Практика № 2
26.01.21

1 Теорема Минковского-Хлавки

Докажите, что с вероятностью $\geq 1 - 2^{-m}$ для $G \in \mathbb{Z}_q^{m \times n}$ выполняется

$$\lambda_1^\infty(L(G)) \geq \frac{1}{4} q^{1-n/m}.$$

Для этого

1. Зафиксируйте $B = \frac{1}{4} q^{1-n/m}$ и рассмотрите $\Pr_G[\lambda_1^\infty(L(G)) < B]$,
2. Покажите, что
$$\Pr_G[\lambda_1^\infty(L(G)) < B] \leq \sum_{s \in \mathbb{Z}_q^n} \sum_{\substack{y \in \mathbb{Z}^m \\ |y|_\infty < B}} \Pr[y = Gs \bmod q]$$
,
3. Покажите, что
$$\sum_{s \in \mathbb{Z}_q^n} \sum_{\substack{y \in \mathbb{Z}^m \\ |y|_\infty < B}} \Pr[y = Gs \bmod q] \begin{cases} = 0, & s = 0, \\ < 2^{-m}, & s \neq 0. \end{cases}$$

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 $\lambda_1(L) \geq \min_i\{r_{ii}\}$.