Практика № 3
К сдаче: 19.02

1 Свойства LLL редуцированного базиса

Докажите Лемму из Лекции: пусть $\delta \in (1/2, 1)$ – параметр LLL редукции, и $\alpha = \frac{1}{\sqrt{\delta - 1/4}}$. Тогда для $B \in \mathbb{Z}^{n\times n}$ – LLL редуцированного базиса справедливо:

1. $\|\mathbf{b}_1\| \leq \alpha^{n-1}\lambda_1(L(B))$
2. $\|\mathbf{b}_1\| \leq \alpha^{\frac{n-1}{2}} \det(L(B))^{1/n}$
3. $\frac{r_{i,i}}{r_{i+1,i+1}} \leq \alpha \quad \forall i \leq n.$

А: Начнём с тривиального пункта 3: так как по условию Ловаца имеем $r_{i,i} \leq \alpha r_{i+1,i+1}$, выражаем последовательно $r_{n,n}$.

П.2: следует из двух фактов: $r_{1,1} = \|\mathbf{b}_1^\star\| = \|\mathbf{b}_1\| \leq \alpha^{n-1} r_{n,n}$, и кроме этого, $\lambda_1(L) \geq \min_i r_{i,i} \geq \min_i \alpha^{-i+1} r_{1,1} = r_{1,1}\alpha^{-n+1} = \|\mathbf{b}_1\|\alpha^{-n+1}$.

П.1 следует из $\det L(B) = \prod_{i-1}^{n} r_{i,i} \geq \prod_{i=1}^{n} \left(\alpha^{-i+1} r_{1,1}\right) = \|\mathbf{b}_1\|^n \alpha^{(-n(n-1))/2}$.

2 Свойство BKZ редуцированного базиса

Пусть B – базис, полученный на вход BKZ алгоритма, а $B_{[i,j]}$ для $i < j$ базис проективной подрешетки, полученный из проекций векторов $(\mathbf{b}_i, \dots \mathbf{b}_j)$,ортогонально векторам $\mathbf{b}_i, \dots \mathbf{b}_j$ (иными словами, вырезанный из R-фактора квадрат на позициях с i по j). Первый вектор любого такого проективного базиса соответствует $\mathbf{b}^\star$ – i-ому вектору базиса Грамма-Шмидта (остальные вектора из этого вырезанного проективного базиса, в общем, не обязаны соответствовать векторам базиса Грама-Шмидта).

1. Примените теорему Минковского к $B_{[i,i+\beta-1]}$ и получите верхнюю границу на $\|\tilde{\mathbf{b}}_i\|$. Конкретно, покажите, что
$$\|\mathbf{b}_i^\star\|^\beta \leq \beta^{\beta/2} \prod_{j=i}^{i+\beta-1} \|\mathbf{b}_j^\star\| \tag{1}$$

   А: Теорема Минковского утверждает $\lambda_1(L) \leq \sqrt{n}(\det L)^{1/n}$ для решетки L ранга n. Для проективного блока $B[i, i+\beta-1]$ эта теорема переписывается как $\lambda_1(B[i, i+\beta-1]) \leq \sqrt{\beta}\det(B[i, i+\beta-1])^{1/\beta} = (\prod_{j=i}^{i+\beta-1} \|\mathbf{b}_j^\star\|)^{1/\beta}$. Искомое неравенство получается возведение последнего в степень β.

2. Используя неравенство выше, покажите, что для $1 \leq i \leq n-\beta+1$'s, справедливо
$$\|\mathbf{b}_1^\star\|^{\beta-1} \cdot \|\mathbf{b}_2^\star\|^{\beta-2} \cdot \dots \cdot \|\mathbf{b}_{\beta-1}^\star\| \leq \beta^{\frac{\beta(n-\beta+1)}{2}} \|\mathbf{b}_{n-\beta+2}^\star\|^{\beta-1} \|\mathbf{b}_{n-\beta+3}^\star\|^{\beta-2} \cdot \dots \cdot \|\mathbf{b}_n^\star\|. \tag{2}$$

   Для этого примените Неравенство (1) к $\prod_{i=1}^{n-\beta+1} \|\mathbf{b}_i^\star\|^\beta$.

A: Применим Неравенство 1 к $\mathbf{b}_i$ для $1 \le i \le n-\beta+1$:

$$\|\mathbf{b}_1^\star\|^\beta \le \beta^{\beta/2} \prod_{j=1}^{\beta} \|\mathbf{b}_j^\star\|$$
$$\|\mathbf{b}_2^\star\|^\beta \le \beta^{\beta/2} \prod_{j=2}^{\beta+1} \|\mathbf{b}_j^\star\|$$
$$\dots$$
$$\|\mathbf{b}_{n-\beta+1}^\star\|^\beta \le \beta^{\beta/2} \prod_{j=n-\beta+1}^{n} \|\mathbf{b}_j^\star\|$$

Рассмотрим произведение всех эти неравенства, получим:

$$\prod_{i=1}^{n-\beta+1} \|\mathbf{b}_i^\star\|^\beta \le \beta^{\frac{\beta(n-\beta+1)}{2}} \prod_{i=1}^{n-\beta+1} \prod_{j=i}^{\beta+i-1} \|\mathbf{b}_j^\star\|.$$

Если проследить, с какими степенями включены в произведения с обеих сторон элементы $\|\mathbf{b}_i^\star\|$, и сократить максимально возможные степени с обеих сторон, мы получим Неравенство 2.

3. Используя тот факт, что не только базис $B_{[1,\beta]}$ SVP-редуцирован (то есть его первый вектор есть кратчайший), но также и базисы $B_{[1,i]}$ при $i \le \beta$ SVP редуцированы (подумайте, почему это верно), сделайте вывод, что:

$$\|\mathbf{b}_1^\star\|^i \le i^{i/2} \prod_{j=1}^{i} \|\mathbf{b}_j^\star\| \quad \forall i \le \beta \tag{3}$$

   Сравните результат с Неравенством (1).

4. Перемножьте Неравенства (3) для $1 \le i \le \beta - 1$ и используйте Неравенство (2), чтобы получить

$$\|\mathbf{b}_1^\star\|^{\frac{\beta(\beta-1)}{2}} \le \beta^{\frac{\beta(n-1)}{2}} \cdot \|\mathbf{b}_{n-\beta+2}^\star\|^{\beta-1} \|\mathbf{b}_{n-\beta+3}^\star\|^{\beta-2} \cdot \ldots \cdot \|\mathbf{b}_n^\star\| \tag{4}$$

   A: Напрямую следует из (грубого) неравенства $\prod_{i=1}^{\beta} i^{i/2} \le \prod_{i=2}^{\beta-1} \beta^{\beta/2}$.

5. Положим, что в нашей решетке существует кратчайший вектора $\mathbf{v}_{\text{shortest}}$, чья проекция ортогонально первым $n-1$ базисным векторам ненулевая (так как иначе, если все кратчайшие вектора ортогональны $\mathbf{b}_n^\star$, то мы знаем, что все они лежат в подрешетке размерности не больше $n-1$, и в таком случае мы можем убрать из базиса $\mathbf{b}_n$).

   Из этого следует, что $\lambda_1 = \|\mathbf{v}_{\text{shortest}}\| \ge \|\mathbf{b}_i^\star\|$ для $n-\beta+2 \le i \le n$ (подумайте, почему). Подставив это неравенство в правую часть Неравенства (4), сделайте следующий вывод:

$$\|\mathbf{b}_1\| \le \beta^{\frac{n-1}{\beta-1}} \lambda_1.$$