# Гауссова выборка над L

Monday 12 April 2021 08:49

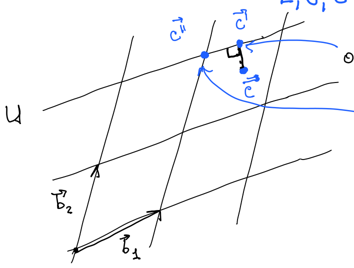
**Замечание:** В предыдущей лекции рассматривали алг-м выборки $D_{\mathbb{Z},\sigma,c}$ с пар-ом $n$.

За время $O(\sqrt{n})$, алг-м выдавал эл-т из $\mathbb{Z}$ в соответствии с распределение $\tilde{D}_{\mathbb{Z},\sigma,c}$, т.ч. $\Delta(D_{\mathbb{Z},\sigma,c}, \tilde{D}_{\mathbb{Z},\sigma,c}) \leq 2^{-n+2}$.

Т.е. чем больше $n$, тем медленнее алг-м, но тем "качественнее" выборка.

## Алгоритм выборки из $D_{L,\sigma,c}$ (Klein'00)

← рандомизированная версия редукции по р-ру




ортогональная проекция $\vec{c}$ на гиперплоскость $U$ – сдвиг $\mathrm{Span}_{\mathbb{R}}(\vec{b}_1)$

ближайший вектор в ЛПИ к $\vec{c}''$

Алгоритм Кляйна выбирает не фиксированную ближайшую гиперплоскость, а рандомную относит. Гауссова распределения.

**Вход:** $B = QR$ – базис $L$, $c$, $\sigma$ – пар-ры

**Выход:** $b \in L$

1. $y = Q^T \cdot c$ (сдвигаем "рисунок" на $c$)
   $b = 0$
2. For $i = n \dots 1$:

   $\begin{bmatrix} \diagdown & R \\ 0 & \diagdown \end{bmatrix}$

   $c_i = y_i - \sum\limits_{j>i} x_j r_{ij}$

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

   $b = b + x_i b_i$

Вывести $b$.

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

1. выход алг-ма $\in L$.
2. $$\Pr_{b\in L}[\text{выход} = b] = \Pr[x_n = \bar{x}_n] \cdot \Pr[x_{n-1} = \bar{x}_{n-1} \mid x_n = \bar{x}_n] \cdot \ldots \cdot \Pr[x_1 = \bar{x}_1 \mid x_i = \bar{x}_i \ \forall i \geq 2] =$$
$$\underset{\bar{x}_i \in \mathbb{Z}}{\sum^{n} \bar{x}_i b_i} = D_{\mathbb{Z}, \frac{\sigma}{r_{nn}}, \frac{c_n}{r_{nn}}}(\bar{x}_n) \cdot D_{\mathbb{Z}, \frac{\sigma}{r_{n-1,n-1}}, \frac{c_{n-1}}{r_{n-1,n-1}}}(\bar{x}_{n-1}) \cdot \ldots \cdot D_{\mathbb{Z}, \frac{\sigma}{r_{11}}, \frac{c_1}{r_{11}}}(x_1) =$$
$$= \frac{1}{\prod_i \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z})} \cdot \underbrace{\prod_i \rho_{\frac{\sigma}{r_{ii}}, c_i}(\bar{x}_i)}_{= \prod\limits_{i=1}^{n} e^{-\pi \frac{(\bar{x}_i - \frac{c_i}{r_{ii}})^2}{(\sigma / r_{ii})^2}} = e^{-\frac{\pi}{\sigma^2} \sum_i (r_{ii} x_i - c_i)^2}} =$$

$$\left\{\begin{array}{l} b = B \cdot x = Q \cdot R \cdot x \\ Q^T \cdot b = R \cdot x \\ (Q^T \cdot b)_i = i \boxed{\diagdown} \overset{x}{\boxed{\ }} = r_{ii} \cdot x_i + \sum\limits_{j>i} r_{ij} \cdot x_j \end{array}\right\}$$

$$= e^{-\frac{\pi}{\sigma^2}} \sum_i \Big(r_{ii} x_i - y_i + \sum_{j>i} r_{ij} x_j\Big)^2 = e^{-\frac{\pi}{\sigma^2}} \sum_i \Big((Q^T b)_i - (Q^T c)_i\Big)^2$$
$$= e^{-\frac{\pi}{\sigma^2}} \, Q \, \|b - c\|^2$$

↑ ортогональная матрица не изменяет норму.

∢ знаменатель $\prod_i \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z})$; $\rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z}) \in [(1-\varepsilon); (1+\varepsilon)] \cdot \rho_{\frac{\sigma}{r_{ii}}}(\mathbb{Z})$ для $\frac{\sigma}{r_{ii}} \geq \eta_\varepsilon(\mathbb{Z})$.

Т.к. $\eta_{2^{-n}}(\mathbb{Z}) \leq \sqrt{n} \cdot \underset{=1}{\lambda_1(\mathbb{Z})} = \sqrt{n} \Rightarrow \forall i \ \ \frac{\rho_{\sigma/r_{ii}, c}(\mathbb{Z})}{\rho_{\sigma/r_{ii}}(\mathbb{Z})} \in [1 - 2^{-n}, 1 + 2^{-n}] \Rightarrow \Pr[\text{выход} = b]$ отстаёт от $\rho_{\sigma,c}(b)$ на фактор $(1 \pm 2^{-n})$.