Сглаживающий параметр

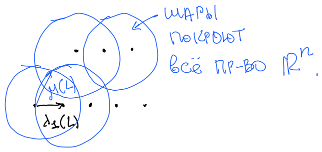
Monday 5 April 2021 08:47

I Transference theorem
(связь решётки с её дуальной)

Для $\forall$ решётки L размерности n:

$$\lambda_1(L)\cdot\mu(\hat{L}) \le n, \text{ где}$$

$$\mu(\hat{L}) = \max_{\hat{c}\in\mathbb{R}^n} \operatorname{dist}(\hat{c},\hat{L}) = \max_{\hat{c}\in\mathbb{R}^n}\min_{\hat{b}\in\hat{L}} \|\hat{b}-\hat{c}\| \text{ — покрывающий радиус}$$



(пример: $\mu(\mathbb{Z}^n) = \frac{\sqrt{n}}{2}$ и определён точкой $\hat{c} = (\frac12,\frac12,\dots,\frac12)$; можно показать, что $\mu_n(L) \ge \frac12\lambda_n(L)$)

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

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

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

$$\rho(\hat{L}-v) = \rho((\hat{L}-v)\setminus B(0,\sqrt{n})) \le 2^{-n}\rho(\hat{L}) \quad (\text{Гауссов хвост}).$$

С другой стороны,

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

$$\left.\begin{array}{l} \ge \det(L)\Big(1-\sum_{b\in L\setminus\{0\}}\rho(b)\Big). \\ \underbrace{\rho(L\setminus\{0\}) = \rho(L\setminus B(\sqrt{n}))}_{\lambda_1(L)>\sqrt{n}} \underset{(\text{т. хвост})}{\le} 2^{-n}\cdot\rho(L) \end{array}\right\} \Rightarrow \rho(\hat{L}-v) \ge \det(L)(1-\rho(L)e^{-n}).$$

Имеем,

$$\left.\begin{array}{l} \rho(\hat{L}-v) \le 2^{-n}\rho(\hat{L}) \overset{PSF}{=} 2^{-n}\det(L)\rho(L) \\ \rho(\hat{L}-v) \ge \det(L)(1-\rho(L)\cdot 2^{-n}) \end{array}\right\} \Rightarrow 2^{-n}\rho(L) \ge 1-2^{-n}\rho(L) \Leftrightarrow 2^{-n+1}\rho(L) \ge 1.$$

Однако, $\rho(L) = \overset{\rho(0)}{1} + \overset{\rho(L\setminus\{0\})}{\varepsilon}$ ≈ 1, $\quad \underline{|\varepsilon| \le 2^{-n}\rho(L)}$

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

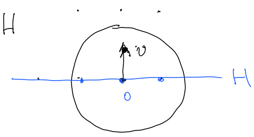
Следствие $\lambda_1(L)\cdot\lambda_n(\hat{L}) \le 2\cdot n$.

◁ Согласно Transf. thm. достаточно показать, что $\lambda_n(\hat{L}) \le 2\mu(\hat{L})$.

$\forall$ открытый шар $B^{open}(0,\lambda_n(\hat{L}))$.

$\exists H$ - подпр-во р-ти $\underline{\le n-1}$ т.ч. $B^{open}(0,\lambda_n(\hat{L}))\cap\hat{L} \subseteq H$

(т.к. мы не достигнем λ_n)



$\forall$ v - ортогонально H т.ч. $\|v\| = \frac{\lambda_n(\hat{L})}{2}$

Утверждение: $\underline{\operatorname{dist}(v,\hat{L}) \ge \lambda_n(\hat{L})/2}$

- Если $\hat{b}\in\hat{L}\cap H \Rightarrow \|v-\hat{b}\| \ge \|v\| = \lambda_n(\hat{L})/2$
- Если $\hat{b}\in\hat{L}/H \Rightarrow \|\hat{b}\| \ge \lambda_1(\hat{L})$ и $\|v-\hat{b}\| \ge \|\|v\|-\|\hat{b}\|\| \ge \lambda_n(\hat{L})/2$.

отсюда $\mu(\hat{L}) \ge \frac{\lambda_n(\hat{L})}{2}$ ▶

II Сглаживающий параметр (smoothing parameter)

Опр-ие $\rceil$ L - решётка, $\varepsilon>0$. ε - сглаживающий пар-р L $\overset{\eta_\varepsilon}{V}$ - это наименьшее $\delta>0$, т.ч.

$$\rho_{\frac{1}{\delta}}(\hat{L}) \le 1+\varepsilon$$

Интуиция: η_ε - min. среднекв. отклонение δ, необходимое для "сглаживания" дискретной структуры L.

Альтернативное опр-ие: η_ε - min. δ, т.ч. любой сдвиг $L+c$ имеет одну и ту же гауссову массу (в точности до ε):
$\rho_\delta(L+c) := \sum_{x\in L+c}\rho_\delta(x+c)$.

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

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

◀ $$\rho_\sigma(L+c) \overset{PSF}{=} \underbrace{\det(\hat{L}) \Big| \sum_{\hat{b}\in\hat{L}} \rho_{\frac{1}{\sigma}}(\hat{b})\, e^{-2\pi i \langle c,\hat{b}\rangle} \Big|}_{\text{т.к. с обеих сторон "=" стоят положительные зн-ия}} = \det(\hat{L}) \Big| \Big(1 + \sum_{\hat{b}\in\hat{L}\setminus\{0\}} \rho_{1/\sigma}(\hat{b})\, e^{-2\pi i \langle c,\hat{b}\rangle}\Big) \Big|$$

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

$$\Downarrow$$

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

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

◀ $*$ $\sigma > \dfrac{\sqrt{n}}{\lambda_1(\hat{L})}$. Покажем, что $\rho_{1/\sigma}(L\setminus\{0\}) \leq 2^{-n}$.

1. $\rho_{\frac{1}{\sigma}}(\hat{L}\setminus\{0\}) = \rho_1(\sigma\hat{L}\setminus\{0\}) \overset{\text{т.к. } \sigma\cdot\lambda_1(\hat{L})>\sqrt{n}}{=} \rho(\sigma\hat{L}\setminus B(\sqrt{n}))$.
   $\rho_{\frac{1}{\sigma}} = e^{-\pi\|x\|^2\sigma^2} = e^{-\pi(\|\sigma x\|^2)}$

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

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

   ($\sigma\hat{L}\cap B(\sqrt{n}) = 0$)

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

В итоге получаем $\rho_{\frac{1}{\sigma}}(\hat{L}\setminus\{0\}) \leq c^n \cdot \dfrac{1}{1-c^n} \leq 2^{-n}$ для $c = \sqrt{\dfrac{2\pi}{e^{2\pi-1}}}$ ▷.

Лемма 3. Пусть $B=QR$ — базис L. Тогда
$$\eta_{2^{-n}}(L) \leq \sqrt{n}\cdot\max_i(r_{ii}) \leq \sqrt{n}\cdot\max_i\|b_i\|$$

◀ Из Леммы 2 достаточно показать, что $\dfrac{1}{\lambda_1(\hat{L})} \leq \max_i r_{ii}$.

Известно (см. лекцию по QR-факторизации), что
$$\lambda_1(\hat{L}) \geq \min_i \hat{r}_{ii} = \min \frac{1}{r_{n-i+1,n-i+1}} \geq \frac{1}{\max_i r_{ii}}$$ ▶

III Гауссова выборка на решётке (Gentry–Peikert–Vaikuntanathan'08).

Опр. Пусть D_1, D_2 — два распределения, заданные над счётным мн-вом Ω.
Статистическая разность м/у D_1, D_2:
$$\Delta(D_1,D_2) = \frac{1}{2}\sum_{x\in\Omega}|D_1(x)-D_2(x)| = \frac{1}{2}\sum_{x\in\Omega}\Big|\Pr_{y\leftarrow D_1}[y=x] - \Pr_{y\leftarrow D_2}[y=x]\Big| = \frac{1}{2}\|D_1-D_2\|.$$

Будем обозначать $\Delta(X_1,X_2)$ для X_1,X_2 — случ. значений

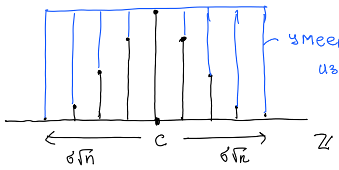
Лемма (св-ва стат. разности)

1. Если Y независимо от X_1, X_2, то $\Delta((X_1,Y),(X_2,Y)) = \Delta(X_1,X_2)$
2. $\Delta((X_i)_i, (Y_i)_i) \leq \sum_i \Delta(X_i,Y_i)$
3. Для ф-ии f (быть может, рандомизированной): $\Delta(f(X_1), f(X_2)) \leq \Delta(X_1,X_2)$.

В частности, f может быть $\forall$ алгоритмом. Если f возвращает бит, то
$$|\Pr[f(X_1)=1] - \Pr[f(X_2)=1]| \leq \Delta(X_1,X_2).$$

III.1 Гауссова выборка над $\mathbb{Z}$

$$D_{\mathbb{Z},\sigma,c}(x) \sim \rho_\sigma(x-c) = e^{-\pi\frac{\|x-c\|^2}{\sigma^2}}$$



умеем эффективно выбирать из случ. равновероятного р-ия.

Алгоритм 1 (выборка $D_{\mathbb{Z},\sigma,c}$)

1. Выбрать $x \leftarrow U(\mathbb{Z}\cap[c-\sigma\sqrt{n},\, c+\sigma\sqrt{n}])$
2. Выдать x с вероятностью $\rho_{\sigma,c}(x)$
   иначе restart.

Сложность алг-ма 1. (кол-во restart'ов): $\Pr\limits_{x\leftarrow U(\mathbb{Z}\cap[c-\sigma\sqrt{n},\, c+\sigma\sqrt{n}])}[x\in[c-\sigma, c+\sigma]] \geq \frac{2\sigma-1}{2\sigma\sqrt{n}-1} = \Omega\left(\frac{1}{\sqrt{n}}\right)$ для $\sigma\geq 1$.

Такой x, (т.е. $x\in[c-\sigma, c+\sigma]$) имеет массу $\rho_{\sigma,c}(x) \geq e^{\frac{-\pi\|x\|^2}{\sigma^2}} \geq e^{-\pi\cdot 1} = \Omega(1)$

$\Rightarrow \mathbb{E}[\#\ \text{restart}] \sim \sqrt{n}$.

Качество выборки:
(стат. разность от $D_{\mathbb{Z},\sigma,c}$)

Алгоритм выводит x с в-тью $\begin{cases} \Pr[x] \sim \rho_{\sigma,c}(x) & \text{для } |x-c| \leq \sigma\sqrt{n} \\ 0, & |x-c| > \sigma\sqrt{n} \end{cases}$

Гауссов хвост: $\rho_{\sigma,c}(\mathbb{Z}\setminus B(\sigma\sqrt{n})) \leq 2^{-n}\rho_{\sigma,c}(\mathbb{Z})$

Сглажив. пар-р: Если $\sigma \geq \eta_{2^{-n}}(\mathbb{Z})$, то $\rho_{\sigma,c}(\mathbb{Z}) \in [1-2^{-n}, 1+2^{-n}]$ $\forall c$

$\Rightarrow \rho_{\sigma,c}(\mathbb{Z}\setminus B(\sigma\sqrt{n})) \leq 2^{-n+2}\rho_{\sigma,c}(\mathbb{Z})$

$$\Delta(\text{сампл Алг-ма } 1, D_{\mathbb{Z},\sigma,c}) = \frac{1}{2}\sum_{\substack{x\in\mathbb{Z}\\ |x-c|\leq\sigma\sqrt{n}}} \left|\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\mathbb{Z}\cap B(\sigma\sqrt{n}))} - \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\mathbb{Z})}\right| + \frac{1}{2}\sum_{\substack{x\in\mathbb{Z}\\ |x-c|>\sigma\sqrt{n}}} \left|0 - \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\mathbb{Z})}\right| =$$

$$= \frac{1}{2}\sum_{\substack{x\in\mathbb{Z}\\ |x-c|\leq\sigma\sqrt{n}}} \rho_{\sigma,c}(x)\left|\frac{1}{\rho_{\sigma,c}(\mathbb{Z}\cap B(\sigma\sqrt{n}))} - \frac{1}{\rho_{\sigma,c}(\mathbb{Z})}\right| + \frac{1}{2}\frac{\overbrace{\rho_{\sigma,c}(\mathbb{Z}\setminus B(\sigma\sqrt{n}))}^{\leq 2^{-n+2}}}{\rho_{\sigma,c}(\mathbb{Z})} =$$

$$= \frac{1}{2}\rho_{\sigma,c}(\mathbb{Z}\cap B(\sigma\sqrt{n}))\left|\frac{1}{\rho_{\sigma,c}(\mathbb{Z}\cap B(\sigma\sqrt{n}))} - \frac{1}{\rho_{\sigma,c}(\mathbb{Z})}\right| + \text{ --- // --- } =$$

$$\leq \frac{1}{2}\left|1 - \frac{\rho_{\sigma,c}(\mathbb{Z}) - \rho_{\sigma,c}(\mathbb{Z}\setminus B(\sigma\sqrt{n}))}{\rho_{\sigma,c}(\mathbb{Z})}\right| + \frac{1}{2}\cdot 2^{-n+2} \leq$$

$$\leq \frac{1}{2}\underbrace{\frac{\rho_{\sigma,c}(\mathbb{Z}\setminus B(\sigma\sqrt{n}))}{\rho_{\sigma,c}(\mathbb{Z})}}_{\leq 2^{-n+2}} + \frac{1}{2}\cdot 2^{-n+2} \leq 2^{-n+2}$$

D.

Вывод: Для $\sigma \geq \sqrt{n}$ Алг-м 1. вернёт x за ожидаемое полиномиальное время; при этом статист. разность м/у р-ием x и $D_{\mathbb{Z},\sigma,c}$ не более 2^{-n+2}.