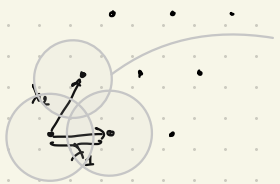
Лекция №10.

Сглаживающий параметр.

I. Transference theorem
(связь решётки и её дуальной)

Опр-ие $\mu(L) = \max\limits_{c \in \mathbb{R}^n} \operatorname{dist}(c, L) = \max\limits_{c \in \mathbb{R}^n} \min\limits_{b \in L} \|b - c\|$ - покрывающий радиус



Шары покрывают всё $\mathbb{R}^2$

Пример: $\mu(\mathbb{Z}^n) = \frac{\sqrt{n}}{2}$ и определяется $c = \left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}\right)$

Можно показать, что $\mu_n(L) \geq \frac{\lambda_n}{2}$

Теорема $\forall$ решётки L размерности n справедливо:

$$\lambda_1(L) \cdot \mu(\hat{L}) \leq n$$

◁ От противного: $\exists L$, т.ч. $\lambda_1(L) \cdot \mu(\hat{L}) > n$.

Мы можем масштабировать L и $\hat{L}$ так чтобы $\lambda_1(L) > \sqrt{n}$ и $\mu(\hat{L}) > \sqrt{n}$.

Рассмотрим $v \in \mathbb{R}^n$, т.ч. $\operatorname{dist}(v, \hat{L}) > \sqrt{n}$

$$\rho(\hat{L} - v) = \rho\left((\hat{L} - v) \setminus B(0, \sqrt{n})\right) \leq 2^{-n} \rho(\hat{L}).$$ - Граница хвоста (см. предыдущую лекцию)

С другой стороны,

$$\rho(\hat{L} - v) \overset{PSF}{=} \det(L) \cdot \sum_{b \in L} \rho(b) \cdot e^{-2\pi i \langle b, v \rangle} = \det(L)\left(1 + \sum_{b \in L \setminus \{0\}} \rho(b) e^{-2\pi i \langle b, v \rangle}\right)$$

$$\geq \det(L)\left(1 - \sum_{b \in L\setminus\{0\}} \rho(b)\right) \quad (*)$$

граница хвоста

$$\sum_{b\in L\setminus\{0\}} \rho(b) = \rho(L\setminus\{0\}) = \rho(L\setminus B(0,\sqrt{n})) \leq 2^{-n}\rho(L) \quad (**)$$

т.к. $\lambda_1(L) > \sqrt{n}$

$(*)$, $(**)$ $\Rightarrow$ $\rho(\hat{L}-v) \geq \det(L)\left(1 - 2^{-n}\rho(L)\right)$

имеем: $\rho(\hat{L}-v) \leq 2^{-n}\rho(\hat{L}) \overset{PSF}{=} 2^{-n}\det(L)\,\rho(L)$

$\rho(\hat{L}-v) \geq \det(L)\left(1-2^{-n}\rho(L)\right)$ $\Rightarrow$

$\det(L)\left(1-2^{-n}\rho(L)\right) \leq 2^{-n}\det(L)\,\rho(L)$

$\Leftrightarrow$

$2^{-n}\rho(L) + 2^{-n}\rho(L) \geq 1$

$2^{-n+1}\rho(L) \geq 1 \Rightarrow \rho(L) \geq 2^{n-1}$

однако, $\rho(L) = \underbrace{\rho(0)}_{=1} + \rho(L\setminus\{0\}) \simeq 1+\varepsilon$, $|\varepsilon| \leq 2^{-n}\rho(L)$

Гауссова ф-ия от "длинных" векторов $\simeq \varepsilon$

$\rho(L) \geq 2^{n-1}$ — ↯ противоречие.

Следствие $\lambda_1(L)\cdot\lambda_n(\hat{L}) \leq 2n$

II Сглаживающий параметр (smoothing parameter)

опр-ие L-решётка, $\varepsilon > 0$. Тогда η_ε – "ε-сглаживающий параметр" – это наименьшее σ, т.ч.

$$\rho_{\frac{1}{\sigma}}(\hat{L}) \leq 1+\varepsilon$$

Интуиция: η_ε - наименьшее среднекв. отклонение σ, необходимое для "сглаживания" дискретной структуры решётки L.

Альтернативное опр-ие η_ε - это $\min \sigma$, т.ч. $\forall$ сдвиг $L+c$ ($c \in \mathbb{R}^n$) имеет одну и ту же Гауссову массу (в точности до ε), т.е. $\rho(L+c) \approx_\varepsilon \rho(L+c') = \rho(L) = \sum_{b \in L} \rho(b)$.

В дальнейшем нам интересно $\varepsilon = 2^{-n}$.

Лемма 1 $\forall L, \forall c, \forall \sigma \geq \eta_\varepsilon(L)$: $\rho_\sigma(L+c) \in [1-\varepsilon, 1+\varepsilon] \cdot \det(\hat{L})$.

$\blacktriangleleft$ $\rho_\sigma(L+c) \overset{PSF}{=} \det(\hat{L}) \sum_{\hat{b} \in \hat{L}} \rho_{\frac{1}{\sigma}}(\hat{b}) e^{-2\pi i \langle \hat{b}, c \rangle} = \det(\hat{L}) \left(\underbrace{1 + \sum_{\hat{b} \in \hat{L} \setminus \{0\}} \rho_{\frac{1}{\sigma}}(\hat{b}) e^{-2\pi i \langle \hat{b}, c \rangle}}_{>0} \right)$

$= \det(\hat{L}) \left| 1 + \sum_{\hat{b} \in \hat{L} \setminus \{0\}} \rho_{\frac{1}{\sigma}}(\hat{b}) e^{-2\pi i \langle \hat{b}, c \rangle} \right| \Rightarrow$

$\Rightarrow |\rho_\sigma(L+c) - \det(\hat{L})| \leq \det(\hat{L}) \underbrace{\sum_{\hat{b} \in \hat{L} \setminus \{0\}} \rho_{\frac{1}{\sigma}}(\hat{b})}_{\rho_{\frac{1}{\sigma}}(\hat{L} \setminus \{0\}) \leq \varepsilon \text{ (по опред-ию)}} \leq \det(\hat{L}) \cdot \varepsilon.$

$\Rightarrow (1-\varepsilon)\det(\hat{L}) \leq \rho_\sigma(L+c) \leq (1+\varepsilon)\det(\hat{L})$. ▶

Лемма 2 $\eta_{2^{-n}}(L) \leq \frac{\sqrt{n}}{\lambda_1(\hat{L})}$, L - решётка, $L \subseteq \mathbb{R}^n$.

$\blacktriangleleft$ $\forall \sigma > \frac{\sqrt{n}}{\lambda_1(\hat{L})}$. Покажем, $\rho_{\frac{1}{\sigma}}(\hat{L}) \leq 1 + 2^{-n}$, т.е. $\rho_{\frac{1}{\sigma}}(\hat{L} \setminus \{0\}) \leq 2^{-n}$

$\Downarrow$

$\sigma \cdot \lambda_1(\hat{L}) > \sqrt{n}$. $\quad \lambda_1(\sigma \hat{L}) = \sigma \cdot \lambda_1(\hat{L}) > \sqrt{n}$

1. $\rho_{\frac{1}{\sigma}}(\hat{L} \setminus \{0\}) = \rho_1(\sigma \cdot \hat{L} \setminus \{0\}) = \rho_1(\sigma \hat{L} \setminus B(0, \sqrt{n}))$.

для $x \in \hat{L}$: $e^{-\pi \|x\|^2 \cdot \sigma^2} = e^{-\pi \|\sigma x\|^2}$

2. Граница хвоста: $\rho_1(\sigma \hat{L} \setminus B(0, \sqrt{n})) \leq c^n \rho(\sigma \hat{L})$, $c \ll 1$.

3. $\rho(\sigma \hat{L}) = \rho(\sigma \hat{L} \setminus B(0, \sqrt{n})) + \underbrace{\rho(\sigma \hat{L} \cap B(0, \sqrt{n}))}_{\neq 0 \Rightarrow = 1} = \rho(\sigma \hat{L} \setminus B(0, \sqrt{n})) + 1$

$$\leq c^n \rho(\sigma L) + 1$$

$$\rho(\sigma L) \leq c^2 \rho(\sigma \hat{L}) + 1 \Rightarrow \rho(\sigma L) \leq \frac{1}{1-c^n}$$

$$\Rightarrow \rho_{\frac{1}{\sigma}}(\hat{L} \setminus \{0\}) \leq c^n \rho(\sigma L) \leq \frac{e^n}{1-c^n} \leq 2^{-n} \text{ для } c = \sqrt{\frac{2\pi}{e^{2\pi}-1}}$$

Лемма 3 $\exists B = QR$ - базис L. Тогда

$$\lambda_{2^n}(L) \leq \sqrt{n} \cdot \max_i r_{ii} \leq \sqrt{n} \max_i \|b_i\|$$

▲ Из леммы 2 достаточно показать, что $\frac{1}{\lambda_1(\hat{L})} \leq \max_i r_{ii}$.

В упражнениях про QR факторизацию было доказано, что

$$\lambda_1(\hat{L}) \geq \min_i \hat{r}_{ii} = \min_i \frac{1}{r_{n-i+1,n-i+1}} \geq \frac{1}{\max_i r_{n-i+1,n+i+1}} \geq \frac{1}{\max_i r_{ii}}$$