Лекция №11.
Гауссова выборка на решётке.

I Статистическая разность

$\exists\, D_1, D_2$ — два распределения, заданные над счётным мн-вом Ω.

Статистическая разность м/д D_1 и D_2:

$$\Delta(D_1, D_2) = \frac{1}{2}\sum_{x\in\Omega} |D_1(x) - D_2(x)| = \frac{1}{2}\sum_{x\in\Omega} \Big|\Pr_{y\leftarrow D_1}[y=x] - \Pr_{y\leftarrow D_2}[y=x]\Big|$$

$$\overset{\text{def}}{=} \|D_1 - D_2\|$$

Будем обозначать $\Delta(X_1, X_2)$ для X_1, X_2 — случайных зн-ий.

__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. $\Delta\big((X_i)_i, (Y_i)_i\big) \le \sum_i \Delta(X_i, Y_i)$
3. Для ф-ии f (быть может, рандомизированной):

$$\Delta(f(X_1), f(X_2)) \le \Delta(X_1, X_2).$$

В частности, f может быть алгоритмом. Если f возвращает $0/1$, то

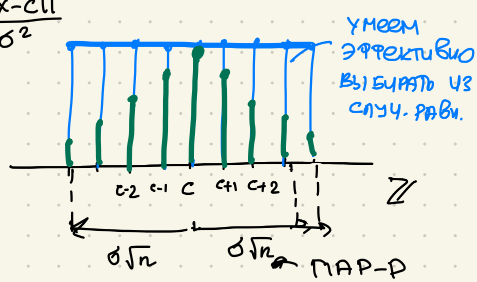
$$|\Pr[f(X_1)=1] - \Pr[f(X_2)=1]| \le \Delta(X_1, X_2).$$

II Гауссова выборка над $\mathbb{Z}$

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

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

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



Сложность Алг-ма 1 (кол-во Restart'ов)

$$\Pr_{x \leftarrow U[\mathbb{Z} \cap [c-\sigma\sqrt{n}, c+\sigma\sqrt{n}]]} [x \in [c-\sigma, c+\sigma]] = \frac{2\sigma - 1}{2\sigma\sqrt{n}+1} = \Omega\left(\frac{1}{\sqrt{n}}\right) \text{ для } \sigma \geq 1.$$

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

$$\geq e^{\frac{-\pi\sigma^2}{\sigma^2}} = e^{-\pi} = \Omega(1)$$

$\Rightarrow \mathbb{E}[\#\text{Restart}] \geq \sqrt{n}$, для пар-ра n.

Качество выборки = стат. разность м/у распределением выборки Алг-ма 1 и $D_{\mathbb{Z},\sigma,c}$.

Алг-м 1. выводит x с в-тью $\begin{cases} \Pr[x] \sim \rho_{\sigma,c}(x), & |x-c| \leq \sigma\sqrt{n} \\ 0, & |x-c| > \sigma\sqrt{n} \end{cases}$

$$\left.\begin{array}{l} \text{Гауссов хвост } \rho_{\sigma,c}(\mathbb{Z} \setminus B(\sigma\sqrt{n})) \leq 2^{-n} \rho_{\sigma,c}(\mathbb{Z}) \\ \text{Сглаживающий пар-р: Если } \sigma \geq \eta_{2^{-n}}(\mathbb{Z}), \text{ то } \rho_{\sigma,c}(\mathbb{Z}) \in [1-2^{-n}, 1+2^{-n}]\ \forall c \end{array}\right\}$$

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

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

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

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

$$\frac{1}{2} \rho_{\sigma,c}(\mathbb{Z} \cap B(\sigma\sqrt{n},c))$$

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

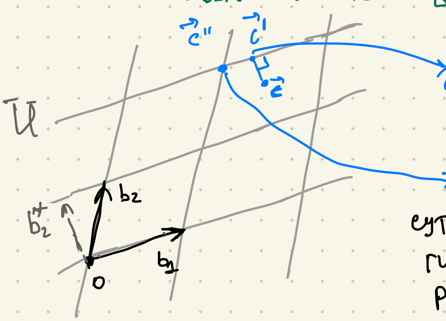
$$=\frac{1}{2}\left|1-\frac{\rho_{\sigma,c}(\mathbb{Z})-\rho_{\sigma,c}(\mathbb{Z}\setminus B(\sigma\sqrt{n}))}{\rho_{\sigma,c}(\mathbb{Z})}\right|+2^{-n-1}$$

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

Вывод: Алг-м 1 вернёт x за ожидаемое полиномиальное (от n) время; при этом стат. разность м/д распределением x и $D_{\mathbb{Z},\sigma,c}$ не более 2^{-n}.

III Гауссова выборка над L

Алг-м выборки из $D_{L,\sigma,c}$ (Klein'00) – рандомизированная версия алг-ма Бабая



ортогональная проекция $\vec{c}$ на гиперплоскость U

ближайший к $\vec{c}$ в $L\cap U$

суть алг-ма Кляйна: выбирать не фикс. ближайш. гиперплоскость, а рандомную относ. гауссова распределения.

Вход: $B = QR$ - базис $L \subseteq \mathbb{R}^n$, c, σ - пар-ры

Выход: $b \in L$

1. $y = Q^T \cdot c$ ("сдвигаем" рисунок на c)

   $b = 0$

2. For $i = n .. 1$:

   $$c_i = y - \sum_{j>i}' x_j r_{ij}$$

   $$x_i \leftarrow D_{\mathbb{Z}, \frac{\sigma}{r_{ii}}, \frac{c}{r_{ii}}}$$

   $$b = b + x_i b_i$$

3. Вернуть b.

Теорема Для $\sigma \geq \sqrt{n} \cdot \max_i r_{ii}$, выход алг-ма имеет распределение, стат. разность которого от $D_{L, \sigma, c}$ равна $2^{-\Omega(n)}$.

$\triangleleft$ 1. Выход алг-ма $\in L$.

2. $$\Pr_{b \in L}[\text{выход} = b] = \Pr[x_n = \bar{x}_n] \cdot \Pr[x_{n-1} = \bar{x}_{n-1} \mid x_n = \bar{x}_n] \cdot \ldots$$

$$b = \sum_{\bar{x}_i \in \mathbb{Z}} \bar{x}_i b_i$$

$$\cdot \Pr[x_1 = \bar{x}_1 \mid x_i = \bar{x}_i \ \forall i \geq 2] =$$

$$= D_{\mathbb{Z}, \frac{\sigma}{r_{nn}}, \frac{c_n}{r_{nn}}}(\bar{x}_n) \cdot D_{\mathbb{Z}, \frac{\sigma}{r_{n-1,n-1}}, \frac{c_{n-1}}{r_{n-1,n-1}}} \cdot \ldots$$

$$\cdot D_{\mathbb{Z}, \frac{\sigma}{r_{11}}, \frac{c_1}{r_{11}}} = \frac{1}{\prod_{i=1}^{n} \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z})} \cdot \prod_{i=1}^{n} \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\bar{x}_i)$$

$\ast$ Числитель $$\prod_{i=1}^{n} \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\bar{x}_i) = \prod_{i=1}^{n} e^{\frac{-\pi\left(\bar{x}_i - \frac{c_{ii}}{r_{ii}}\right)^2}{(\sigma / r_{ii})^2}} = e^{-\frac{\pi}{\sigma^2} \sum_i (r_{ii} \bar{x}_i - c_i)^2} =$$

$$= e^{-\frac{\pi}{\sigma^2} \sum_i \left(r_{ii} \bar{x}_i - y_i + \sum_{j>i} r \bar{x}_j\right)^2} = e^{-\frac{\pi}{\sigma^2} \sum_i \left((Q^T b)_i - (Q^T c)_i\right)^2}$$

$$\begin{cases} b = B\bar{x} = QR\bar{x} \\ Q^T \cdot b = R\bar{x} \\ \left(Q^T \cdot b\right)_i = \underbrace{R}_{R}\,\bar{x} = r_{ii}\cdot \bar{x}_i + \sum\limits_{j>i} r_{ij}\,\bar{x}_j \end{cases}$$

$$\begin{aligned} &= e^{-\pi/\sigma^2 \|Q^T b - Q^T c\|^2} \\ &= e^{-\pi/\sigma^2 \underbrace{\|Q^T(b-c)\|^2}_{Q \text{ не меняет норм}}} \\ &= e^{-\frac{\pi}{\sigma^2}\|b-c\|^2} = \rho_{\sigma,c}(\vec{b}) \end{aligned}$$

Знаменатель $\prod\limits_{i=1}^{n} \rho_{\frac{\sigma}{r_{ii}}, \frac{c}{r_{ii}}}(\mathbb{Z})$

$$\rho_{\frac{\sigma}{r_{ii}}, \frac{c}{r_{ii}}}(\mathbb{Z}) \in \left[(1-\varepsilon), (1+\varepsilon)\right] \cdot \rho_{\frac{\sigma}{r_{ii}}}(\mathbb{Z}) \qquad \frac{\sigma}{r_{ii}} \geq \eta_\varepsilon(\mathbb{Z})$$

По лемме 2 из пред. лекции: $\eta_{2^{-n}}(\mathbb{Z}) \leq \dfrac{\sqrt{n}}{\underbrace{\lambda_n(\mathbb{Z})}_{1}} \leq \sqrt{n} \Rightarrow$

$\Rightarrow$ по условию т-мы $\forall i \quad \dfrac{\rho_{\sigma/r_{ii}, \frac{c_i}{r_{ii}}}(\mathbb{Z})}{\rho_{\frac{\sigma}{r_{ii}}}(\mathbb{Z})} \in \left[1-2^{-n};\ 1+2^{-n}\right]$

$$\Rightarrow \underbrace{\rho_{\frac{\sigma}{r_{ii}}}(\mathbb{Z})}_{\text{не зависит от } b, \text{ от } c} \simeq \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z}) \Rightarrow$$

$\Rightarrow \Pr[\text{выход} = b] \approx \rho_{\sigma,c}(b).$ ∎