Лекция №9

Гауссова функция

I Анализ Фурье

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

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

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

Лемма 1 (Св-ва преобразования Фурье)

1. Если $h(x) = f(T\cdot x)$, где $T \in \mathbb{R}^{n\times n}$ - несингулярная, то
$$\hat{h}(y) = (\det T)^{-1} \hat{f}(T^{-t}\cdot y)$$
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 $h(x) = f(x)\cdot e^{2\pi i \langle v, y\rangle}$, то
$$\hat{h}(y) = \hat{f}(y-v)$$
4. Определим $(f * g)(z) := \int_{x\in\mathbb{R}^n} f(x)\cdot g(z-x)\, dx$.

Тогда
$$\widehat{f*g} = \hat{f}\cdot\hat{g}$$

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

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

$e^{-2\pi i \langle x', T^{-t} y\rangle} dx' = \frac{1}{\det T}\cdot \hat{f}(T^{-t}\cdot y).$

2-3. – см. Упр-ия.

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

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

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

$\blacktriangleright$

Лемма 2 (св-ва преобразования Фурье, ч.2)

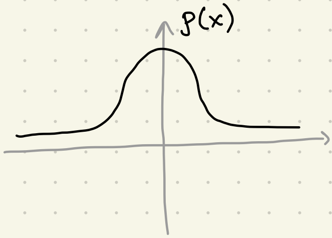
1. $\hat{\hat f}(x) = f(-x)$

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

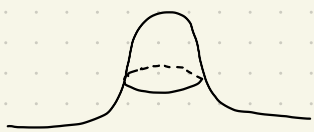
2. $p(x) = e^{-\pi\|x\|^2}$ – Гауссова ф-ия

$\hat p(x) = p(x)$. (Иначе, Гауссова ф-ия – это Айгенфции преобразования Фурье).

В $\mathbb{R}^1$



В $\mathbb{R}^2$



$\triangleleft$ 2. $$\hat p(x) = \int\limits_{x\in\mathbb{R}^n} p(x)\cdot e^{-2\pi i\langle x,y\rangle}\,dx = \int\limits_{x\in\mathbb{R}^n} e^{-\pi\|x\|^2 - 2\pi i\langle x,y\rangle}\,dx$$

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

$$= e^{-\pi\|y\|^2} \cdot \int_{x\in\mathbb{R}^n} e^{-\pi(\|x\|+i\|y\|)^2} dx = e^{-\pi\|y\|^2} \cdot \sqrt{\frac{\pi}{\pi}} = e^{-\pi\|y\|^2}$$ ▶

$$\int_{x\in\mathbb{R}^n} e^{-ax^2} = \sqrt{\frac{a}{\pi}}$$

Теорема (ф-ла сложения Пуассона / PSF)

Для $\forall$ достаточно "хорошей" ф-ии f (т.е. $\int_0^1 f dx$ существует), верно

$$\sum_{k\in\mathbb{Z}^n} f(k) = \sum_{k\in\mathbb{Z}^n} \hat{f}(k)$$

$$(\text{или} \quad f(\mathbb{Z}^n) = \hat{f}(\mathbb{Z}^n))$$

$\triangleleft$ обозначим $\varphi(x) := f(x+\mathbb{Z}^n) = \sum_{k\in\mathbb{Z}^n} f(x+k)$ для $x\in\mathbb{R}^n$

$\uparrow$

ф-ия с периодом 1, т.е. если $x\in\mathbb{Z}^n$, зн-ия $\varphi(x)$ совпадают.

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

Преобр-ие Фурье для $\mathbb{Z}^n$-периодичной ф-ии $\varphi(x)$ есть

$$\hat{\varphi}(z) : \mathbb{Z}^n \to \mathbb{C}$$

$$z \longmapsto \int_{x\in[0,1)^n} \varphi(x) e^{-2\pi i\langle x,z\rangle} dx$$

и справедливо

$$\varphi(x) = \sum_{z\in\mathbb{Z}^n} \hat{\varphi}(z) e^{-2\pi i\langle x,z\rangle}$$ – разложение по базису Фурье

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

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

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

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

Следствие $\forall$ решётки L и "хорошей" f:

$$f(L) = \det(\hat{L}) \cdot \hat{f}(\hat{L}) \qquad \Big(\sum_{x \in L} f(x) = \det(\hat{L}) \sum_{\hat{x} \in \hat{L}} \hat{f}(\hat{x}) \Big)$$

дуальная решётка

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

II Гауссово распределение на решётке

$\rho(x) = e^{-\pi \|x\|^2}$ задаёт вероятностное распр-ие на $\mathbb{R}^n$ $\Big(\int_{x \in \mathbb{R}^n} \rho(x) = 1 \Big)$

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

Кандидат: $\quad D(b) = \dfrac{e^{-\pi \|x\|^2}}{\rho(L)}$

Покажем, что $\rho(L)$ конечно.

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

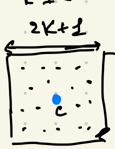
Более того, $\forall c \in \mathbb{R}^n$ $\ \rho(L - c) < +\infty$.

1 Покажем для $L = \mathbb{Z}^n$ (для $\forall$ другой решётки, $\exists$ коэф-ты её векторов относ. $\forall$ базиса, делаем замену переменных).

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

$k-1 \le \|b-c\| < k$

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



всевозможные b $\Rightarrow$ их число ограничено объёмом куба, т.е. $\le (2k+1)^n$

$$\textcircled{\leq} \sum_{k\in\mathbb{Z}_+} (2k+1)^n e^{-\pi(k-1)^2} \leq 1 + \sum_{k\in\mathbb{Z}_+} \underbrace{(2k+1)^n e^{-\pi k^2}}_{} < +\infty$$

$e^{-\pi\cdot k^2}$ убывает быстрее, чем $(2k+1)^n$

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

$$D_{L,\underset{\uparrow}{s},\underset{\uparrow \text{сдвиг}}{c}} = \frac{\rho_{s,c}(b)}{\rho_{s,c}(L)} = \frac{e^{-\frac{\pi\|b-c\|^2}{s^2}}}{\sum_{v\in L} e^{-\frac{\pi\|v-c\|^2}{s^2}}}.$$

среднекв. отклонение

Лемма (св-ва $D_{L,s,c}$)

1) $\forall L, \forall k\geq 1: \rho(L/k) \leq k^n \rho(L)$
2) $\forall L, \forall c\in\mathbb{R}^n: \rho(L+c) \leq \rho(L)$
3) $\rho_s(L+c) \leq s^n \rho(L)$
4) "Tail bound" "Гауссов хвост" $\forall L, \forall c\in\mathbb{R}^n, \forall d>0$:

$$\frac{\rho\left(L+c \setminus B^{(n)}\left(d\cdot\sqrt{\frac{n}{2\pi}}\right)\right)}{\rho(L+c)} \leq \left(\frac{d^2}{e^{d^2-1}}\right)^{\frac{n}{2}}$$

Для $c=0$, $s=1$ это св-во переписывается:

$$\Pr\left[b\leftarrow D_{L,1,0} : \|b\| > d\sqrt{\frac{n}{2\pi}}\right] \leq \left(\frac{d}{e^{d^2-1}}\right)^{\frac{n}{2}}.$$

$\triangleleft$ 1) $$\rho(L/k) \overset{PSF}{=} \det(\widehat{(L/k)})\cdot\hat{\rho}(\widehat{L/k}) \underset{\widehat{L/k}=k\hat{L}}{=} \det(k\cdot\hat{L})\cdot\rho(k\cdot\hat{L})$$
$$= k^n\cdot\det(\hat{L})\cdot\rho(k\cdot\hat{L}) \underset{\rho(1\cdot L)\geq\rho(kL) \text{ для } k\geq 1}{\leq} k^n\cdot\det(\hat{L})\cdot\rho(\hat{L}) \overset{PSF}{=} k^n\cdot\rho(L).$$

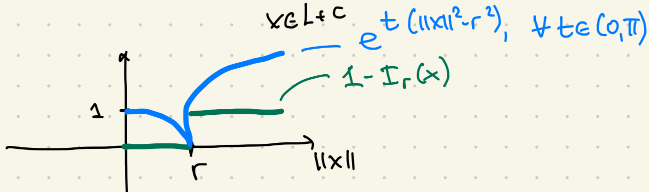
2) $$\rho(L+c) \overset{PSF}{=} \det(\hat{L})\cdot\underbrace{\sum_{\hat{b}\in\hat{L}}{}' \rho(\hat{b})\, e^{2\pi i\langle\hat{b},c\rangle}}_{\in\mathbb{R}_+} =$$

$$= \det(\hat{L}) \cdot \left| \sum_{\hat{b} \in \hat{L}} \rho(\hat{b})\, e^{2\pi i \langle \hat{b}, c \rangle} \right| \underset{\text{н-во } \Delta\text{-ка}}{\le} \det(\hat{L}) \cdot \sum_{\hat{b} \in \hat{L}} \rho(\hat{b}) \overset{PSF}{=} \rho(L).$$

4) Положим $I_r(x)$ – индикатор $B^{(n)}(r)$, т.е. $I_r(x) = \begin{cases} 1, & x \in B^{(n)}(r) \\ 0, & \text{иначе} \end{cases}$

$\exists r := \alpha \sqrt{\frac{n}{2\pi}}$

$$\rho\left(L+c \setminus B^{(n)}(r)\right) = \sum_{x \in L+c} \rho(x) \cdot [1 - I_r(x)] \le \sum_{x \in L+c} \rho(x) \frac{e^{t\|x\|^2}}{e^{tr^2}} =$$



$$= e^{-tr^2} \sum_{x \in L+c} e^{-\pi\|x\|^2 + t\|x\|^2} = e^{-tr^2} \sum_{x \in L} \underbrace{e^{\|x\|^2 \left(-\pi \left(\sqrt{1 - \frac{t}{\pi}}\right)^2\right)}}_{\rho_{\frac{1}{\sqrt{1-\frac{t}{\pi}}}}(x)} =$$

$$= e^{-tr^2} \cdot \rho_{\frac{1}{\sqrt{1-\frac{t}{\pi}}}}(L+c) \underset{\text{св-во } 2.}{\le} e^{-tr^2} \rho_{\frac{1}{\sqrt{1-\frac{t}{\pi}}}}(L).$$

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

Численно: для $\alpha = 1.93 < \sqrt{2\pi}$, правая сторона н-ва $\le 2^{-n}$.