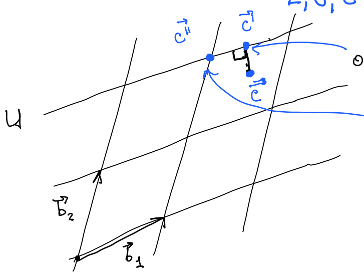
Замечание: в предыдущей лекции рассматривали алг-м выборки $D_{\mathbb{Z},\sigma,c}$ с пар-ом n.

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. $\Delta(D_{\mathbb{Z},\sigma,c}, \tilde{D}_{\mathbb{Z},\sigma,c}) \le 2^{-n+2}$.

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 $L \cap U$ к $\vec{c}''$

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

Вход: $B = QR$ – базис L, c, σ – пар-ры

Выход: $b \in L$

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

   $b = 0$

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

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

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

   $b = b + x_i b_i$

$$\boxed{{}_0\diagdown^R}$$

Вывести b.

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

1. выход алг-ма $\in L$.

2. $\Pr_{b\in L}[\text{выход} = b] = \Pr[x_n = \bar{x}_n] \cdot \Pr[x_{n-1} = \bar{x}_{n-1} \mid x_n = \bar{x}_n] \cdot \ldots \cdot \Pr[x_1 = \bar{x}_1 \mid x_i = \bar{x}_i \ \forall i \geq 2] =$

$\sum^n \bar{x}_i b_i$, $\bar{x}_i \in \mathbb{Z}$

$$= D_{\mathbb{Z}, \frac{\sigma}{r_{nn}}, \frac{c_n}{r_{nn}}}(\bar{x}_n) \cdot D_{\mathbb{Z}, \frac{\sigma}{r_{n-1,n-1}}, \frac{c_{n-1}}{r_{n-1,n-1}}}(\bar{x}_{n-1}) \cdot \ldots \cdot D_{\mathbb{Z}, \frac{\sigma}{r_{11}}, \frac{c_1}{r_{11}}}(x_1) =$$

$$= \frac{1}{\prod_i \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z})} \cdot \underbrace{\prod_i \rho_{\frac{\sigma}{r_{ii}}, c_i}(\bar{x}_i)}_{= \prod_{i=1}^n e^{-\pi \frac{(\bar{x}_i - \frac{c_i}{r_{ii}})^2}{(\sigma/r_{ii})^2}} = e^{-\frac{\pi}{\sigma^2}\sum_i (r_{ii}x_i - c_i)^2}} =$$

$$\left\{\begin{array}{l} b = B\cdot x = Q\cdot R\cdot x \\ Q^T b = R\cdot x \\ (Q^T b)_i = i\boxed{\diagdown}\left[\,\right]^x = r_{ii}x_i + \sum_{j>i} r_{ij}x_j \end{array}\right\} \quad = e^{-\frac{\pi}{\sigma^2}} \sum_i \Big(r_{ii}x_i - y_i + \sum_{j>i} r_{ij}x_j\Big)^2 = e^{-\frac{\pi}{\sigma^2}} \sum_i \big((Q^T b)_i - (Q^T c)_i\big)^2$$

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

↑ 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 $\frac{\sigma}{r_{ii}} \geq \eta_\varepsilon(\mathbb{Z})$. (по опр-ю $\eta_\varepsilon(\mathbb{Z})$)

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

↑ по условию теоремы

$\Rightarrow \rho_{\frac{\sigma}{r_{ii}}}(\mathbb{Z}) \approx \rho_{\frac{\sigma}{r_{ii}}, \frac{c_i}{r_{ii}}}(\mathbb{Z}) \Rightarrow \Pr[\text{выход} = b] \sim \rho_{\sigma,c}(b)$.

↑ независимо от b, от c