Лекция № 2
Теорема Минковского. Построение решёток из кодов. QR-факторизация

I. Теорема Минковского

<u>Теорема 1</u> (т-ма Минковского)

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

1) $\lambda_1(L) \le \sqrt{d} \cdot (\det L)^{\frac{1}{d}}$ // $\lambda_1(L) = \min\limits_{b \in L \setminus \{0\}} \|b\|_2$

2) $\lambda_1^{\infty}(L) \le (\det L)^{\frac{1}{d}}$ // $\lambda_1^{\infty}(L) = \min\limits_{b \in L \setminus \{0\}} \|b\|_{\infty}$

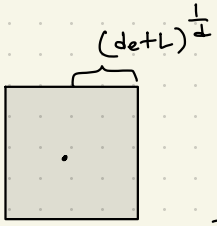
$\|\cdot\|_{\infty} = \max\limits_i |b_i|$

Для док-ва т-мы Минковского ∄ 2 другие теоремы.

<u>Теорема 2</u>] $S \subseteq \mathbb{R}^d$ – симметричное, выпуклое компактное мн-во, т.ч. $\mathrm{Vol}(S) \ge 2^d \cdot \det L$.

Тогда S содержит ненулевой вектор L.

<u>Т-ма 2 ⇒ Т-ма Минковского:</u>



$S = [-(\det L)^{\frac{1}{d}}, (\det L)^{\frac{1}{d}}]$

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

По т-ме 2: $\exists b \in L \setminus \{0\}$ и т.к. $b \in S$, то $\|b\|_{\infty} \le (\det L)^{\frac{1}{d}} \Rightarrow$

$\Rightarrow$ выполняется (2) т-мы 1.

$\|b\|_2 \le \sqrt{d}\, \|b\|_{\infty} \Rightarrow \|b\|_2 \le \sqrt{d} \cdot (\det L)^{\frac{1}{d}} \Rightarrow$ выполняется (1).

Теорема 3 (Блихфельд) $L \subseteq \mathbb{R}^d$ – решётка, $E \subseteq \mathbb{R}^d$, т.ч. $\mathrm{Vol}(E) \geq \det(L)$. Тогда $\exists\, z_1, z_2 \in E$, $z_1 \neq z_2$, т.ч. $z_1 - z_2 \in L$.

$\boxed{\text{Т-ма 3} \Rightarrow \text{Т-ма 2}}$

В качестве $E = \frac{S}{2}$. Тогда $\mathrm{Vol}(E) = \frac{\mathrm{Vol}(S)}{2^d} \geq \det(L)$. Тогда $\exists\, z_1, z_2 \in E$, т.ч. $z_1 - z_2 \in L$.

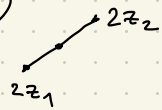
Покажем, что $z_1 - z_2 \in S$:

$$z_1 - z_2 = 2 \cdot \frac{z_1 - z_2}{2} = \frac{1}{2}(2z_1 - 2z_2)$$

$z_1, z_2 \in E \Rightarrow 2z_1, 2z_2 \in S$;

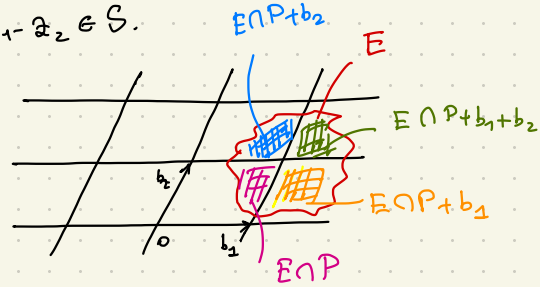
$-2z_2 \in S$ (S – симметрично)

$\frac{2z_1 - 2z_2}{2} \in S$ (выпукло)



$\Rightarrow z_1 - z_2 \in S$.

$\boxed{\text{Док-во теоремы 3}}$



$\bigcup_{b \in L} \{P + b\}$ – это разбиение в $\mathbb{R}^d$ (tiling)

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

непересекающееся объединение

для "=" используем компактность E.

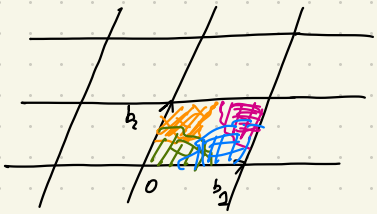
$$\det L = \underset{\mathrm{Vol}(P)}{\underset{\parallel}{\mathrm{Vol}(L)}} < \mathrm{Vol}(E) = \sum_{b \in L} \mathrm{Vol}(E \cap P + b) = \sum_{b \in L} \mathrm{Vol}((E - b) \cap P)$$

по усл-ию т-мы

$\exists\, v_1, v_2 \in L$, т.ч.

$$((E - v_1) \cap P) \cap ((E - v_2) \cap P) \neq \varnothing$$

$\triangleleft\ z \in ((E - v_1) \cap P) \cap ((E - v_2) \cap P)$



$$z_1 = \underbrace{z + v_1}_{\in E}, \quad z_2 \in \underbrace{z + v_2}_{\in E}$$

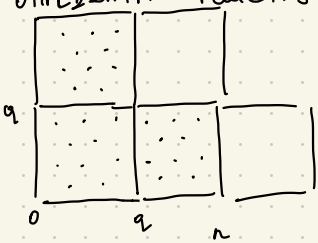
$$z_1 - z_2 = z + v_1 - z - v_2 = \overset{\in L}{v_1} - \overset{\in L}{v_2} \in L. \quad \blacktriangleright$$

II Построение решёток из кодов

Опр. 1 Конструкция "А" C - лин. код $[\overset{\text{длина}}{m}, \overset{\text{размерность}}{n}]_q$ - код, т.е.

$$C = G \cdot x, \quad x \in \mathbb{Z}_q^n \qquad \begin{array}{c} \leftarrow n \rightarrow \\ \uparrow m \downarrow \end{array} \boxed{G}$$

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



$$G = \begin{array}{c} n \\ m-n \end{array} \left[\begin{array}{c} G_{top} \\ \hline G_{bot} \end{array} \right]$$

Положим, $G_{top} \in \mathbb{Z}_q^{n \times n}$ - обратима. Тогда

$$G \cdot G_{top}^{-1} = \left[\begin{array}{c} I_n \\ \hline G_{bot} \cdot G_{top}^{-1} \end{array} \right] \xrightarrow{\text{базис } L(C):} \left[\begin{array}{c|c} I_n & 0 \\ \hline G_{bot} G_{top}^{-1} & q I_{m-n} \end{array} \right]$$

$\dim L(C) = m$

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

По т-ме Минковского: $\lambda_1^\infty \le \det(L)^{\frac{1}{m}} = q^{\frac{m-n}{m}} = q^{1-\frac{n}{m}}$

Теорема 4 (Минковский - Хлавка)

$\exists\, q \geq 2$ - простое, G - выбрана случайно равномерно из $\mathbb{Z}_q^{m \times n}$. Тогда с вероятностью $\geq 1 - 2^{-m}$

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

III QR-факторизация

III.1 HNF (Hermit Normal Form)
Эрмитова нормальная форма

$\forall B \in \mathbb{Z}^{n\times k}$ $\exists\, U \in GL_k(\mathbb{Z})$ т.ч. $B\cdot U = \left[\begin{array}{ccc|c} 0 & \dots & 0 & \\ \times & & & \\ & \times & & 0 \\ & & \times\times\times & \end{array}\right]$ и

коэффициенты в строке с эл-том X на главной диагонали будут лежать в интервале $[0, X)$

Полученная матрица для B уникальна и носит название HNF формы B.

Находится HNF аналог. "Гауссовому" преобразованию, где деление заменяется на НОД.

<u>Приложение</u> B_1, B_2 - базисы $L_1, L_2 \subseteq \mathbb{Z}^n$, HNF позволяет вычислить базис $L_1 + L_2 = B_1\mathbb{Z}^n + B_2\mathbb{Z}^n$, а именно $HNF(B_1 \| B_2)$.

Сложность вычисления $\tilde{O}\left(\max(n,k)^{\omega+1} \cdot \lg \max_i \|b_i\|\right)$ бит. операций

где ω - константа умножения матриц

$\tilde{O}(f(n)) = O(f(n)\cdot \log f(n))$

III.2 QR-факторизацию

$Q\cdot Q^T = Q^T\cdot Q = Id$

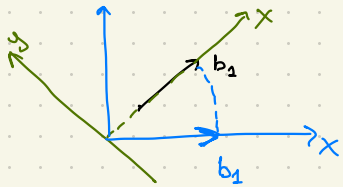
$\Updownarrow$

<u>Опр.2</u> $\exists B \in \mathbb{R}^{n\times n}$ $(\det B \neq 0)$ $\exists\, Q$ - ортогональная и R - Δ-ая, т.ч.

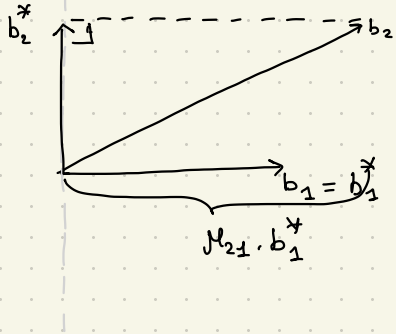
$B = QR$ $\quad \boxed{B} = \boxed{Q}\cdot\boxed{R}$, $r_{ii} > 0\ \forall i$

Такая декомпозиция уникальна.

<u>Смысл</u>



QR факторизация связана с процессом ортогонализации Грам-Шмидта (ГШ)



1. $b_1^* = b_1$
2. $b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^*$,

где $\mu_{ij} = \dfrac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$

$\mu_{ii} = 1$

$$B = Q \cdot R = \underbrace{Q \cdot (\mathrm{diag}\, r_{ii})}_{B^*} \cdot \underbrace{(\mathrm{diag}\, r_{ii})^{-1} \cdot R}_{(\mu_{ij})^T}$$

$$\begin{bmatrix} | & & | \\ b_1^* & \dots & b_n^* \\ | & & | \end{bmatrix}$$

<u>Замечание</u> QR и ГШ несут одну и ту же информацию о решётке. Q, R не обязаны быть рациональными, (B^*, μ) — рациональные для $B \in \mathbb{Z}^{n \times n}$ и их битовая длина числ./знам. элтов B^* ограничена — $\mathrm{poly}(\lg b_{ij})$.

Сложность $O(n^3)$ арифм. операций — точно в ГШ.
— приблизительно в QR.

В упр-ниях:

1) $\forall x: \|Bx\| = \|Rx\|$ $(B = QR)$
2) $B = QR$ $\lambda_1(L(B)) \geq \min_i (r_{ii})$.