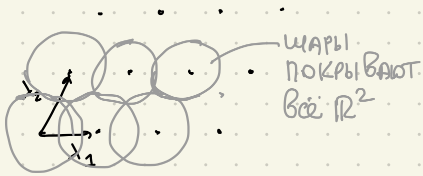
Лекция №10.
Сглаживающий параметр

I Transference Theorem
(связь решётки и её дуальной)

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



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 $\mu_n(L) \geq \frac{\lambda_n}{2}$.

Thm ∀ решётки L размерности n, справедливо:

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

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

Мы можем масштабировать L и $\hat{L}$, т.ч. $\lambda_1(L) > \sqrt{n}$, и $\mu(\hat{L}) > \sqrt{n}$.

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

$$\rho(\hat{L} - v) = \rho\big((\hat{L}-v)\setminus B(0,\sqrt{n})\big) \leq 2^{-n}\rho(\hat{L})$$ – Гауссов хвост (см. Лемма 4 предыдущей лекции)

С другой стороны,

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

$$= \det(L)\Big(1 + \sum_{b\in L\setminus\{0\}} \rho(b)\cdot e^{2\pi i\langle b,v\rangle}\Big) \geq \det(L)\Big(1 - \sum_{b\in L\setminus\{0\}} \rho(b)\Big) \quad (*)$$

$$\rho(L\setminus\{0\}) \underset{\lambda_1(L)>\sqrt{n}}{=} \rho\big(L\setminus B(0,\sqrt{n})\big) \underset{\text{(Г. хвост)}}{\leq} 2^{-n}\rho(L) \quad (**)$$

$$\left.\begin{matrix}(*)\\(**)\end{matrix}\right\}\quad \rho(\hat{L}-v) \geq \det(L)\left(1-2^{-n}\rho(L)\right)$$

Имеем:
$$\left.\begin{aligned}\rho(\hat{L}-v) &\leq 2^{-n}\rho(\hat{L}) \overset{PSF}{=} 2^{-n}\det(L)\cdot\rho(L)\\ \rho(\hat{L}-v) &\geq \det(L)\left(1-2^{-n}\rho(L)\right)\end{aligned}\right\} \Rightarrow$$

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

$$\Leftrightarrow$$

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

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

однако, $\rho(L) = \overset{1}{\overset{\shortparallel}{\rho(0)}} + \overset{\varepsilon}{\overset{\shortparallel}{\rho(L\setminus\{0\})}} \approx 1$, $|\varepsilon| \leq 2^{-n}\rho(L)$

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

↯ Противоречие

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

II Сглаживающий параметр (smoothing parameter)

Опр-ие: $\exists L$-решётка, $\varepsilon > 0$. Тогда η_ε – "ε"-сглаживающий пар-р – это наименьшее $\sigma > 0$, т.ч.

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

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

Альтернативное опр-ие: η_ε – это min. σ, т.ч. $\forall$ сдвиг $L+c$ имеет одну и ту же Гаусову массу (с точностью до ε) $\left(\rho_\sigma(L+c) = \sum_{b\in L+c}\rho_\sigma(b)\right)$

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

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

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

$$|\rho_\sigma(L+c) - \det(\hat{L})| \leq \det(\hat{L}) \cdot \underbrace{\sum_{\hat{b}\in\hat{L}\setminus\{0\}} \rho_{1/\sigma}(\hat{b})}_{\rho_{\frac{1}{\sigma}}(\hat{L}\setminus\{0\})\ \leq\ \varepsilon} \leq \det(\hat{L})\cdot\varepsilon$$

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

▶

Лемма 2
$$\eta_{2^{-n}}(L) \leq \frac{\sqrt{n}}{\lambda_1(\hat{L})}$$

$\triangle$ Рассм. $\sigma > \dfrac{\sqrt{n}}{\lambda_1(\hat{L})}$. Покажем, $\rho_{\frac{1}{\sigma}}(\hat{L}) \leq 1 + 2^{-n}$, т.е.

$\Downarrow$ $\qquad \rho_{\frac{1}{\sigma}}(\hat{L}\setminus\{0\}) \leq 2^{-n}$.

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

1. $$\underbrace{\rho_{\frac{1}{\sigma}}(\hat{L}\setminus\{0\})}_{\Downarrow} = \rho_1(\sigma\hat{L}\setminus\{0\}) \overset{\text{т.к. } \sigma\cdot\lambda_1(\hat{L}) > \sqrt{n}}{=} \rho_1(\sigma\hat{L}\setminus B(0,\sqrt{n})).$$

для $x\in\hat{L}\setminus\{0\}$: $e^{-\pi\|x\|^2\sigma^2} = e^{-\pi\|\sigma\cdot x\|}$

2. Гауссов хвост: $\rho(\sigma\hat{L}\setminus B(0,\sqrt{n})) \leq c^n \rho(\sigma\hat{L})$, $c<1$.

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

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

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

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

▶

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

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

$\triangleleft$ Из Леммы 2 достаточно показать, что $\frac{1}{\lambda_1(\mathcal{L})} \le \max_i r_{ii}$.

В упр-ниях по QR факторизации док-но, что

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

$\blacktriangleright$