I. Теорема Минковского

Для решётки $L \subseteq \mathbb{R}^d$ ранга d справедливо

(1) $\lambda_1(L) \le \sqrt{d} \cdot (\det L)^{1/d}$ $\qquad \lambda_1(L) = \min\limits_{b \in L,\ b \ne 0} \|b\|$

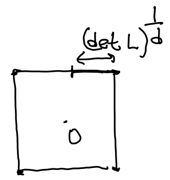
(2) $\lambda_1^{\infty}(L) \le (\det L)^{1/d}$ $\qquad \lambda_1^{\infty}(L) = \min\limits_{b \in L,\ b \ne 0} \|b\|_\infty$, $\|\cdot\|_\infty = \max\limits_i |b_i|$

Для док-ва т-мы Минковского $\divideontimes$ 2 другие теоремы.

Теорема 1. $\exists S \subseteq \mathbb{R}^d$ – симметрическое, выпуклое мн-во, т.ч. $\underline{\mathrm{vol}(S) > 2^d \cdot \det(L)}$

Тогда S содержит ненулевой вектор L.

(Если S компактно, достаточно условия $\mathrm{vol}(S) \ge 2^d \cdot \det(L)$)



Т-ма 1 $\Rightarrow$ т-му Минковского. $\quad S = [-(\det L)^{1/d}, (\det L)^{\frac{1}{d}}]$

$\mathrm{vol}(S) = 2^d \left((\det L)^{\frac{1}{d}}\right)^d = 2^d \cdot \det(L)$

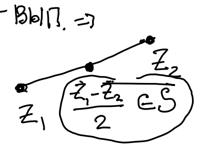
В S $\underline{\exists b \in L \setminus \{0\}}$ и $\underline{\|b\|_\infty \le (\det L)^{1/d}}$ $\Rightarrow$ выполняется (2)

$\underline{\|b\|_2 \le \sqrt{d} \cdot \|b\|_\infty} \le \sqrt{d} \cdot (\det L)^{1/d} \Rightarrow$ —//— (1)

Теорема 2 (Блихфельд) $\underline{L \subseteq \mathbb{R}^d \text{ – решётка},\ E \subseteq \mathbb{R}^d, \text{ т.ч. } \mathrm{vol}(E) > \det(L).}$

$\underline{\text{Тогда } \exists z_1 \ne z_2 \in E, \text{ т.ч. } z_1 - z_2 \in L.}$

S-вып. $\Rightarrow$



Теорема 2 $\Rightarrow$ Теорема 1. В качестве $E = S/2$. Тогда $\mathrm{vol}(E) > \det(L) \Rightarrow$

$\Rightarrow \exists z_1 \ne z_2 \in E : z_1 - z_2 \in L$;

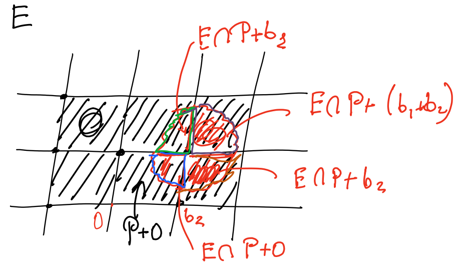
$z_1 - z_2 = 2 \cdot \underbrace{\frac{z_1 - z_2}{2}}_{\text{выпукл.}}$ симм. $\Rightarrow \frac{z_1 - z_2}{2} \in \frac{S}{2} \Rightarrow z_1 - z_2 \in E \Rightarrow \underline{\exists z_1 - z_2 \in L.}$ $\ne 0$

$\frac{S}{2} = E$

Док-во т-мы 2. $\divideontimes$ $\bigcup\limits_{b \in L} \{P + b\}$ – это разбиение $\mathbb{R}^d$ (tiling)

$E = \coprod\limits_{b \in L} \{E \cap P + b\}$

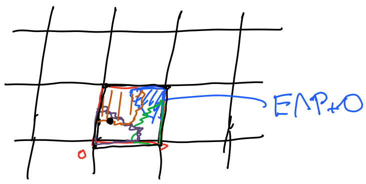
непересекающееся объединение



$\mathrm{vol}(L) < \mathrm{vol}(E) = \sum\limits_{b \in L} \mathrm{vol}\,(\underbrace{E \cap P + b}_{})$

$\mathrm{vol}(L) < \mathrm{vol}(E) = \sum\limits_{b \in L} \mathrm{vol}\left(\underbrace{(E - b) \cap P}_{}\right)$

$\mathrm{vol}(L) = \mathrm{vol}(P)$ $\qquad$ содержатся в P



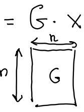
$\exists b_1 \ne b_2 \in L$ т.ч. $((E - b_1) \cap P) \cap ((E - b_2) \cap P) \ne \varnothing$

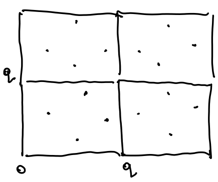
Возьмём $z \in (\underline{(E - b_1)} \cap P) \cap (\underline{(E - b_2)} \cap P)$, $z_1 = \underbrace{z + b_1}_{\in E}$, $z_2 = \underbrace{z + b_2}_{\in E}$, $z_1 - z_2 = b_1 - b_2 \in L$. ◆

II. Построение решёток из кодов

Опр. 1 "Конструкция A". C – линейный $[m, n, q]$ – код (т.е. $C = G \cdot x$, $x \in \mathbb{Z}_q^n$)

m – длина, n – размерность, q – простое





Определим $L(C) = L(G) = \underline{C} + q\mathbb{Z}^m = \underline{G\mathbb{Z}_q^n} + \underline{q\mathbb{Z}^m}$

$$G = \begin{array}{c} n \\ m-n \end{array}\begin{bmatrix} G_{top} \\ G_{bot} \end{bmatrix}$$

Положим $G_{Top} \in \mathbb{Z}_q^{n \times n}$ – обратима. Тогда $\underline{G \cdot G_{Top}^{-1}} = \begin{bmatrix} Id_n \\ G_{bot} \cdot G_{Top}^{-1} \end{bmatrix}$

$$\left[\begin{array}{c|c} Id_n & \\ G_{bot} \cdot G_{Top}^{-1} & \end{array}\right] \left|\ q I_m \right]$$

Отсюда, столбцы матрицы образуют базис $L(C) = L(G)$

$$\begin{array}{c} \\ m \end{array} \overset{m}{\left[\begin{array}{c|c} I_n & 0 \\ \hline G_{bot} \cdot G_{Top}^{-1} & q I_{m-n} \end{array}\right]}$$

- $\dim(L) = m$
- $\det(L) = q^{m-n}$

по теореме Минковского $\lambda_1^{\infty}(L(C)) \leqslant (\det L)^{\frac{1}{d}} = q^{\frac{m-n}{m}} = \underline{q^{1-\frac{n}{m}}}$.

Теорема Минковского-Хлавки. С вероятностью $\geqslant 1 - 2^{-m}$ (над случ. выбором $G \in \mathbb{Z}_q^{m\times n}$) имеем

$$\underline{\lambda_1^{\infty}(L(G)) \geqslant \frac{1}{4} q^{1-\frac{n}{m}}}.$$

◀ Зафиксируем $\underline{B = \frac{1}{4} q^{1-\frac{n}{m}}}$

$$\Pr_{G \leftarrow \mathbb{Z}_q^{m\times n}}[\lambda_1^{\infty}(L(G)) < B] = \Pr_G[\exists s \in \mathbb{Z}_q^n, y \in \mathbb{Z}_q^m : 0 < \|y\|_\infty < B \text{ и } y = \underline{G\cdot s} \bmod q] \leqslant \underbrace{\sum_{s\in\mathbb{Z}_q^n} \sum_{\substack{y\in\mathbb{Z}_q^m \\ 0<\|y\|_\infty<B}}}_{\substack{\text{(union bound, н-во Буля)} \\ \Pr[\cup A_i] \leqslant \sum \Pr[A_i]}} \Pr[y = G\cdot \underline{s} \bmod q]$$

(1) $s = 0 \Rightarrow \Pr[\ldots] = 0$

(2) $y = G\cdot s$, $s \neq 0$ — фиксировано

$$y = \boxed{G}\, s$$

$$\leqslant \sum_{s\in\mathbb{Z}_q^n\setminus\{0\}} \sum_{\substack{y\in\mathbb{Z}^m \\ 0<\|y\|_\infty<B \\ = \\ \underline{-B<y_i<B}}} \Big[\prod_{i=1}^{m} \underbrace{\langle \underset{\substack{\uparrow \\ i\text{-ая строка } G}}{g_i}, \underline{s}\rangle = \underline{y_i} \bmod q}_{= \frac{1}{q}\ (s\neq 0)}\Big] = q^n \cdot (2(B-1))^m \cdot q^{-m} =$$

$$= \frac{(2B-1)^m}{q^{m-n}} = \left(\frac{2B-1}{q^{1-\frac{n}{m}}}\right)^m < 2^{-m} \text{ (для заданного } B\text{)}.$$

▷.