Практика № 2
22.01.24

1 Теорема Минковского-Хлавки

Для простого $q \geq 2$, $m > n > 0$ и матрицы A, выбранной случайно равномерно из $\mathbb{Z}_q^{m \times n}$, покажите

$$\lambda_1(L(A)) \geq \min\left(q, \frac{1}{10}\sqrt{m} q^{1-n/m} - \sqrt{m/2}\right).$$

Для этого сперва покажите, что для $\rho < q$, справедливо

$$\Pr_A[\lambda_1(L(A)) \leq \rho] \leq \sum_{\mathbf{y} \in \mathcal{B}(0,\rho) \cap \mathbb{Z}^m, \mathbf{s} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}} \Pr_A[A\mathbf{s} = \mathbf{y} \mod q],$$

где $\mathcal{B}(0, \rho)$ – шар радиусом ρ с центром в 0. Используя распределение A и простоту q, покажите, что из неравенства выше следует

$$\Pr_A[\lambda_1(L(A)) \leq \rho] \leq |\mathcal{B}(0, \rho) \cap \mathbb{Z}^m| \cdot q^{n-m}.$$

Шар $\mathcal{B}(0, \sqrt{m/2}\rho)$ (с увеличенным радиусом) содержит все единичные гипекубы, с центрами в точках $\mathcal{B}(0, \rho) \cap \mathbb{Z}^m$. Отсюда ограничьте сверху $|\mathcal{B}(0, \rho) \cap \mathbb{Z}^m|$.

2 QR-факторизация

Покажите, что

- Для $B = QR$ и любого $x \in \mathbb{R}^n$, выполняется $\|Bx\| = \|Rx\|$.
- Для решетки $L = L(B)$ и $B = QR$, выполняется $\lambda_1(L) \geq \min_i\{r_{ii}\}$.