Лекция №11.
Алгоритм Гауссовой выборки на решётке

I. Статистическая разность

D_1, D_2 — два вероятностных распределения, заданные над счётным мн-вом Ω.

Опр-ие Статистическая разность м/д D_1 и D_2

$$\Delta(D_1, D_2) = \frac{1}{2} \sum_{x \in \Omega} |D_1(x) - D_2(x)| = \frac{1}{2} \sum_{x \in \Omega} \left| \Pr_{y \leftarrow D_1}[y = x] - \Pr_{y \leftarrow D_2}[y = x] \right| \overset{\text{def.}}{=} \| D_1 - D_2 \|$$

Будем обозначать $\Delta(X_1, X_2)$ для случайных значений x_1, x_2.

Лемма (свойства 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 алгоритмом. Если f возвращает бит, то

$$\left| \Pr[f(X_1) = 1] - \Pr[f(X_2) = 1] \right| \leq \Delta(X_1, X_2)$$

II Гауссова выборка над $\mathbb{Z}$

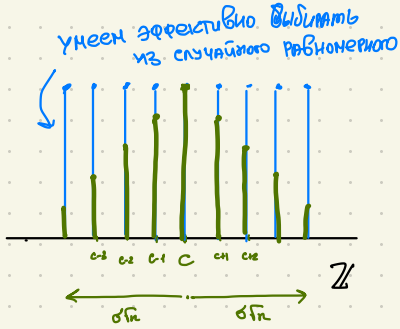
$$D_{\mathbb{Z},\sigma,c}(x) \sim \rho_\sigma(x-c) = e^{\frac{-\pi\|x-c\|^2}{\sigma^2}}$$

Алгоритм 1 : Выборка $D_{\mathbb{Z},\sigma,c}$

Вход: Параметр $n > 1$

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

   иначе Restart



Сложность Алгоритма 1 (кол-во Restart'ов)

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

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

$\Rightarrow \mathbb{E}[\#\text{Restart'ов}] \approx \sqrt{n}$ для пар-ра n.

"Качество" выборки из алг-ма 1 (= стат разность м/у выходом алг-ма 1 и $D_{\mathbb{Z},\sigma,c}$)

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

(*) "Граница хвоста" (лекция №9): $\rho_{\sigma,c}(\mathbb{Z} \setminus B(\sigma\sqrt{n})) \leq 2^{-n}\rho_{\sigma,c}(\mathbb{Z})$ (радиус)

(**) Сглаживающий пар-р (лекция №10, лемма 1): если $\sigma \geq \eta_{2^{-n}}(\mathbb{Z})$, то $\rho_{\sigma,c}(\mathbb{Z}) \in [1-2^{-n}, 1+2^{-n}] \cdot 1$, $\forall c$

(*) + (**): $\rho_{\sigma,c}(\mathbb{Z} \setminus B(\sigma\sqrt{n})) \leq 2^{-n}(1-2^{-n}) \leq 2^{-n}$

В итоге, рассмотрим Δ(сэмпл из Алг-ма 1, $D_{\mathbb{Z},\sigma,c}$) $\Subset$

$$\ominus \quad \frac{1}{2} \sum_{x \in \mathbb{Z}} \left| \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\mathbb{Z} \cap B(c, \sigma\sqrt{n}))} - \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\mathbb{Z})} \right| =$$

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

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

$$\le 2^{-n-1}$$

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

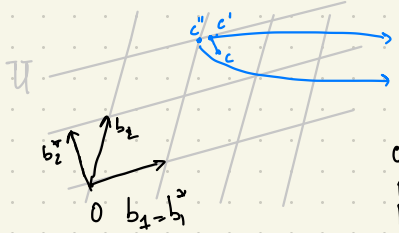
$$= \frac{1}{2} \left| 1 - \frac{\rho_{\sigma,c}(\mathbb{Z}) - \rho_{\sigma,c}(\mathbb{Z} \setminus B(c, \sigma\sqrt{n}))}{\rho_{\sigma,c}(\mathbb{Z})} \right| + 2^{-n-1} = \frac{1}{2} \underbrace{\frac{\rho_{\sigma,c}(\mathbb{Z} \setminus B(c, \sigma\sqrt{n}))}{\rho_{\sigma,c}(\mathbb{Z})}}_{\le 2^{-n}}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

$$\le 2^{-n-1} + 2^{-n-1} = 2^{-n}.$$

Вывод: Алг. 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, чем 2^{-n}

III Гауссова выборка над L

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



Суть алгоритма Клейна: выбирать не фиксированную гиперплоскость, а рандомную относительно Гауссова распределения.

Алгоритм 2. Выборка $D_{L,\sigma,c}$

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

Выход: $b \in L$

1. $y = Q^T \cdot c$ ("двигаем" рисунок на c)
   $b = 0$
2. For $i = n \dots 1$:
   $$c_i = y_i - \sum_{j>i} x_j r_{ij}$$
   $$x_i \leftarrow D_{\mathbb{Z}, \frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}$$
   $$b = b + x_i b_i$$
3. Вернуть b.

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

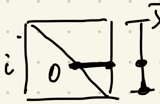
◁ 1 Выход алгоритма $\in L$.

2 $$\Pr_{b \in L}[\text{Выход} = b] = \sum_{\overline{x_i} \in \mathbb{Z}} \Pr[x_n = \overline{x_n}] \cdot \Pr[x_{n-1} = \overline{x_{n-1}} \mid x_n = \overline{x_n}] \cdot \dots \cdot \Pr[x_1 = \overline{x_1} \mid x_i = \overline{x_i}\ \forall i \geq 2] = D_{\mathbb{Z}, \frac{\sigma}{r_{nn}}, \frac{c_n}{r_{nn}}}(\overline{x_n}) \cdot D_{\mathbb{Z}, \frac{\sigma}{r_{n-1,n-1}}, \frac{c_{n-1}}{r_{n-1,n-1}}}(\overline{x_{n-1}}) \cdot \dots \cdot D_{\mathbb{Z}, \frac{\sigma}{r_{11}}, \frac{c_1}{r_{11}}}(\overline{x_1}) = \frac{1}{\prod_{i=1}^{n} \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z})} \cdot \prod_{i=1}^{n} \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\overline{x_i})$$

* числитель: $\prod_{i=1}^{n} \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\bar{x}_i) = \prod_{i=1}^{n} e^{\frac{-\pi \left(x_i - \frac{c_i}{r_{ii}}\right)^2}{(\sigma / r_{ii})^2}} =$

$$= e^{-\frac{\pi}{\sigma^2} \sum_i (r_{ii} x_i - c_i)^2} \overset{\text{шаг 2}}{=} e^{-\frac{\pi}{\sigma^2} \sum_i \left(r_{ii} \bar{x}_i - \underset{(Q^T c)_i}{\underset{\parallel}{x_i}} + \sum_{j>i} \bar{x}_j \cdot r_{ij} \right)^2} \; \textcircled{=}$$

$$\left\{ \begin{array}{l} b = B \cdot \bar{x} = Q \cdot R \bar{x} \\ Q^T \cdot b = R \bar{x} \\ (Q^T b)_i = \end{array} \right.$$



$$= r_{ii} \cdot \bar{x}_i + \sum_{j>i} r_{ij} \bar{x}_j$$

$$\textcircled{=} \; e^{-\frac{\pi}{\sigma^2} \sum_i \left((Q^T b)_i - (Q^T \cdot c)_i \right)^2} = e^{-\frac{\pi}{\sigma^2} \| Q^T b - Q^T \cdot c \|^2} =$$

$$= e^{-\frac{\pi}{\sigma^2} \| Q^T (b - c) \|^2} = e^{-\frac{\pi}{\sigma^2} \| b - c \|^2} = \rho_{\sigma, c}(b).$$

* знаменатель:

$$\rho_{\frac{\sigma}{r_{ii}}, \frac{c}{r_{ii}}}(\mathbb{Z}) \in [1 - \varepsilon, 1 + \varepsilon] \cdot \rho_{\frac{\sigma}{r_{ii}}}(\mathbb{Z}), \text{ если } \frac{\sigma}{r_{ii}} \geq \eta_{\varepsilon}(\mathbb{Z}) \text{ (лемма 1, лек-10)}$$

По лемме 2 из лекции 10: $\eta_{2^{-n}}(\mathbb{Z}) \leq \frac{\sqrt{n}}{\underbrace{\lambda_1(\mathbb{Z})}_{=1}} \leq \sqrt{n}$.

По условию теоремы: $\sigma \geq \sqrt{n} \cdot \max_i r_{ii} \geq \eta_{2^{-n}}(\mathbb{Z})$

$$\forall i: \frac{\rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z})}{\rho_{\frac{\sigma}{r_{ii}}}(\mathbb{Z})} \in [1 - 2^{-n}, 1 + 2^{-n}] \Rightarrow \underbrace{\rho_{\frac{\sigma}{r_{ii}}}(\mathbb{Z})}_{} \simeq \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z})$$

↑ не зависит от b, от c.

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