Лекция №4

Алг-м перечисления для SVP.
(Shortest vector Problem)

BKZ-редукция базиса.

I Enumeration algorithm (Алг-м перечисления)

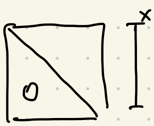
Kannan' 88

Finke-Post'83

Находит кратчайший вектор в решётке $\underbrace{\mathcal{L}(B)}_{"\{B\cdot x,\; x\in\mathbb{Z}^n\}}$, $B\in\mathbb{Z}^{n\times n}$, используя R-факт.

Задача: найти все $x\in\mathbb{Z}^n$: $\|Bx\| \le \underset{\text{граница}}{\overset{}{K}}$ $(K\in\mathbb{R})$ (1)

$$\underset{Q\cdot R}{\|Bx\|^2} = \|Rx\|^2 = \left\|\left(\sum_{i=1}^{n} r_{1i}x_i,\ \sum_{i=2}^{n} r_{2i}\cdot x_i,\ \dots,\ r_{nn}\cdot x_n\right)\right\|^2 = \sum_{j=1}^{n}\left(\sum_{i\ge j} r_{j,i}x_i\right)^2$$



• Если $\|Bx\|^2 \le K^2 \Rightarrow (r_{nn}\cdot x_n)^2 \le K^2$

т.к. $x_n\in\mathbb{Z}$, то $|x_n| \le \frac{K}{r_{nn}}$.

Всего $\left(2\cdot\frac{K}{r_{nn}}+1\right)$ всевозможных значений для x_n.

• Для фиксированного x_n, $\ast$ 2 последних слагаемых в (1).

$$\left(r_{n-1,n-1}x_{n-1} + r_{n-1,n}\cdot x_n\right)^2 + \left(r_{nn}\cdot x_n\right)^2 < K^2$$

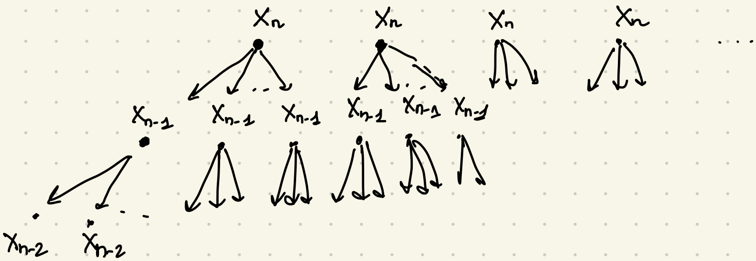
$$\Downarrow$$

$$\left|x_{n-1} + \frac{r_{n-1,n}}{r_{n-1,n-1}}x_n\right| \le \left(\frac{K^2-(r_{nn}x_n)^2}{r_{n-1,n-1}}\right)^{1/2}$$

Из н-ва для фикс. x_n, имеем $x_{n-1}\in\mathbb{Z}$ принадлежит интервалу длины $\le \frac{2K}{r_{n-1,n-1}}+1$.

⋮

Реализация такого алг-ма — проход по дереву (в глубину / depth-first)



Время работы $\quad \mathrm{poly}(n)\cdot|\text{дерева}| \le \mathrm{poly}(n)\sum_{j=1}^{n}\prod_{i\le j}\left(\frac{2K}{r_{ii}}+1\right)$ (2)

Оценим грубо (2)

Если запускать предварительно LLL-редукцию, то $\frac{r_{11}}{r_{ii}} \le d^{i-1}$ (св-во LLL-редуцированного базиса).

Для $K = r_{11} = \|b_1\| \le d^{\frac{n-1}{2}}(\det L)^{\frac{1}{n}}$: (2) $= \sum_{j=1}^{n}\prod_{i\le j}\left(2\underbrace{\frac{r_{11}}{r_{ii}}}_{\le 2\cdot d^{ii} = 2^i \text{ для } d=2}+1\right) = \sum_{j=1}^{n}\prod_{i\le j}(2^i+1) \le$

$$\le \sum_{j=1}^{n}\prod_{i\le j}3^i \le n\cdot\prod_{i=1}^{n}3^i = n\cdot 3^{n^2} = 2^{O(n^2)}$$ ← двойная эксп. сложность.

Суть: чем меньше r_{ii}, тем шире дерево и тем медленнее работает алгоритм. ⇒ можно запускать "предобработку" базиса B и сделать последние r_{ii} большими.

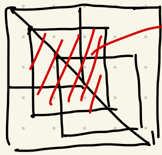
$\exists$ "предобработка" базиса B, т.ч. время работы алг-ма

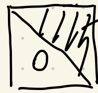
$\le n^{\frac{1}{2e}n+o(n)} = 2^{\frac{1}{2e}n\lg n+o(n)}$ ← время

Память: $\mathrm{poly}(n)$

III BKZ-редукция (Шнорр / Schnorr '87)
(block Korkin-Zolotarev)

LLL: блок р-ти 2 $\Rightarrow$ блок р-ти $k \in [2, n]$

$B = QR = Q \cdot$ 

- ∀ блок $k \times k$  R-фактор какой-то решётки р-ти k
- вызываем SVP (алг-м перечисления) на этом R-факторе $\Rightarrow$ кратчайший вектор в решётке р-ти k
- добавляем этот кратчайший вектор в B
- запускаем LLL на $\left[B \,\middle|\, \begin{array}{c}\text{кратч.}\\ \text{вектор}\end{array} \right]$, чтобы убрать лин. зависимость
- повторяем процедуру для $R_{[i+1,(i+1)k]\times[i+1,(i+1)k]}$

повторяем poly(n) раз

<u>Замечание</u> для того, чтобы показать, что BKZ алг-м терминируется, ∀ $d_i = \prod_{j=i+1}^{k(i+1)} r_{jj}$, повторяем анализ как в LLL, где вместо r_{ii} используем d_i.

	SVP	BKZ	LLL
время работы	$2^{\frac{n}{2e}\lg(n)+o(n)}$ $2^{O(n)+o(n)}$	$2^{O(k\lg k)+o(k)}$	poly(n)
качество $(\underbrace{\|b_1\|}_{\text{возвращаемое алг-мом значение}} / \lambda_1(L))$	1	$k^{O(\frac{n}{k})}$ $k<n$.	$2^{O(n)}$