Алгоритм перечисления для SVP. BKZ редукция

Tuesday 9 February 2021 08:14

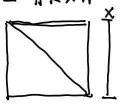
I Enumeration alg. (алг-м перечисл.)

Находит кратчайший вектор в решётке $L(B)$, используя R-фактор. $(B=QR)$

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

Задача: найти все $x\in\mathbb{Z}^n$: $\|B\cdot x\| \le k$ $(k\in\mathbb{R})$; если $k\ge\lambda_1(L)$, храним кратчайший;

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



- Если $\|Bx\|^2\le k^2$, то $(r_{nn}\cdot x_n)^2 \le k^2$

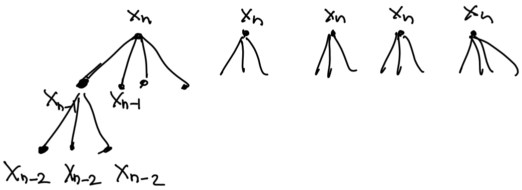
  т.к. $x_n\in\mathbb{Z}$, то $|x_n| \le \frac{k}{r_{nn}}$; всего $\left(2\cdot\frac{k}{r_{nn}}+1\right)$ возможных значений x_n

- для фикс. x_n, рассмотрим 2 последних слагаемых в $\color{blue}{(1)}$

$$(r_{n-1,n-1}\,x_{n-1} + r_{n-1,n}\,x_n)^2 \le k^2 - (r_{nn}\cdot x_n)^2$$
$$\Updownarrow$$
$$\left|x_{n-1} + \frac{r_{n-1,n}}{r_{n-1,n-1}}\cdot x_n\right| \le \left(\frac{k^2-(r_{n,n}x_n)^2}{r^2_{n-1,n-1}}\right)^{1/2};$$

$x_{n-1}\in\mathbb{Z}$, принадлежит интервалу длины $\le \frac{2k}{r_{n-1,n-1}}$

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



Время: $\mathrm{poly}(n)\cdot|\text{дерева}| \le \mathrm{poly}(n)\cdot\sum_{j\le n}\prod_{i\le j}\left(\frac{2k}{r_{i,i}}+1\right)$;

Чем меньше $r_{i,i}$, тем шире дерево (тем медленнее работает алг-м перечисл.)

$\Rightarrow$ запускаем "предобработку" базиса B. (делаем последние r_{ii} большими).

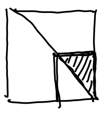
$\exists$ предобработка B, т.ч. время работы алг-ма $\le n^{\frac{n}{2e}+o(n)} = 2^{\frac{n}{2e}\lg n + o(n)}$;

суперэксп-ое время от n;

Память: $\mathrm{poly}(n)$

<u>Опр-ие</u> $B=Q\cdot R$ называется HKZ-редуцированным, если $\forall k$: $r_{k,k} = \lambda_1\left(L\left((r_{i,j})_{i,j\ge k}\right)\right)$ и (Hermite-Korkin-Zolotarev)

B редуцировано по раз-му.



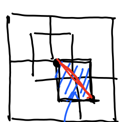
HKZ-базис существует:

- запускаем алг-м перечисл. на $L(B)$, находим $b\in L(B)$ — кратчайший
- преобразуем $[b\,|\,b_1\dots b_n]$ в базис $[b_1'|\dots b_n']$ такой, что $\|b_1'\|=\|b\|=\lambda_1(B)$
- вычисляем $R_{B'}$ и вызываем этот алг-м рекурсивно на R-фактор $(r_{ij})_{i,j\ge 2}$
- выполняем редукцию по р-ру

II BKZ-редукция (Шнорр, Schnorr)

(block Korkin-Zolotarev)

Блок р-ти 2 (LLL) $\Rightarrow$ Блок р-ти $k\in[2,n]$

$B = Q\cdot R = Q\cdot$  (полагаем, что $k\,|\,n$)

i-ый блок

для каждого $R_{[i\cdot k+1,\,(i+1)k]\times[i\cdot k+1,\,(i+1)k]}$ вызываем HKZ-редукцию.

Лемма. Положим $d_i = \prod_{j=ik+1}^{(i+1)k} r_{jj}$. Тогда если $R_{[i\cdot k+1,(i+1)\cdot k]\times[i\cdot k+1,(i+1)\cdot k]}$ – HKZ редуцировано, то

$$\frac{d_i}{d_{i+1}} \leq k^{c\cdot k} \quad \text{для константы } c.$$

(док-во: комбинация н-ва Минковского с опр-ем HKZ-ред. базиса).

Алгоритм BKZ

Вход: B, $\delta < 1$

Выход: BKZ-редуц базис

1. Вычисляем R-фактор
2. Редуцируем по р-ру
3. Если $\exists i$: $\frac{d_i}{d_{i+1}} > \frac{1}{\delta} k^{c\cdot k}$

   HKZ-редуцируем $R_{[i\cdot k+1,(i+1)k]\times[i\cdot k+1,(i+1)\cdot k]}$

   Restart

   Иначе

   HKZ-редуцируем блок №1 ($R_{[1,k]\times[1,k]}$) (1-ый вектор гарантированно короткий)

   Return

Анализ: аналог. LLL, где вместо r_{ii} рассматр. d_{ii}

	HKZ	Шнорр (k)	LLL
Time	$2^{n\cdot \lg n\cdot const + o(n\lg n)}$	$2^{O(k\lg k)} poly(n)$	$poly(n)$
Quality ($\|b_1\|/\lambda_1$)	1	$k^{O(\frac{n}{k})}$ для $k \ll n$	$2^{O(n)}$