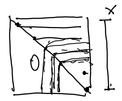
I Enumeration alg (алг-м перечисления) Kannan'88, Finke-Pohst'83

Находит кратчайший вектор в решётке $\mathcal{L}(B)$, $B \in \mathbb{Z}^{n\times n}$, используя R-фактор ($B=QR$)

$\mathcal{L}(B) = \{B\cdot x,\ x\in\mathbb{Z}^n\}$

Задача: найти все $x\in\mathbb{Z}^n$: $\|Bx\|<K$ ($K\in\mathbb{R}$) — граница; если $K\geq \lambda_1(L)$, храним кратчайший

$$\|Bx\|^2 = \|Rx\|^2 = \Big\|\Big(\sum_{i=1}^n r_{1i}x_i, \sum_{i=2}^n r_{2i}\cdot x_i, \dots, r_{nn}x_n\Big)\Big\|^2 = \sum_{j=1}^n \Big(\sum_{i\geq j} r_{j,i}x_i\Big)^2 \quad (1)$$

R: 

- Если $\|Bx\|^2<K^2$, то $(r_{nn}\cdot x_n)^2 \leq K^2$

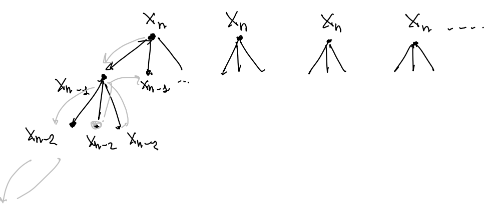
  Т.к. $x_n\in\mathbb{Z}$, то $|x_n|\leq \frac{K}{r_{nn}}$, всего $\left(2\frac{K}{r_{nn}}+1\right)$ всевозможных значений x_n

- Для фикс. x_n, рассмотрим 2 последних слагаемых в (1)

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

Из неравенства ⇒ для фикс. x_n, $x_{n-1}\in\mathbb{Z}$ принадлежит интервалу длины $\leq \frac{2K}{r_{n-1,n-1}}+1$.

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



Время работы: $\text{poly}(n)\ |\text{дерева}| \leq \text{poly}(n)\sum_{j=1}^n\prod_{i\leq j}\left(\frac{2K}{r_{jj}}+1\right)$ (2)

Оценим грубо (2)

Если запускать предварительно на $\mathcal{L}(B)$ алг-м LLL, то

$K = r_{11} = \|b_1\| = 2^n\det(L)^{1/n}$ (для $\alpha=2$)

$\frac{r_{11}}{r_{ii}}\leq\alpha^{i-1}$ (св-во LLL-редуцированного базиса)

$$(2) = \sum_{j=1}^n\prod_{i\leq j}\Big(2\underbrace{\frac{r_{11}}{r_{ii}}}_{\leq 2\alpha^{i-1}=2^i \text{ для } \alpha=2}+1\Big) \lesssim \sum_{j=1}^n\prod_{i\leq j}3^i \leq n\cdot\prod_{i=1}^n 3^i = n\cdot 3^{n^2} = \underbrace{2^{O(n^2)}}_{\text{двойное-экспоненц. алг-м.}}$$

Суть: чем меньше r_{ii}, тем шире дерево, тем медленнее работает алг-м.

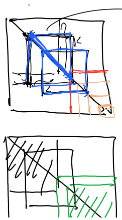
⇒ можно запустить "предобработку" базиса B и сделать последние r_{ii} большими.

∃ "предобработка" B, т.ч. время работы алг-ма $\leq n^{\frac{1}{2e}n+o(n)} = \underbrace{2^{\frac{1}{2e}n\lg n+o(n\lg n)}}_{\text{супер-экспоненциальное}}$

память: poly(n)

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

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

$B = QR = Q\cdot$  → * блок $k\times k$:  R-фактор решётки р-ти k

- вызываем SVP (перечисления) на этом R-факторе ⇒ кратчайший вектор в этой решётке — самый затратный шаг
- добавляем этот кратчайший вектор в B

- запускаем LLL на $[B \mid \text{кратч. вектор}]$, чтобы убрать лин. зависимость
- повторяем процедуру для $R_{[i+1,(i+1)k] \times [i+1,(i+1)k]}$

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

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

BKZ используется для вычисления ур-ня безопасности криптосистем.

Нахождение γ - аппрокс. короткого вектора $\Rightarrow$ взлом криптосистемы с пар-ми, зависящими от γ.

$\gamma = k^{\theta(\frac{n}{k})} \Rightarrow$ время работы алг-ма BKZ для k, удовлетвор. ур-ию $\Rightarrow$