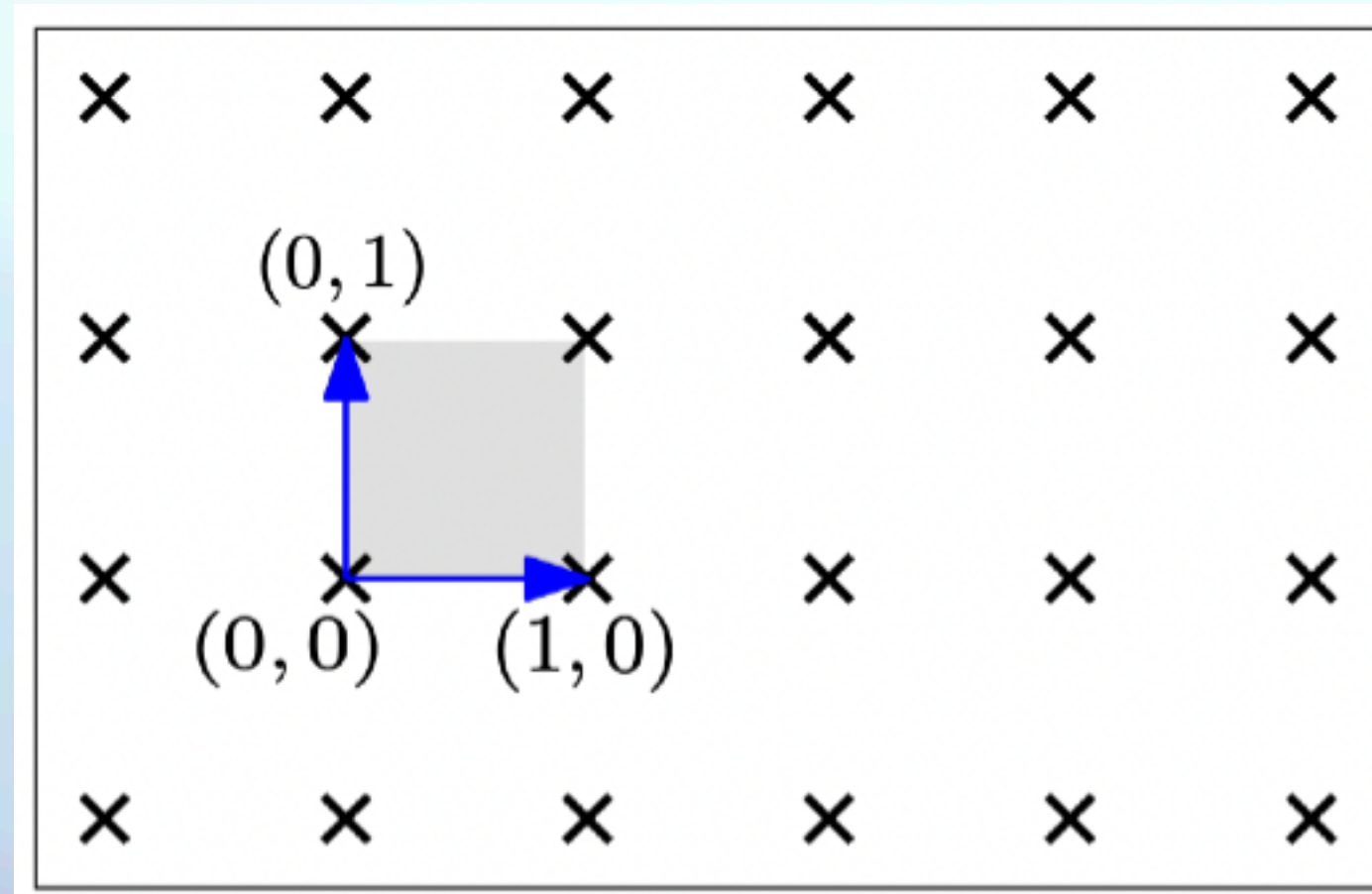
# Réseau d'un espace vectoriel Euclidien

a.k.a. a lattice, a discrete subgroup of  $\mathbb{R}^n$

- Soient  $n \in \mathbb{N}$  et  $B \in GL_n(\mathbb{R})$  avec colonnes  $b_1, \dots, b_n \in \mathbb{R}^n$
- Alors le réseau  $\mathcal{L}$  engendré par la base  $B$  se note

$$\mathcal{L}(B) = \left\{ \sum_{i=1}^n x_i b_i : x_i \in \mathbb{Z} \right\} \subseteq \mathbb{R}^n$$

- Ex  $\mathbb{Z}^2$ :



# Problème du vecteur le plus court

a.k.a. the Shortest Vector Problem (SVP)

- Étant donné un réseau  $\mathcal{L}$ , notons la longueur de son plus petit vecteur non nul

$$\lambda(\mathcal{L}) = \min_{v \in \mathcal{L} \setminus \{0\}} \|v\|$$

- Le problème du vecteur le plus court demande à trouver un tel  $v$  étant donné une base  $B$

