Лекция №2

Теорема Минковского

QR-факторизация

I. Теорема Минковского.

Теорема 1 (Т-ма Минковского)

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

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

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

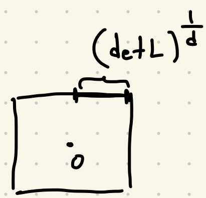
$\|\cdot\|_\infty = \max\limits_i |b_i| \}$

Для док-ва теоремы Минковского $\ast$ 2 другие теоремы.

Теорема 2 $\exists S \subseteq \mathbb{R}^d$ – симметричное, выпуклое мн-во, что $\mathrm{vol}(S) > 2^d \det L$

Тогда S содержит ненулевой вектор L.

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



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

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

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

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

Теорема 3 (Блихфельд) $L \subseteq \mathbb{R}^d$ – решётка, $E \subseteq \mathbb{R}^d$, т.ч. $\mathrm{vol}(E) > \det(L)$;

Тогда $\exists\ z_1, z_2 \in E$, т.ч. $z_1 - z_2 \in L$.
$z_1 \neq z_2$

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

В качестве $E = \frac{S}{2}$; Тогда $\mathrm{vol}(E) = \frac{\mathrm{vol}\, S}{2^d} > \det L$.

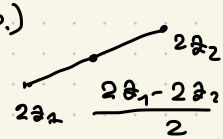
$\exists\, a_1, a_2 \in E$, т.ч. $a_1 - a_2 \in L$.

Покажем, $a_1 - a_2 \in S$. $a_1 - a_2 = 2 \cdot \frac{a_1 - a_2}{2} = \frac{1}{2}(2a_1 - 2a_2)$;

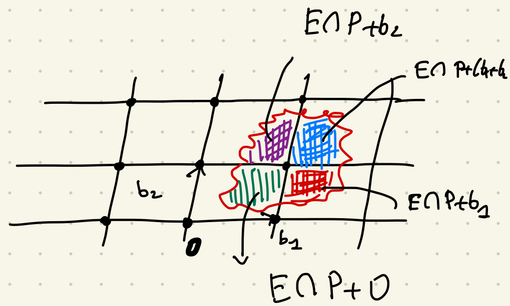
$a_1, a_2 \in E \Rightarrow 2a_1, 2a_2 \in S$;

$-2a_2 \in S$ (S - симметр.)

$\frac{2a_1 - 2a_2}{2} \in S$ (S - выпукл.)



$\Rightarrow \underbrace{\overset{\ne 0}{a_1 - a_2}}_{\in L} \in S$.



$\boxed{\text{Док-во теоремы 3}}$

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

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

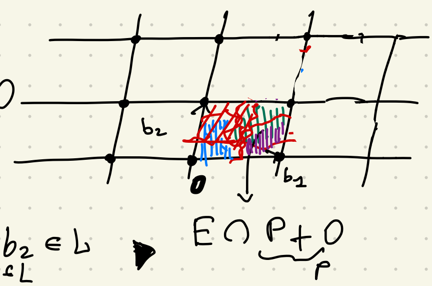
непересекающееся объединение

$\det L = \mathrm{vol}(L) \underset{\text{(по усл-ию т-мы)}}{<} \mathrm{vol}(E) = \sum_{b\in L} \mathrm{vol}(E\cap P+b)$

$\mathrm{vol}(L) < \mathrm{vol}(E) = \sum'_{b\in L} \mathrm{vol}(\underbrace{(E-b)\cap P}_{\text{содержится в } P})$

$\exists\, b_1 \ne b_2 \in L$, т.ч.

$((E - b_1)\cap P) \cap ((E - b_2)\cap P) \ne 0$



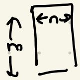
Возьмём $a \in ((E-b_1)\cap P)\cap((E-b_2)\cap P)$

$a_1 = \underbrace{a+b_1}_{E}$, $a_2 = \underbrace{a+b_2}_{\in E}$, $a_1 - a_2 = \underbrace{b_1}_{\in L} - \underbrace{b_2}_{\in L} \in L$ ▶

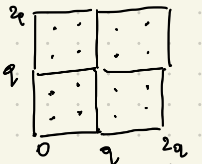
II Построение решёток из кодов

Опр. 1 Конструкция "A": C – линейный $[m, n, q]$ – код
длина (m), размерность (n), простое (q)

(т.е. $C = G \cdot x$, $x \in \mathbb{Z}_q^n$)



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



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

Положим $G_{top} \in \mathbb{Z}_q^{n\times n}$ – обратима. Тогда $G \cdot G_{top}^{-1} = \left[\begin{array}{c} I_n \\ \hline G_{bot} \cdot G_{top}^{-1} \end{array}\right]$

$$\left[\begin{array}{c|c} I_n & \\ & qI_m \\ G_{bot} \cdot G_{top}^{-1} & \end{array}\right] \rightarrow \underbrace{\left[\begin{array}{c|c} I_n & 0 \\ G_{bot} \cdot G_{top}^{-1} & qI_{m-n} \end{array}\right]}_{\text{базис } L(C)}$$

$\dim L(C) = m$

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

По т-ме Минковского, $\lambda_1^\infty \leq (\det L)^{\frac{1}{\dim}} = q^{\frac{m-n}{m}} = q^{1-\frac{n}{m}}$.

Теорема (Минковский – Хлавка)

С вероятностью $\geq 1 - 2^{-m}$ (над случайным выбором $G \in \mathbb{Z}_q^{m\times n}$):

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

III Редукция базиса решётки: начало.

III.1

Смысл: нахождение "хорошего" представление базиса решётки.

HNF (Hermit Normal Form)
Эрмитова нормальная форма

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

коэфф-ты в строке с эл-том X на гл. диагонали лежат в интервале $[0, X)$.

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

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

Приложение: 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: $\tilde{O}\left(\max(n,k)^{\omega+1} \cdot \lg \max\|b_i\|\right)$ - бит. сложность

ω - конст. умножения матриц;

III.2 QR-факторизация

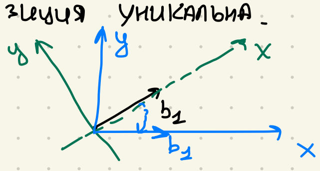
$$Q\cdot Q^T = Q^T\cdot Q = Id$$
$$\Uparrow$$

Опр 1. $\forall B \in \mathbb{R}^{n\times n}$ $(\det B \neq 0)$. $\exists Q$ - ортогональная и R - $\triangle$ая, т.ч.

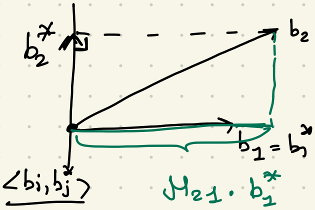
$$B = Q\cdot R \qquad \boxed{B} = \boxed{Q}\cdot\boxed{R}, \quad r_{ii} > 0 \ \forall i.$$

Такая декомпозиция уникальна.

Смысл Q:



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



$b_1^* = b_1$

$$b_i^* = b_i - \sum_{j<i} \mu_{i,j} b_j^*, \quad \mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\|b_j\|^2}$$

$\mu_{ii} = 1$

диагональные в R

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

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

<u>Замечание</u> QR и ГШ несут одну и ту же инфу о решётке

Q, R не обязаны быть рациональные, B^*, μ – рациональные для $B \in \mathbb{Z}^{n \times n}$ и их битовая длина числ./знамен. эл-тов B^*, μ – $poly(\lg(b_{ij}))$.

Сложность $O(n^3)$ арифм. операций → точно в ГШ
↘ прибл. в QR.

В упр:

1) $\forall x: \|Bx\| = \|Rx\| \quad (B = QR)$

2) $B = QR \quad \lambda_1(L(B)) \geq \min_i (r_{ii})$