Гауссово распределение на решётке

Sunday 28 March 2021 19:17

I Анализ Фурье

Опр.1 $\exists\, f: \mathbb{R}^n \to \mathbb{C}$, т.ч. $\int |f| < \infty$.

Преобразование Фурье ф-ии f : $\hat{f}: \mathbb{R}^n \to \mathbb{C}$

$$y \mapsto \int\limits_{x \in \mathbb{R}^n} f(x)\, e^{-2\pi i \langle x, y\rangle}\, dx$$

Лемма 1. (св-ва пр-ия Фурье):

1. Если $h(x) = f(T\cdot x)$ для $T \in \mathbb{R}^{n\times n}$ — несингулярной, то
$$\hat{h}(y) = (\det T)^{-1} \cdot \hat{f}(T^{-t}\cdot y)$$

2. Если $h(x) = f(x+v)$ $\forall v \in \mathbb{R}^n$, то
$$\hat{h}(y) = \hat{f}(y)\cdot e^{2\pi i \langle v, y\rangle}$$

3. Если $h(x) = f(x)\cdot e^{2\pi i \langle x, v\rangle}$, то
$$\hat{h}(y) = \hat{f}(y - v)$$

4. Определим $(f * g)(z) := \int\limits_{x \in \mathbb{R}^n} f(x) g(z-x)\, dx$. Тогда
$$\widehat{f * g} = \hat{f}\cdot\hat{g}.$$

$\triangleleft$ 1. $\hat{h}(y) = \int\limits_{x\in\mathbb{R}^n} f(T\cdot x)\, e^{-2\pi i\langle x, y\rangle}\, dx = \left\{ \begin{array}{l} \langle x, y\rangle = x^t\cdot y = x^t\cdot T^t\cdot (T^t)^{-1}\cdot y = \\ = (T\cdot x)^t\cdot (T^{-t} y) = \langle T\cdot x, T^{-t} y\rangle \end{array} \right\} =$

$= \int\limits_{x\in\mathbb{R}^n} f(T\cdot x)\, e^{-2\pi i \langle Tx, T^{-t} y\rangle}\, dx = \left\{ \begin{array}{l} x' = Tx \\ dx' = \det T\, dx \end{array} \right\} = \frac{1}{\det T} \int\limits_{x'\in\mathbb{R}^n} f(x')\, e^{-2\pi i\langle x', T^{-t} y\rangle}\, dx' =$

$= \frac{1}{\det T}\cdot \hat{f}(T^{-t}\cdot y)$.

2.-3. См. упражнения.

4. $\widehat{f*g}(y) = \int\limits_{z\in\mathbb{R}^n} (f*g)(z)\, e^{-2\pi i\langle z, y\rangle}\, dz = \int\limits_{\substack{z\in\mathbb{R}^n \\ x\in\mathbb{R}^n}} f(x) g(z-x)\, e^{-2\pi i\langle z, y\rangle}\, dx\, dz \overset{z' = z-x,\ dz' = dz}{=}$

$= \int\limits_{\substack{z'\in\mathbb{R}^n \\ x\in\mathbb{R}^n}} f(x) g(z') \underbrace{e^{-2\pi i\langle y, z'+x\rangle}}_{= e^{-2\pi i\langle y, z'\rangle}\cdot e^{-2\pi i\langle y, x\rangle}}\, dz'\, dx = \underbrace{\int\limits_{z'\in\mathbb{R}^n} g(z')\, e^{-2\pi i\langle y, z'\rangle}\, dz'}_{\hat{g}(y)} \cdot \underbrace{\int\limits_{x\in\mathbb{R}^n} f(x)\cdot e^{-2\pi i\langle y, x\rangle}\, dx}_{\hat{f}(y)}$. $\triangleright$

Лемма 2. (св-ва #2)

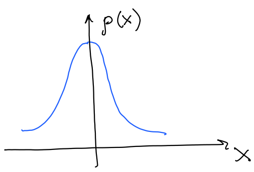
1. $\hat{\hat{f}}(x) = f(-x)$

$\hat{\hat{\hat{\hat{f}}}}(x) = f(x)$

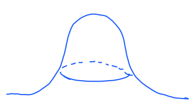
2. $p(x) = e^{-\pi\cdot\|x\|^2}$. Тогда $\hat{p} = p$.

(иначе, Гауссовы фун p — айген фун преобр-ия Фурье).

в $\mathbb{R}^1$:



в $\mathbb{R}^2$:



$\triangleleft$ 2. $\hat{p}(y) = \int\limits_x p(x)\, e^{-2\pi i\langle x, y\rangle}\, dx = \int\limits_x e^{-\pi\|x\|^2 - 2\pi i\langle x, y\rangle}\, dx =$

$= \int\limits_x e^{-\pi\|x\|^2 - 2\pi i\langle x, y\rangle + i^2\pi\|y\|^2 + \pi\|y\|^2}\, dx =$

$= \int e^{-\pi(\|x\|^2 + 2i\langle x, y\rangle - i^2\|y\|^2) + i^2\pi\|y\|^2}\, dx =$

$= e^{-\pi\|y\|^2} \underbrace{\int e^{-\pi(\|x\| + i\|y\|)^2}\, dx}_{= \frac{\sqrt{\pi}}{\sqrt{\pi}} = 1} = e^{-\pi\|y\|^2}$ $\triangleright$

Теорема (ф-ла сложения Пуассона / PSF).

Для $\forall$ "достаточно хорошей" ф-ции f (т.е. такой, что $\int_0^1 f\,dx$ существует), верно
$$\sum_{k\in\mathbb{Z}^n} f(k) = \sum_{k\in\mathbb{Z}^n} \hat{f}(k) \quad (\text{или } f(\mathbb{Z}^n) = \hat{f}(\mathbb{Z}^n))$$

$\triangleleft$ Обозначим $\varphi(x) := f(x+\mathbb{Z}^n)$, $x\in\mathbb{R}^n$

$= \sum_{k\in\mathbb{Z}^n} f(x+k)$ — ф-ция с периодом 1 (если x - любое целое, значения $\varphi(x)$ совпадают)

$\Rightarrow$ можем рассматривать $\varphi(x)$ для $x\in[0,1)^n$

Ряд Фурье для $\mathbb{Z}^n$-периодичной ф-ции $\varphi(x)$ есть $\hat{\varphi}(z): \mathbb{Z}^n \to \mathbb{C}$
$$z \mapsto \int_{x\in[0,1)^n} \varphi(x)\, e^{-2\pi i\langle x, z\rangle}dx$$

и справедливо $\varphi(x) = \sum_{z\in\mathbb{Z}^n} \hat{\varphi}(z)\cdot e^{-2\pi i\langle x,z\rangle}$.

$$f(\mathbb{Z}^n) = \varphi(0) = \sum_{z\in\mathbb{Z}^n} \hat{\varphi}(z)\, \underbrace{e^{-2\pi i\, 0\cdot z}}_{=1} = \hat{\varphi}(\mathbb{Z}^n)$$

$$\hat{\varphi}(z) = \int_{x\in[0,1)^n} \varphi(x)\, e^{-2\pi i\langle x,z\rangle}dx = \int_{x\in[0,1)^n} \Big(\sum_{k\in\mathbb{Z}^n} f(x+k)\Big) e^{-2\pi i\langle x,z\rangle}dx \overset{e^{-2\pi i \underbrace{\langle x,k\rangle}_{\in\mathbb{Z}}} = 1}{=}$$

$$= \underbrace{\int_{x\in[0,1)^n}\sum_{k\in\mathbb{Z}^n}}_{x'\in\mathbb{R}^n} f(x+k)\, e^{-2\pi i\langle x+k, z\rangle}dx = \int_{\substack{x'\in\mathbb{R}^n\\ x' = x+k}} f(x')\, e^{-2\pi i\langle x', z\rangle}dx = \hat{f}(z)$$

$$\Rightarrow f(\mathbb{Z}^n) = \hat{\varphi}(\mathbb{Z}^n) = \hat{f}(\mathbb{Z}^n).$$ $\triangleright$

Следствие. $\forall$ решётки L и "хорошей" f:
$$f(L) = \det(\hat{L})\cdot \hat{f}(\hat{L})$$
$$\Big(\sum_{x\in L} f(x) = \det(\hat{L})\cdot \sum_{\hat{x}\in\hat{L}} \hat{f}(\hat{x})\Big)$$

В общем, $\forall u\in\mathbb{R}^n$ $\quad f(L+u) = \det(\hat{L}) \sum_{\hat{x}\in\hat{L}} \hat{f}(\hat{x})\, e^{2\pi i\langle x, u\rangle}$.

Док-во в упражнениях

II Гауссово распределение на решётке

$p(x) = e^{-\pi\|x\|^2}$ даёт вероятностное распределение на $\mathbb{R}^n$ $\quad(\int p(x) = 1)$

Цель: $p(x)$, $x\in\mathbb{R}^n$ $\longrightarrow$ $D(b)$, $b\in L$
$\qquad\qquad\qquad\qquad\approx e^{-\pi\|b\|^2}$

Кандидат: $D(b) = \dfrac{e^{-\pi\cdot\|x\|^2}}{p(L)}$. Покажем, что $p(L)$ конечно.

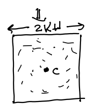
Лемма $\forall$ решётки L р-ти n, $p(L) = \sum_{b\in L} e^{-\pi\cdot\|b\|^2} < +\infty$.

Более того, $\forall c\in\mathbb{R}^n$: $p(L-c) < +\infty$

$\triangleleft$ Покажем для $L = \mathbb{Z}^n$ (для $\forall$ другой решётки, $\nexists$ коэфф. векторов относ. $\forall$ базиса, делаем замену переменных).

$$\sum_{b\in\mathbb{Z}^n} e^{-\pi\|b-c\|^2} = \sum_{k\in\mathbb{Z}_+}\ \sum_{\substack{b\in\mathbb{Z}^n:\\ k-1\le\|b-c\|<k}} e^{-\pi\|b-c\|^2} \le \sum_{k\in\mathbb{Z}_+}\ \sum_{\substack{b\in\mathbb{Z}^n:\\ \underbrace{k-1\le\|b-c\|<k}}} e^{-\pi(k-1)^2} \le \sum_{k\in\mathbb{Z}_+} (2k+1)^n e^{-\pi(k-1)^2}$$

$k-1\le\|b-c\|<k \Rightarrow$
$\Rightarrow \|b-c\|_\infty < k \Rightarrow$



$$\le 1 + \sum_{k\in\mathbb{Z}_{\ge 0}} \underbrace{(10k)^n\cdot e^{-k}}_{\text{exp. "убывает быстрее } k^n\text{"}} < +\infty.$$ $\triangleright$

Опр-ие. Гауссово распределение на решётке L с пар-ми $c \in \mathbb{R}^n$ и $s>0$ задаётся

$$D_{L,s,c}(b) = \frac{\rho_{s,c}(b)}{\rho_{s,c}(L)} = \frac{e^{-\frac{\pi\|b-c\|^2}{s^2}}}{\sum\limits_{v\in L} e^{-\frac{\pi\|v-c\|^2}{s^2}}}.$$

s — среднекв. отклонение, c — сдвиг

Лемма (св-ва $D_{L,s,c}$)

1. $\forall L,\ \forall s\geq 1:\ \rho(L/s) \leq s^n \rho(L);$
2. $\forall L,\ \forall c\in\mathbb{R}^n:\ \rho(L+c) \leq \rho(L)$

} 3. $\rho_s(L+u) \leq s^n \rho(L)$.

4. "Tail bound" "Гауссов хвост" $\forall L,\ \forall c\in\mathbb{R}^n,\ \forall d>0:$
$$\frac{\rho\left((L+c)\setminus \mathcal{B}\left(d\cdot\sqrt{\frac{n}{2\pi}}\right)\right)}{\rho(L)} \leq \left(\frac{d^2}{e^{d^2-1}}\right)^{\frac{n}{2}}$$

Для $c=0$, $s=1$ это св-во переписывается $\Pr\left[b\leftarrow D_{L,1,0},\ \|b\|> d\sqrt{\frac{n}{2\pi}}\right] \leq \left(\frac{d^2}{e^{d^2-1}}\right)^{\frac{n}{2}}.$

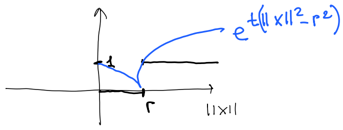
◁ 1. $\rho(L/s) \overset{PSF}{=} \det\left(\widehat{(L/s)}\right)\cdot\hat\rho\left(\widehat{L/s}\right) \underset{\widehat{L/s}=s\cdot\hat L}{=} \det(s\cdot\hat L)\,\rho(s\hat L) = s^n\cdot\det(\hat L)\,\rho(s\cdot\hat L) \underset{\rho(1\cdot L)\leq\rho(s\cdot L)}{\leq} s^n\,\underbrace{\det(\hat L)\,\rho(\hat L)}\overset{PSF}{=} s^n\cdot\rho(L).$

2. $\rho(L+c) \overset{PSF}{=} \underbrace{\det(\hat L)\sum_{\hat b\in\hat L}\rho(\hat b)\,e^{2\pi i\langle \hat b,c\rangle}}_{\in\mathbb{R}_+} = \det(\hat L)\left|\sum_{\hat b\in L}\rho(\hat b)\,e^{2\pi i\langle\hat b,c\rangle}\right| \underset{\text{н-во }\Delta\text{-ка}}{\overset{s\geq 1}{\leq}} \det(\hat L)\sum_{\hat b\in L}\rho(\hat b)\overset{PSF}{=}\rho(L).$

4. Положим $I_r(x)$ - индикатор $B_n(r)$ $\left(I_r(x) = \begin{cases}1, & x\in B_n(r)\\ 0, & \text{иначе}\end{cases}\right)$

Возьмём $r = d\sqrt{\frac{n}{2\pi}}$

$$\rho(\Lambda+c\setminus\mathcal{B}(r)) = \sum_{x\in\Lambda+c}\rho(x)\,\underbrace{[1-I_r(x)]} \overset{\forall t\in(0,\pi)}{\leq} \sum_{x\in\Lambda+c}\rho(x)\,\frac{e^{t\|x\|^2}}{e^{tr^2}} = e^{-tr^2}\sum_{x\in\Lambda+c} e^{-\pi\|x\|^2+t\|x\|^2}$$



$$= e^{-tr^2}\sum_{x\in\Lambda+c}\underbrace{e^{\|x\|^2\left(-\pi\left(\sqrt{1-\frac{t}{\pi}}\right)^2\right)}}_{\rho_{\frac{1}{\sqrt{1-\frac{t}{\pi}}}}(x)} = e^{-tr^2}\rho_{\frac{1}{\sqrt{1-\frac{t}{\pi}}}}(\Lambda+c) \underset{\text{св-во }2^\circ}{\leq} e^{-tr^2}\rho_{\frac{1}{\sqrt{1-\frac{t}{\pi}}}}(\Lambda).$$

Для $t = \pi - \frac{n}{2r^2}$ получаем утверждение леммы. ▷

Численно: для $d = 1.83 < \sqrt{2\pi}$, правая сторона н-ва $< 2^{-n}$.

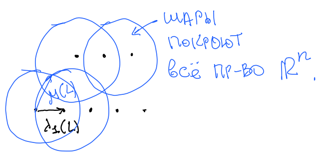
III Transference theorem

(связь решётки с её дуальной)

Для $\forall$ решётки L размерности n:

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

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



◁ 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

$\rho(\hat L-v) = \rho\left((\hat L-v)\setminus\mathcal{B}(0,\sqrt n)\right)\leq 2^{-n}\rho(\hat L)$ (Гауссов хвост).

С другой стороны,

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

$$\left.\begin{aligned}&\geq\det(L)\left(1-\sum_{b\in L\setminus\{0\}}\rho(b)\right),\\ &\underset{\lambda_1(L)>\sqrt n}{\rho(L\setminus\{0\})} = \rho(L\setminus\mathcal{B}(\sqrt n))\underset{(\text{т. хвост})}{\leq} 2^{-n}\cdot\rho(\Lambda)\end{aligned}\right\}\Rightarrow\rho(\hat L-v)\geq\det(L)\left(1-\rho(L)2^{-n}\right).$$

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

$\Leftrightarrow$

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

Однако, $\rho(L) = \overset{\rho(0)}{1} + \overset{\rho(L \setminus \{0\})}{\varepsilon} \approx 1$, $|\varepsilon| \leq 2^{-n} \rho(L)$ $\Big\downarrow$ Противоречие.

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

$\blacktriangleright$

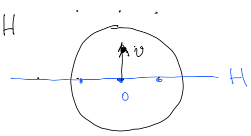
<u>Следствие</u> $\lambda_1(L) \cdot \lambda_n(\hat{L}) \leq 2 \cdot n$.

$\triangleleft$ Согласно Transf. thm. достаточно показать, что $\lambda_n(\hat{L}) \leq 2 \cdot \mu(\hat{L})$.

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

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

(т.к. мы не достигнем λ_n)



$\measuredangle$ v – ортогонально H т.ч. $\|v\| = \dfrac{\lambda_n(\hat{L})}{2}$

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

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

Отсюда $\mu(\hat{L}) \geqslant \dfrac{\lambda_n(\hat{L})}{2}$ $\blacktriangleright$