原-对偶规约基与连续最小元

谢朝海[1,2], 陶 然[1], 王 越[1], 李继勇[1]
(1. 北京理工大学信息科学技术学院, 北京 100081; 2. 公安部信息安全等级保护评估中心, 北京 100036)

摘 要: 最近 Koy 提出一种质量优于 LLL 规约基的原-对偶规约基, 但没有给出该规约基与最小元比值因子的上界和下界. 本文首先分析了原-对偶规约基的性质, 然后给出并证明了原-对偶规约基与连续最小元比值因子的上界和下界, 最后用原-对偶规约基改进 Babai 的近似 CVP 算法——舍入算法, 提高了其近似因子.

关键词: 格; 规约基; 连续最小元; 长度亏损; 最近向量问题
中图分类号: TP393; O15 文献标识码: A 文章编号: 0372-2112 (2008) 06-1124-06

Primal-Dual Bases and Successive Minima

XIE Chao-hai[1,2], TAO Ran[1], WANG Yue[1], LI Ji-yong[1]
(1. *School of Information Science and Technology, Beijing Institute of Technology, Beijing* 100081, *China*;
2. *MPS Information Classified Security Protection Evaluation Center, Beijing* 100036, *China*)

Abstract: Recently Koy proposed primal-dual bases which have better quality than LLL-reduced bases in higher dimensional lattice, but his efforts did not take into account the low and upper bounds for the ratios of primal-dual bases to successive minima. In this paper some useful properties of Koy's primal-dual bases are analyzed and then the low and upper bounds for the ratios of primal-dual bases to successive minima are introduced and proved. At the end, the Round-off algorithm for the approximate CVP is improved using primal-dual bases and its result has a better approximation factor than L. Babai's.

Key words: lattice; reduced bases; successive minima; length defect; the closest vector problem (CVP)

1 引言

格基规约理论主要研究如何从格的所有基中找出一组含短向量的规范基[1]. 虽然对格基规约理论的研究已有 100 多年, 并取得了很多重要结果, 但是在高维格上一直没有取得维数多项式时间算法的满意结果. 上世纪 80 年代, A. K. Lenstra、H. W. Lenstra 和 L. Lovász 等人发表了著名的 LLL 规约算法, 在高维格上才取得了较好的规约效果, 使得格理论在现代密码学和密码分析学中, 得到迅速的推广应用, 成为人们研究的热点. LLL 规约算法可以看作 HKZ 规约算法的推广, 它降低了 HKZ 规约算法的条件, 降低了输出质量, 输出一组近似最短向量规约基, 以保证能在多项式时间内求解. 为了提高 LLL 规约算法的输出质量, 人们提出了一些近多项式时间算法, 有 1987 年 Schnorr 在文献[2]中提出的 β-BKZ 规约算法和 Koy 在文献[3]中提出的原-对偶规约算法等. 对原-对偶规约算法, 2006 年 Schnorr 在文献[4]中作了进一步优化改进.

连续最小元是格上一个重要的概念, 有着广泛的应用. 人们常用规约基与连续最小元比值作为一项衡量规约算法质量的重要指标[5]. 早在 1938 年 Mahler 就给出了 HKZ 规约基与连续最小元比值因子的上界[6], 之后直到 1990 年, J. C. Lagarias 等人才给出 HKZ 规约基与连续最小元比值因子的下界[7]. Lenstra 等人在文献[8]中给出 LLL 规约算法的同时, 给出了 LLL 规约基与连续最小元比值因子的上界和下界. 记为 $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ 格 L 的一组带参数 δLLL 规约基, 他们证明有 $\alpha^{1-i} \leqslant \|\boldsymbol{b}_i\|^2 \cdot \lambda_i(L)^{-2} \leqslant \alpha^{n-1}$, 其中, $\alpha = 1/(\delta - 1/4)$. Schnorr 在其提出 β-BKZ 规约基 7 年后, 才给出了该规约基与连续最小元比值因子的上界和下界[9]. 人们自然会问, 对于 Koy 提出的原-对偶规约基, 其与连续最小元比值因子的上界和下界又会是多少呢?

Koy 在文献[3]中给出了原-对偶规约基长度亏损 (length defect) 的上界, Schnorr 在文献[4]中取得了比 Koy 更紧的长度亏损上界, 但是他们都没有给出原-对偶规约基与连续最小元比值因子的上界和下界. 本文首先把 LLL 规约基的一些重要性质推广到原-对偶规约基上, 在此基础上, 提出并证明了原-对偶规约基与连续最小元比值因子的上界和下界. 最后, 作为原-对偶规约基性质的一个应用实例, 用原-对偶规约基改进 Babai 的近似 CVP 算法[10], 证明在原-对偶规约基上舍入 (Round off) 算法近似因子为 $(1+(2n)3^{\frac{n-1}{2}}(3\alpha/4)^{\alpha/4-1})$. 当 δ 取 $\frac{3}{4}$, α = 2 时, 比 Babai 的舍入算法约提高了

收稿日期: 2007-04-02; 修回日期: 2008-01-26
基金项目: 国家 863 高技术研究发展计划 (No. 2006AA01Z450); 国防基础科研项目 (No. C1120060497)

$\frac{3\sqrt{2}}{2}\left(\frac{3}{2}\right)^{(1-1/k)\frac{n}{2}}$倍.

2 相关知识和记号

2.1 定义和记号

设 $\boldsymbol{B}=[\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n], \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n \in \mathbf{R}^m (n \leqslant m)$ 是 n 个线性无关的实向量, 集合 $L(\boldsymbol{B})=\left\{\sum_{i=1}^{n} x_i \boldsymbol{b}_i \mid x_i \in \mathbf{Z}\right\}$ 是一个格. 向量 $\boldsymbol{b}_i (1 \leqslant i \leqslant n)$ 称为格 L 的基向量, 矩阵 $\boldsymbol{B}$ 称为格L 的基矩阵. 格 L 的维数 $\dim(L)$ 为基向量个数 n. 记 $d_i=\det([\boldsymbol{b}_1, \cdots, \boldsymbol{b}_i]^t[\boldsymbol{b}_1, \cdots, \boldsymbol{b}_i])$, 格 L 的行列式 $\det(L)=\det(\boldsymbol{B}^t\boldsymbol{B})^{1/2}=d_n^{1/2}$. 向量 $\boldsymbol{b} \in \mathbf{R}^m$ 的长度为 $\|\boldsymbol{b}\|=|\boldsymbol{b}^t\boldsymbol{b}|^{1/2}$.

设格 L 的一组基为 $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n \in \mathbf{R}^m (n \leqslant m)$, 秩为 n, 第 i 连续最小元定义为: $\lambda_i(L)=\inf\{r \mid \dim(\operatorname{span}(L \cap \bar{B}(o, r))) \geqslant i\}$, 这里 $\bar{B}(o, r)=\{x \in \mathbf{R}^m \mid \|x\| \leqslant r\}$. 显然, λ_1 是格L 中所有最短非零向量的长度. 规约基的长度亏损定义为 $\|\boldsymbol{b}_i\| / \lambda$

Hermite 常数 γ_n 定义为: $\gamma_n=\sup\{\lambda_1(L)^2 \cdot \det(L)^{-2/n}: \forall L, \dim(L)=n\}$. 目前已经知道 $n \leqslant 8$ 的 Hermite 常数的值. $\gamma_2^2=\frac{4}{3}$, $\gamma_3^3=2$, $\gamma_4^4=4$, $\gamma_5^5=8$, $\gamma_6^6=2^6/3$, $\gamma_7^7=2^6$, $\gamma_8^8=2^8$, 且 $\gamma_n \leqslant \frac{2}{3}n$, $n \geqslant 2$.

对格 L 的一组基 $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n \in \mathbf{R}^m$ 进行标准 Gram-Schmidt 正交化, 通过递归循环: $\boldsymbol{b}_1^*=\boldsymbol{b}_1$ 和 $\boldsymbol{b}_i^*=\boldsymbol{b}_i-\sum_{j=1}^{i-1}\mu_{i,j}\boldsymbol{b}_j^*$, 可以得到一组 GSO 向量 $\boldsymbol{b}_1^*, \cdots, \boldsymbol{b}_n^* \in \mathbf{R}^m$, 这里 $\mu_{i,j}=\langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle \setminus \|\boldsymbol{b}_j^*\|^2$, $i>j$, 为 GS 系数. 显然, $\det(L)=\prod_{i=1}^{n}\|\boldsymbol{b}_i^*\|$.

定义正交投影 $\pi_i: \mathbf{R}^m \to \operatorname{span}(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{i-1})^{\perp}$, 这样就有. $\boldsymbol{b}-\pi_i(\boldsymbol{b}) \in \operatorname{span}(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{i-1})$. 记 $L_i=\pi_i(L)=\pi_i(L(\boldsymbol{b}_i, \cdots, \boldsymbol{b}_n))=L(\pi_i(\boldsymbol{b}_i), \cdots, \pi_i(\boldsymbol{b}_n))$, 有 $\dim(L_i)=n-i+1$, 其一组基 $\pi_i(\boldsymbol{b}_i), \pi_i(\boldsymbol{b}_{i+1}), \cdots, \pi_i(\boldsymbol{b}_m)$, 有 $\pi_i(\boldsymbol{b}_i)=\boldsymbol{b}_i^*$ 和 $\pi_i(\boldsymbol{b}_j)=\boldsymbol{b}_j^*+\sum_{k=i}^{j-1}\mu_{j,k}\boldsymbol{b}_k^*$.

称矩阵 $\boldsymbol{Q} \in \mathbf{R}^{m \times n}$ 是等距矩阵, 如果对任意 $\boldsymbol{x}, \boldsymbol{y} \in \mathbf{R}^m$, $\langle \boldsymbol{Q}\boldsymbol{x}, \boldsymbol{Q}\boldsymbol{y} \rangle=\langle \boldsymbol{x}, \boldsymbol{y} \rangle=\boldsymbol{x}^t\boldsymbol{y}$. 格基矩阵 $\boldsymbol{B} \in \mathbf{R}^{m \times n}$ 的 $\boldsymbol{QR}$ 分解 $\boldsymbol{B}=\boldsymbol{QR}$ 由一个等距矩阵 $\boldsymbol{Q} \in \mathbf{R}^{m \times n}$ 和一个有正对角元素的上三角矩阵 $\boldsymbol{R}=[r_1, \cdots, r_n]=[r_{i,j}] \in \mathbf{R}^{n \times n}$ 组成. 对矩阵 $\boldsymbol{B}$ 实施等距变换时, 矩阵 $\boldsymbol{R}$ 保持不变. 我们称矩阵 $\boldsymbol{R}$ 是 $\boldsymbol{B}$ 的几何标准型(GNF), $R=\mathrm{GNF}(B)$. 根据矩阵 $\boldsymbol{QR}$ 分解的性质可得 Gram-Schmidt 系数 $\mu_{j,i}=r_{i,j}/r_{i,i}$, 并且 $r_{i,i}=\|\boldsymbol{b}_i^*\|$ ($\boldsymbol{b}_i^*$ 为向量 $\boldsymbol{b}_i$ 对应的 Gram-Schmidt 正交化向量); 同时还有 $\|\boldsymbol{b}_i\|^2=\sum_{j=1}^{i}r_{j,i}^2$, $\|\boldsymbol{b}_1\|=r_{1,1}$.

2.2 HKZ 和 LLL 规约基

设 $\boldsymbol{B}$ 为格的一组基, 对任意一个么模矩阵 $\boldsymbol{U}$, 有 $\boldsymbol{B}'=\boldsymbol{BU}$ 也是格L 的格基矩阵. 在所有这些格基中, 根据实际应用的需要, 通常把近似垂直的、短的格基认为是好的格基, 也是我们常说的规约基. 目前人们定义了多种不同规约基, 其中两个较重要的规约基是 HKZ 规约基和 LLL 规约基.

格基 $\boldsymbol{B} \in \mathbf{R}^{m \times n}$ 是 HKZ 规约基, 如果满足下面两个条件:

$$|r_{i,j}| \leqslant \frac{1}{2}r_{i,i}, \quad 1 \leqslant i < j \leqslant n \tag{1}$$

$$\|r_{i,i}\|=\lambda_1(L_i), \quad i=1, \cdots, n \tag{2}$$

Kannan 和 Schnorr 分别给出了一个计算 HKZ 规约基的指数时间算法, 时间复杂度为 $O(mn^{n/2+o(n)})$, 这是目前计算 HKZ 规约基比较有效的算法.

格基 $\boldsymbol{B}$ 是带参数 $\delta \in (\frac{1}{4}, 1]$ 的 δ-LLL 规约基, 如果满足上面的条件式(1), 且满足:

$$\delta r_{i,i}^2 \leqslant r_{i,i+1}^2+r_{i+1,i+1}^2, \quad i=1, \cdots, n-1 \tag{3}$$

显然, LLL 规约基满足 $r_{i,i}^2 \leqslant \alpha r_{i+1,i+1}^2$, $\alpha=1/(\delta-\frac{1}{4})$. 通常 δ 取 $\frac{3}{4}$, $\alpha=2$. 文献[8]给出了一个计算 LLL 规约基的多项式时间算法和 LLL 规约基的一些性质. Cohen 在文献[11]补充了 LLL 规约基的一些有用的性质.

3 原-对偶规约基

3.1 定义

格 $L=L(\boldsymbol{QR})$ 的对偶格定义为:

$$L'=\{z \in \operatorname{span}(L) \mid z^t y \in \mathbf{Z}, \ \forall y \in L\} \tag{4}$$

因为有 $(\boldsymbol{QR}^{-t})^t\boldsymbol{QR}=\boldsymbol{R}^{-1}\boldsymbol{Q}^t\boldsymbol{QR}=\boldsymbol{R}^{-1}\boldsymbol{R}=\boldsymbol{I}_n$ 所以 $L'=L(\boldsymbol{QR}^{-t})$. 设转置矩阵 $\boldsymbol{U}_k=\begin{bmatrix} & & 1 \\ & \cdots & \\ 1 & & \end{bmatrix} \in \mathbf{Z}^{k \times k}$, $\boldsymbol{U}_k$ 可以通过右乘或左乘矩阵 $\boldsymbol{B} \in \mathbf{R}^{m \times n}$ 使其列或行发生翻转. 称 $\boldsymbol{B}'=\boldsymbol{QR}^{-t}\boldsymbol{U}_n$ 为格基 $\boldsymbol{B}=\boldsymbol{QR}$ 的(互逆)对偶基. (互逆)对偶基有 $(\boldsymbol{B}')'=\boldsymbol{B}$, 其几何标准型 GNF $\boldsymbol{R}'=\boldsymbol{U}_n\boldsymbol{R}^{-t}\boldsymbol{U}_n$. 格基 $\boldsymbol{B}=[\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n]$, 其(互逆)对偶基 $\boldsymbol{B}'=[\boldsymbol{b}_1', \cdots, \boldsymbol{b}_n']$, 有:

$$\langle \boldsymbol{b}_i, \boldsymbol{b}_{n-j+1}' \rangle=\langle \boldsymbol{b}_i', \boldsymbol{b}_{n-j+1} \rangle=\delta_{i,j}, \ \delta_{i,j}=\begin{cases} 0, & i \neq j \\ 1, & i=j \end{cases} \tag{5}$$

对应几何标准型 $\boldsymbol{R}=[r_{i,j}]$ 和 $\boldsymbol{R}'=[r_{i,j}']$ 有:

$$r_{i,i}=1/r_{n-i+1,n-i+1}' \quad (i=1, \cdots, n) \tag{6}$$

原-对偶规约基的规约是分段进行的. 设段大小为 k, $n=hk$. 对格基 $\boldsymbol{B}=\boldsymbol{QR}$, $\boldsymbol{R}=[r_{i,j}]_{1 \leqslant i,j \leqslant n}$, 记格基第 l 段 $\boldsymbol{B}_l=[\boldsymbol{b}_{kl-k+1}, \cdots, \boldsymbol{b}_{kl}]$ 在格基 $\boldsymbol{B}$ 几何标准型 GNF $\boldsymbol{R}$ 中对

应的子矩阵分别为 $\boldsymbol{R}_l$ 如下:

$$\boldsymbol{R}_l=[r_{i,j}]_{kl-k<i,j\leqslant kl}\in\mathbf{R}^{k\times k},\ kl\leqslant n \qquad (7)$$

定义 1[4] 格基矩阵 $\boldsymbol{B}=\boldsymbol{QR}\in\mathbf{R}^{m\times n}$, $n=hk$ 是(k,δ)原-对偶规约基$(\delta\in(1/4,1])$, 如果它的 GNF $\boldsymbol{R}=[r_{i,j}]_{1\leqslant i,j\leqslant n}$满足下面两个条件:

(1) $\boldsymbol{R}_1,\ \cdots,\ \boldsymbol{R}_h\subset\boldsymbol{R}$ 都是HKZ规约的

(2) $\overrightarrow{r}_{kl,kl}\leqslant\alpha\overrightarrow{r}^2_{kl+1,kl+1}$, $l=1,\ \cdots,\ h-1$

其中, $\overrightarrow{r}_{kl,kl}$为所有 GNF$(\boldsymbol{R}_l\boldsymbol{U})=[\tilde{r}_{i,j}]_{kl-k<i,j\leqslant kl}$中最大的 $\tilde{r}_{kl,kl}$, $\alpha=1/(\delta-\frac{1}{4})$.

显然, 当 $k=1$ 时, 原-对偶规约基为 δLLL 规约基. 由式(6)和定义 1 的条件 2 易知, 原-对偶规约基$\boldsymbol{B}$ 的对偶基$\boldsymbol{B}'$ 也满足定义 1 的条件 2. Koy 给出一个时间复杂度为 $O((n^4+n^2(2k)^{k+o(k)})\log M)$且参加运算的数位长为 $O(n\log M)$的原-对偶规约算法, 其中 M 为基向量的最大长度[4].

3.2 性质

性质 1 格基 $\boldsymbol{B}=[\boldsymbol{b}_1,\ \cdots,\ \boldsymbol{b}_n]=\boldsymbol{QR}\in\mathbf{R}^{m\times n}$是格$L$的一组$(k,\delta)$原-对偶规约基, $n=hk$, 对 $1\leqslant j\leqslant i\leqslant n$, 有 $\|\boldsymbol{b}_j^*\|^2\leqslant(4/3)^{i-j}(3\alpha/4)^d\|\boldsymbol{b}_i^*\|^2$, 其中, $\alpha=1/(\delta-\frac{1}{4})$, $d=\lceil i/k\rceil-\lceil j/k\rceil$

证: 因为 $\|\boldsymbol{b}_i^*\|=r_{i,i}$, 所以只需证: $r^2_{j,j}\leqslant(4/3)^{i-j}(3\alpha/4)^d r^2_{i,i}$.

当 $d=0$ 时, $r_{j,j}$, $r_{i,i}$ 同属于一个 $\boldsymbol{R}_l=[r_{i,j}]_{kl-k<i,j\leqslant kl}\in\mathbf{R}^{k\times k}$, $kl\leqslant n$, 由定义 1 条件 1 知, $\boldsymbol{R}_l$ 是KZ规约的, 所以对 $\boldsymbol{R}_l$ 中任一元素 $r_{v,v}$, $kl-k<v<kl$, 有 $r_{v,v}\leqslant r_{v,v+1}$, 于是有

$$r^2_{v,v}\leqslant r^2_{v,v+1}=r^2_{v+1,v+1}+\mu^2_{v+1,v}r^2_{v,v}\leqslant r^2_{v+1,v+1}+\frac{1}{4}r^2_{v,v}$$

即 $r^2_{v,v}\leqslant\frac{4}{3}r^2_{v+1,v+1}$, $kl-k<v<kl$. 所以

$$r^2_{j,j}\leqslant(4/3)^{i-j}r^2_{i,i}=(4/3)^{i-j}(3\alpha/4)^d r^2_{i,i}$$

当 $d=1$ 时, 令 $u=\lceil j/k\rceil$则 $r_{j,j}$, $r_{uk,uk}$同属于$\boldsymbol{R}_u$, $r_{uk+1,uk+1}$, $r_{i,i}$同属于$\boldsymbol{R}_{u+1}$, 于是有

$$r^2_{j,j}\leqslant(4/3)^{uk-j}r^2_{uk,uk},\ r^2_{uk+1,uk+1}\leqslant(4/3)^{i-uk-1}r^2_{i,i}$$

由定义 1 条件 2 知, $r^2_{uk,uk}\leqslant\alpha r^2_{uk+1,uk+1}$, 得

$$r^2_{j,j}\leqslant(4/3)^{i-j-1}\alpha r^2_{i,i}=(4/3)^{i-j}(3\alpha/4)^d r^2_{i,i}$$

同理, 当 $d>1$ 时, 有 $r^2_{j,j}\leqslant(4/3)^{i-j-d}\alpha^d r^2_{i,i}=(4/3)^{i-j}(3\alpha/4)^d r^2_{i,i}$.

性质 2 格基 $\boldsymbol{B}=[\boldsymbol{b}_1,\ \cdots,\ \boldsymbol{b}_n]\in\mathbf{R}^{m\times n}$是格$L$的一组$(k,\delta)$原-对偶规约基, $n=hk$, 对任意 i, $1\leqslant j\leqslant i\leqslant n$, 有 $\|\boldsymbol{b}_j\|^2\leqslant(4/3)^{i-1}(3\alpha/4)^{d-1}\|\boldsymbol{b}_i^*\|^2$, 其中, $\alpha=1/(\delta-\frac{1}{4})$, $d=\lceil i/k\rceil$

证: 令 $u=\lceil j/k\rceil$ $s=j-(u-1)k$. 由 Gram-Schmidt 正交化公式和 $|\mu_{jp}|\leqslant\frac{1}{2}$, 得 $\|\boldsymbol{b}_j\|^2\leqslant\|\boldsymbol{b}_j^*\|^2+\frac{1}{4}\sum_{p=1}^{i-1}\|\boldsymbol{b}_p^*\|^2$. 根据性质 1 有

$$\|\boldsymbol{b}_j\|^2\leqslant\|\boldsymbol{b}_j^*\|^2+\frac{1}{4}\|\boldsymbol{b}_j^*\|^2\sum_{p=1}^{uk-1}(4/3)^p+\frac{1}{4}\|\boldsymbol{b}_j^*\|^2\sum_{g=1}^{u-1}[(3\alpha/4)^{u-g}(4/3)^{j-gk}\sum_{p=1}^{k}(4/3)^{p-1}]$$

把 1/4 变为$(4/3)^{-1}(4/3-1)$后, 与两个求和式相乘, 整理上式得

$$\begin{aligned}\text{右边}&=\|\boldsymbol{b}_i^*\|^2+\|\boldsymbol{b}_j^*\|^2[(4/3)^{s-1}-1]\\&\quad+\|\boldsymbol{b}_j^*\|^2\sum_{g=1}^{u-1}\{(3\alpha/4)^{u-g}(4/3)^{j-gk-1}[(4/3)^k-1]\}\\&=\|\boldsymbol{b}_j^*\|^2+\|\boldsymbol{b}_j^*\|^2[(4/3)^{s-1}-1]+\|\boldsymbol{b}_j^*\|^2(3\alpha/4)\\&\quad(4/3)^{s-1}[(4/3)^k-1]\sum_{g=1}^{u-1}[(3\alpha-4)^{(u-1)-g}\\&\quad(4/3)^{(u-1-g)k}]\\&=\|\boldsymbol{b}_j^*\|^2+\|\boldsymbol{b}_j^*\|^2[(4/3)^{s-1}-1]+\|\boldsymbol{b}_j^*\|^2(3\alpha/4)\\&\quad(4/3)^{s-1}[(4/3)^k-1]\frac{(3\alpha/4)^{(u-1)}(4/3)^{(u-1)k}-1}{(3\alpha/4)(4/3)^k-1}\end{aligned}$$

因为 $\alpha=1/(\delta-1/4)\geqslant4/3$, 所以有

$$\begin{aligned}\|\boldsymbol{b}_j^*\|^2&\leqslant\|\boldsymbol{b}_j^*\|^2+\|\boldsymbol{b}_j^*\|^2[(4/3)^{s-1}-1]\\&\quad+\|\boldsymbol{b}_j^*\|^2(4/3)^{s-1}[(3\alpha/4)^{(u-1)}(4/3)^{(u-1)k}-1]\\&=\|\boldsymbol{b}_j^*\|^2+\|\boldsymbol{b}_j^*\|^2[(4/3)^{s-1}-1]+\|\boldsymbol{b}_j^*\|^2\\&\quad[(3\alpha/4)^{(u-1)}(4/3)^{s+(u-1)k-1}-(4/3)^{s-1}]\\&=(4/3)^{j-1}(3\alpha/4)^{u-1}\|\boldsymbol{b}_j^*\|^2\end{aligned}$$

再根据性质 1, 有

$$\begin{aligned}\|\boldsymbol{b}_j\|^2&=(4/3)^{j-1}(3\alpha/4)^{u-1}\|\boldsymbol{b}_j^*\|^2\\&\leqslant(4/3)^{j-1}(3\alpha/4)^{(u-1)}(4/3)^{i-j}(3\alpha/4)^{d-u}\|\boldsymbol{b}_i^*\|^2\end{aligned}$$

即 $\|\boldsymbol{b}_j\|^2\leqslant(4/3)^{i-1}(3\alpha/4)^{d-1}\|\boldsymbol{b}_i^*\|^2$.

性质 3 格基 $\boldsymbol{B}=[\boldsymbol{b}_1,\ \cdots,\ \boldsymbol{b}_n]\in\mathbf{R}^{m\times n}$是格$L$的一组$(k,\delta)$原-对偶规约基, $n=hk$, 有 $\|\boldsymbol{b}_1\|\leqslant(4/3)^{\frac{n-1}{4}}(3\alpha/4)^{\frac{h-1}{4}}\det(L)^{1/n}$, 其中, $\alpha=1/(\delta-\frac{1}{4})$.

证: 由性质 2, 取$j=1$, 然后把 i 从 1 取到 n 的不等式连乘得 $\|\boldsymbol{b}_1\|^{2n}\leqslant(4/3)^{\sum_{i=1}^{n}(i-1)}(3\alpha/4)^{k(\sum_{d=1}^{h}(d-1))}\prod_{i=1}^{n}\|\boldsymbol{b}_i^*\|^2=(4/3)^{\frac{n-1}{2}n}(3\alpha/4)^{\frac{h-1}{2}n}\det(L)^2$, 得证.

性质 4 格基 $\boldsymbol{B}=[\boldsymbol{b}_1,\ \cdots,\ \boldsymbol{b}_n]\in\mathbf{R}^{m\times n}$是格$L$的一组$(k,\delta)$原-对偶规约基, $n=hk$, 有

$$\det(L)\leqslant\prod_{i=1}^{n}\|\boldsymbol{b}_i\|\leqslant(4/3)^{\frac{n(n-1)}{4}}(3\alpha/4)^{\frac{n(n-1)}{4}}\det(L),$$

其中, $\alpha=1/(\delta-\frac{1}{4})$.

证: 左边的不等式为 Hadamard 不等式[11], 只需证右边的不等式.

由性质 2, 取 $j=i$, 然后把 i 从 1 取到 n 的不等式

连乘得

$$\prod_{i=1}^{n}\|\boldsymbol{b}_i\|^2 \leqslant (4/3)^{\sum_{i=1}^{n}(i-1)}(3\alpha/4)^{k(\sum_{d=1}^{h}(d-1))}\prod_{i=1}^{n}\|\boldsymbol{b}_i^*\|^2$$

$$= (4/3)^{\frac{n-1}{2}n}(3\alpha/4)^{\frac{h-1}{2}n}\det(L)^2,\ \text{得证.}$$

比值$\prod_{i=1}^{n}\|\boldsymbol{b}_i\|/\det(L)$定义为格基的正交亏损(orthogonality defect). 显然, 正交亏损不会小于1, 当且仅当格基向量均相互垂直时, 正交亏损取1.

性质**5**　格基$\boldsymbol{B}=[\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n]\in\mathbf{R}^{m\times n}$是格$L$的一组$(k, \delta)$原-对偶规约基, $n=hk$, 对$\forall \boldsymbol{x}\in L(\boldsymbol{B})-\{\boldsymbol{o}\}$, 有$\|\boldsymbol{b}_1\|\leqslant(4/3)^{\frac{n-1}{2}}(3\alpha/4)^{\frac{h-1}{2}}\|\boldsymbol{x}\|$, 其中, $\alpha=1/(\delta-\frac{1}{4})$.

证: 令$\boldsymbol{x}=\sum_{i=1}^{n}x_i\boldsymbol{b}_i=\sum_{i=1}^{n}x_i^*\boldsymbol{b}_i^*$, 这里$x_i\in\mathbf{Z}$, $x_i^*\in\mathbf{R}$记$i_{\max}=\max_{1\leqslant i\leqslant n}\{x_i\neq0\}$, 则对$i>i_{\max}$, 有$x_i^*=0$, 由$\boldsymbol{b}_i^*$的定义易知$x_{i_{\max}}^*=x_{i_{\max}}\neq0$, 因此

$$\|\boldsymbol{x}\|^2\geqslant(x_{i_{\max}}^*)^2\|\boldsymbol{b}_{i_{\max}}^*\|^2\geqslant\|\boldsymbol{b}_{i_{\max}}^*\|^2$$

再由性质2, 可得

$$\|\boldsymbol{b}_1\|^2\leqslant(4/3)^{i_{\max}-1}(3\alpha/4)^{\lceil i_{\max}/k\rceil-1}\|\boldsymbol{b}_{i_{\max}}^*\|^2$$
$$\leqslant(4/3)^{n-1}(3\alpha/4)^{h-1}\|\boldsymbol{b}_{i_{\max}}^*\|^2$$
$$\leqslant(4/3)^{n-1}(3\alpha/4)^{h-1}\|\boldsymbol{x}\|^2,\ \text{得证.}$$

性质**6**　格基$\boldsymbol{B}=[\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n]\in\mathbf{R}^{m\times n}$是格$L$的一组$(k, \delta)$原-对偶规约基, $n=hk$, 任给格L上t个线性无关向量$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t$, 对$1\leqslant i\leqslant t$有

$$\|\boldsymbol{b}_i\|\leqslant(4/3)^{\frac{n-1}{2}}(3\alpha/4)^{\frac{h-1}{2}}\max\{\|\boldsymbol{x}_1\|, \|\boldsymbol{x}_2\|, \ldots, \|\boldsymbol{x}_t\|\}$$

其中, $\alpha=1/(\delta-\frac{1}{4})$.

证: 令$\boldsymbol{x}_i=\sum_{j=1}^{n}x_{ij}\boldsymbol{b}_i$, $i=1, 2, \ldots, t$, 记$j_{i\text{-}\max}=\max_{1\leqslant j\leqslant n}\{x_{ij}\neq0\}$, 由性质5的证明过程知$\|\boldsymbol{b}_{j_{i\text{-}\max}}^*\|^2\leqslant\|\boldsymbol{x}_i\|^2$. 按$j_{1\text{-}\max}\leqslant j_{2\text{-}\max}\leqslant\ldots\leqslant j_{t\text{-}\max}$重新排序$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t$. $\forall i\in\{1, 2, \ldots, t\}$, 由于$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_i$线性无关, 因此, 必有$i\leqslant j_{i\text{-}\max}$. 再由性质2, 可得

$$\|\boldsymbol{b}_i\|^2\leqslant(4/3)^{j_{i\text{-}\max}-1}(3\alpha/4)^{\lceil j_{i\text{-}\max}/k\rceil-1}\|\boldsymbol{b}_{j_{i\text{-}\max}}^*\|^2$$
$$\leqslant(4/3)^{n-1}(3\alpha/4)^{h-1}\|\boldsymbol{b}_{j_{i\text{-}\max}}^*\|^2$$
$$\leqslant(4/3)^{n-1}(3\alpha/4)^{h-1}\max\{\|\boldsymbol{x}_1\|^2, \|\boldsymbol{x}_2\|^2, \ldots, \|\boldsymbol{x}_t\|^2\},\ \text{得证.}$$

4　原-对偶规约基与连续最小元

本节首先分析原-对偶规约基向量与连续最小元的关系不等式, 然后再分析原-对偶规约基GSO向量与连续最小元的关系不等式.

定理**1**[4]　格基$\boldsymbol{B}=[\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n]=\boldsymbol{QR}\in\mathbf{R}^{m\times n}$是格$L$的一组$(k, \delta)$原-对偶规约基$(\delta\in(1/4, 1])$, $n=hk$, 则有$\|\boldsymbol{b}_1\|^2\leqslant(\alpha\gamma_k^2)^{h-1}\lambda_1^2(L)$, 其中, γ_k为Hermite常数, $\alpha=1/(\delta-\frac{1}{4})$.

证: 由$\boldsymbol{R}_l$和其对偶$\boldsymbol{R}_l'$都是HKZ规约的, 易得$\lambda_1^2(L(\boldsymbol{R}_l'))/D_l'^{1/k}=D_l^{1/k}/r_{kl, kl}^2\leqslant\gamma_k$, 即$D_l^{1/k}\leqslant\gamma_k r_{kl, kl}^2=\gamma_k/\lambda_1^2(L(\boldsymbol{R}_l'))$.

由$\boldsymbol{R}_{l+1}$是HKZ规约的得$\lambda_1^2(L(\boldsymbol{R}_{l+1}))=r_{kl+1, kl+1}^2\leqslant\gamma_k D_{l+1}^{1/k}$.

合并上两式和定义1条件2, 得$D_l^{1/k}\leqslant\alpha\gamma_k^2 D_{l+1}^{1/k}$, $l=1, \ldots, h-1$.

因为$\boldsymbol{R}_1$是HKZ规约的, 所以有$\|\boldsymbol{b}_1\|^2\leqslant\gamma_k D_1^{1/k}\leqslant\gamma_k(\alpha\gamma_k^2)^{l-1}D_l^{1/k}$, $l=1, \ldots, h$, 把l从1到h的不等式相乘, 取h次根, 得$\|\boldsymbol{b}_1\|^2\geqslant\gamma_k(\alpha\gamma_k^2)^{\frac{h-1}{2}}\det(L)^{2/n}$.

同理, 对偶基$\boldsymbol{B}'$有$\|\boldsymbol{b}_1'\|^2\leqslant\gamma_k(\alpha\gamma_k^2)^{l-1}(D_l')^{1/k}$, $l=1, \ldots, h$, 即得$r_{n, n}^2\geqslant\gamma_k^{-1}(\alpha\gamma_k^2)^{-(l-1)}(D_{h-l})^{1/k}$, $l=1, \ldots, h$, 把l从1到h的不等式相乘, 取h次根, 得$r_{n, n}^2\geqslant\gamma_k^{-1}(\alpha\gamma_k^2)^{-\frac{h-1}{2}}\det(L)^{2/n}$.

所以$\|\boldsymbol{b}_1\|^2\leqslant\gamma_k^2(\alpha\gamma_k^2)^{h-1}r_{n, n}^2$. 该结论可以推广到格$L$的子格$L_s=[\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{kl}]$, $l=1, \ldots, h-1$上, 得

$$\|\boldsymbol{b}_1\|^2\leqslant\gamma_k^2(\alpha\gamma_k^2)^{(l-1)-1}r_{kl, kl}^2\leqslant(\alpha\gamma_k^2)^{l-1}r_{kl+1, kl+1}^2,$$
$$l=1, \ldots, h-1$$

另一方面, 设格L的最短向量$\boldsymbol{x}=\sum_{j=1}^{n}x_j\boldsymbol{b}_j\neq0$, 设$x_{\max}=\max\{j\mid x_j\neq0\}$.

当$x_{\max}\leqslant k$时, 显然有$\|\boldsymbol{b}_1\|^2=\lambda_1^2\leqslant(\alpha\gamma_k^2)^{h-1}\cdot\lambda_1^2(L)$.

当$kl<x_{\max}\leqslant kl+k$, 有$r_{kl+1, kl+1}^2\leqslant\|\pi_{kl+1}(x)\|^2\leqslant\lambda_1(L)$, 得$\|\boldsymbol{b}_1\|^2\leqslant(\alpha\gamma_k^2)^{h-1}\lambda_1(L)$.

定理**2**　格基$\boldsymbol{B}=[\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n]\in\mathbf{R}^{m\times n}$是格$L$的一组$(k, \delta)$原-对偶规约基$(\delta\in(1/4, 1])$, $n=hk$, 则对$1\leqslant i\leqslant n$有$(4/3)^{1-i}(3\alpha/4)^{1-d}\leqslant\|\boldsymbol{b}_i\|^2/\lambda_i^2(L)\leqslant(4/3)^{n-1}(3\alpha/4)^{h-1}$, 其中, $\alpha=1/(\delta-\frac{1}{4})$, $d=\lceil1/k\rceil$

证: 根据$\lambda_i(L)$的定义知, 在格L中至少有i个线性无关向量的长度不大于$\lambda_i(L)$, 设这i个线性无关向量为$\boldsymbol{x}_i, \ldots, \boldsymbol{x}_i$, 则有$\lambda_i(L)\geqslant\max(\|\boldsymbol{x}_1\|, \ldots, \|\boldsymbol{x}_i\|)$. 由性质6得

$$\|\boldsymbol{b}_i\|^2\leqslant(4/3)^{n-1}(3\alpha/4)^{h-1}\max\{\|\boldsymbol{x}_1\|^2, \|\boldsymbol{x}_2\|^2, \ldots, \|\boldsymbol{x}_i\|^2\}$$
$$\leqslant(4/3)^{n-1}(3\alpha/4)^{h-1}\lambda_i^2(L)$$

右边不等式得证. 下面证左边不等式:

因为$\lambda_i^2(L)\leqslant\max\{\|\boldsymbol{b}_1\|^2, \|\boldsymbol{b}_2\|^2, \ldots, \|\boldsymbol{b}_i\|^2\}$, 所以由性质2得

$$\lambda_i^2(L) \leqslant (4/3)^{i-1}(3\alpha/4)^{d-1} \| \boldsymbol{b}_i^* \|^2 \leqslant (4/3)^{i-1}(3\alpha/4)^{d-1} \| \boldsymbol{b}_i \|^2$$

不等式左边得证.

推论 1 格基 $\boldsymbol{B}=[\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n] \in \mathbf{R}^{m\times n}$ 是格 L 的一组(k, δ)原-对偶规约基$(\delta \in (1/4, 1])$, $n=hk$, 则对 $1 \leqslant i \leqslant n$ 有 $(4/3)^{1-i}(3\alpha/4)^{1-d} \leqslant \| \boldsymbol{b}_i^* \|^2/\lambda_i^2(L) \leqslant (4/3)^{n-1}(3\alpha/4)^{h-1}$, 其中, $\alpha=1/(\delta-\frac{1}{4})$, $d=\lceil i/k \rceil$.

由定理 2 和 $\| \boldsymbol{b}_i^* \|^2 \leqslant \| \boldsymbol{b}_i \|^2$, 易得推论 1.

5 原-对偶规约基上的舍入算法

最近向量问题 CVP 是格论中两个最基本问题之一, Boas 在文献[12]和 Micciancio 在文献[13]分别证明了 CVP 是 NP-难的. 因此, 人们在难题上降低约束条件, 进行近似化处理, 得到近似 CVP 问题. 近似 CVP 问题可以描述为: 给定格 $L(B)$ 和目标向量 $\boldsymbol{t}$, 在格 L 中找出一个向量 $\boldsymbol{x}$, 满足 $\| \boldsymbol{x}-\boldsymbol{t} \| \leqslant \lambda \min_{\boldsymbol{y}\in L} \| \boldsymbol{y}-\boldsymbol{t} \|$, 其中 λ 为近似因子.

基于 LLL 规约基, Babai 在文献[10]给出了一种求解近似 CVP 的舍入算法: 设是格 L 的一组 $\delta=\frac{3}{4}$的 LLL 规约基, $\boldsymbol{x}=\sum_{i=1}^{n} x_i \boldsymbol{b}_i \in \mathrm{span}(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$, 令 $\boldsymbol{v}=\sum_{i=1}^{n} \lfloor x_i \rceil \boldsymbol{b}_i$, $\boldsymbol{u}$ 是格 L 上离 $\boldsymbol{x}$ 最近点, 则有 $\| \boldsymbol{x}-\boldsymbol{v} \| \leqslant (1+2n(9/2)^{n/2}) \| \boldsymbol{x}-\boldsymbol{u} \|$. 下面分析用原-对偶规约基改进 Babai 的舍入算法.

命题 1 格基 $\boldsymbol{B}=[\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n] \in \mathbf{R}^{m\times n}$ 是格 L 的一组(k, δ)原-对偶规约基, $n=hk$, 对 $\forall t \in \{1, 2, \cdots, n\}$, 有 $\| \boldsymbol{b}_t \|^2 \leqslant 3^{n-1}(3\alpha/4)^{h-1} \| \boldsymbol{x}-\boldsymbol{b}_t \|^2$, 其中, $\alpha=1/(\delta-\frac{1}{4})$, $x \in \mathrm{span}(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_{t-1}, \boldsymbol{b}_{t+1}, \cdots, \boldsymbol{b}_n)$.

证: 设 $\boldsymbol{x}=\sum_{i=1}^{n} x_i \boldsymbol{b}_i=\sum_{i=1}^{n} x_i^* \boldsymbol{b}_i^*$, 由 $\boldsymbol{b}_i^*$ 的定义易得 $\boldsymbol{x}-\boldsymbol{b}_t=\sum_{i=1}^{n} v_i \boldsymbol{b}_i^*$, $v_i=x_i^*-\mu_{ti}$.

Babai 在文献[10]已经证明 $\sum_{i\geqslant t} y_i=(2/3)^{2(n-t)}$. 又

$$\| \boldsymbol{x}-\boldsymbol{b}_t \|^2=\sum_{i=1}^{n} v_i^2 \| \boldsymbol{b}_i^* \|^2 \geqslant \sum_{i=s}^{n} v_i^2 \| \boldsymbol{b}_i^* \|^2$$

根据性质 1 有

$$\| \boldsymbol{x}-\boldsymbol{b}_t \|^2 \geqslant \sum_{i=t}^{n} [v_i^2 (4/3)^{-(i-t)}(3\alpha/4)^{-(\lceil i/k \rceil - \lceil t/k \rceil)}] \| \boldsymbol{b}_t^* \|^2$$

$$\geqslant (4/3)^{-(n-t)}(3\alpha/4)^{-(\lceil n/k \rceil - \lceil t/k \rceil)} \| \boldsymbol{b}_t^* \|^2 \sum_{i=t}^{n} y_i^2$$

$$= (2/3)^{2(n-t)}(4/3)^{-(n-t)}(3\alpha/4)^{-(\lceil n/k \rceil - \lceil t/k \rceil)} \| \boldsymbol{b}_t^* \|^2$$

$$= (1/3)^{n-t}(3\alpha/4)^{-(\lceil n/k \rceil - \lceil t/k \rceil)} \| \boldsymbol{b}_t^* \|^2$$

再根据性质 2 有

$$\| \boldsymbol{b}_t \|^2 \leqslant (4/3)^{t-1}(3\alpha/4)^{\lceil t/k \rceil - 1} \| \boldsymbol{b}_t^* \|^2$$

$$\leqslant (4/3)^{t-1}(3\alpha/4)^{\lceil t/k \rceil - 1} 3^{n-t}(3\alpha/4)^{\lceil n/k \rceil - \lceil t/k \rceil} \| \boldsymbol{x}-\boldsymbol{b}_t \|^2$$

$$= (4/3)^{t-1}(1/3)^{t-1} 3^{n-1}(3\alpha/4)^{h-1} \| \boldsymbol{x}-\boldsymbol{b}_t \|^2$$

$$\leqslant 3^{n-1}(3\alpha/4)^{h-1} \| \boldsymbol{x}-\boldsymbol{b}_t \|^2$$

定理 3 格基 $\boldsymbol{B}=[\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n] \in \mathbf{R}^{m\times n}$ 是格 L 的一组(k, δ)原-对偶规约基$(\delta \in (1/4, 1])$, $n=hk$, $x=\sum_{i=1}^{n} x_i \boldsymbol{b}_i \in \mathrm{span}(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$, 令 $\boldsymbol{v}=\sum_{i=1}^{n} \lfloor x_i \rceil \boldsymbol{b}_i$, $\boldsymbol{u}$ 是格 L 上离 $\boldsymbol{x}$ 最近点, 则有 $\| \boldsymbol{x}-\boldsymbol{v} \| \leqslant (1+(2n)3^{\frac{n-1}{2}}(3\alpha/4)^{\frac{h-1}{2}}) \| \boldsymbol{x}-\boldsymbol{u} \|$, 其中 $\alpha=1/(\delta-\frac{1}{4})$.

证: 要证 $\| \boldsymbol{x}-\boldsymbol{v} \| \leqslant (1+(2n)3^{\frac{n-1}{2}}(3\alpha/4)^{\frac{h-1}{2}}) \| \boldsymbol{x}-\boldsymbol{u} \|$, 只需证 $\| \boldsymbol{u}-\boldsymbol{v} \| \leqslant (2n)3^{\frac{n-1}{2}}(3\alpha/4)^{\frac{h-1}{2}} \| \boldsymbol{x}-\boldsymbol{u} \|$.

记 $\boldsymbol{v}-\boldsymbol{x}=\sum_{i=1}^{n} a_i \boldsymbol{b}_i$, 则 $a_i=\lfloor x_i \rceil - x_i$, $-1/2 \leqslant a_i \leqslant 1/2$.

因 $\boldsymbol{u}, \boldsymbol{v}$ 均为格 L 上的点, 所以 $\boldsymbol{u}-\boldsymbol{v}$ 也是格 L 上的点, 记 $\boldsymbol{u}-\boldsymbol{v}=\sum_{i=1}^{n} e_i \boldsymbol{b}_i$, 其中 $e_i \in \mathbf{Z}$.

记 $\| e_m \boldsymbol{b}_m \| = \max_{1\leqslant i\leqslant n} \| e_i \boldsymbol{b}_i \|$, 则有 $\| \boldsymbol{u}-\boldsymbol{v} \| = n \| e_m \boldsymbol{b}_m \|$.

当 $e_m=0$ 时, 不等式 $\| \boldsymbol{u}-\boldsymbol{v} \| \leqslant (2n)3^{\frac{n-1}{2}}(3\alpha/4)^{\frac{h-1}{2}} \| \boldsymbol{x}-\boldsymbol{u} \|$ 显然成立.

当 $e_m \neq 0$ 时, $e_m+a_m \neq 0$, $|e_m+a_m| \geqslant \frac{|e_m|}{2}$,

$$\boldsymbol{u}-\boldsymbol{x}=(\boldsymbol{u}-\boldsymbol{v})+(\boldsymbol{v}-\boldsymbol{x})=\sum_{i=1}^{n}(e_i+a_i)\boldsymbol{b}_i$$

$$=(e_m+a_m)\left(\boldsymbol{b}_m-\left(-\frac{1}{e_m+a_m}\sum_{i=1, i\neq m}^{n}(e_i+a_i)\boldsymbol{b}_i\right)\right)$$

记 $\boldsymbol{y}=-\frac{1}{e_m+a_m}\sum_{i=1, i\neq m}^{n}(e_i+a_m)\boldsymbol{b}_i$, 有 $\boldsymbol{y} \in \mathrm{span}(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_{m-1}, \boldsymbol{b}_{m+1}, \cdots, \boldsymbol{b}_n)$, 根据命题 1 有

$$\| \boldsymbol{u}-\boldsymbol{x} \| = |e_m+a_m| \| \boldsymbol{b}_m-\boldsymbol{y} \| \geqslant \frac{|e_m|}{2} 3^{-\frac{n-1}{2}}(3\alpha/4)^{-\frac{h-1}{2}} \| \boldsymbol{b}_m \|$$

$$= \frac{|e_m|}{2} 3^{-\frac{n-1}{2}}(3\alpha/4)^{-\frac{h-1}{2}} \frac{1}{n|e_m|} \| \boldsymbol{u}-\boldsymbol{v} \|$$

即 $\| \boldsymbol{u}-\boldsymbol{v} \| \leqslant (2n)3^{\frac{n-1}{2}}(3\alpha/4)^{\frac{h-1}{2}} \| \boldsymbol{u}-\boldsymbol{v} \|$, 得证.

可见, 当 δ 取 $\frac{3}{4}$, $\alpha=2$ 时, 用原-对偶规约基改进 Babai 的舍入算法, 可以提高原算法的近似因子.

6 结论

近年来, 虽然许多研究人员都在致力于寻找高维格的多项式或近多项式时间规约基, 但是比较有名的规约

基只有极少几个[14]. Koy 提出的原-对偶规约基是一种近多项式时间规约基,比 LLL 规约基具有更紧的约束条件,更好的质量. 本文把 LLL 规约基的一些性质推广到原-对偶规约基上,取得规约基六个实用的性质不等式. 规约基与连续最小元比值是衡量规约算法质量的一项重要指标,多数规约基都已对该项指标进行了论证,如文献[7~9]. 本文在 Koy 给出的原-对偶规约基长度亏损上界的基础上,进一步给出原-对偶规约基与连续最小元比值因子的上界和下界,证明原-对偶规约基满足 $(4/3)^{1-i}(3\alpha/4)^{1-\lceil i/k\rceil} \leqslant \|\boldsymbol{b}_i\|^2/\lambda_i^2(L) \leqslant (4/3)^{n-1}(3\alpha/4)^{n/k-1}$, 其中, $\alpha = 1/(\delta - \frac{1}{4})$. 作为一个应用实例,本文用原-对偶规约基改进 Babai 的近似 CVP 算法,证明在原-对偶规约基上舍入算法近似因子为 $(1+(2n)3^{\frac{n-1}{2}}(3\alpha/4)^{\frac{n/k-1}{2}})$, 当 δ 取 $\frac{3}{4}$, $\alpha = 2$ 时,比 Babai 的舍入算法约提高了 $\frac{3\sqrt{2}}{2}\left(\frac{3}{2}\right)^{(1-1/k)\frac{n}{2}}$ 倍. Lagarias 等人在文献[7]中给出 HKZ 规约基与连续最小元比值因子上界和下界的同时,举例论证了它们是不能再提高的、紧的界. 本文没有进一步论证所给原-对偶规约基与连续最小元比值因子的上界和下界是不能提高的、紧的界.

参考文献:

[1] P Nguyen, J Stern. Lattice reduction in cryptology: An update [A]. W. Bosma. Algorithmic Number Theory-Proceedings of ANTS-IV, Lecture Notes in Computer Science, vol. 1838[C]. Berlin: Springer-Verlag, 2000. 85– 112.

[2] C P Schnorr. A hierarchy of polynomial lattice basis reduction algorithms[J]. Theoretical Computer Science, 1987, 53(2): 201– 224.

[3] H Koy. Primal/duale Segment-Reduktion von Gitterbasen[EB/OL]. http://www.mi.informatik.unifrankfurt.de/research/papers.html.

[4] C P Schnorr. Blockwise Lattice Basis Reduction Revisited[EB/OL]. http://www.mi.informatik.unir frankfurt.de/research/papers.html.

[5] C P Schnorr. Fast LLL-type lattice reduction[J]. Information and Computation, 2006, 204(1): 1– 25.

[6] K Mahler. A theorem on inhomogeneous diophantine inequalities[J]. Nederl Akad Wetensch, Proc, 1938, 4: 634– 637.

[7] J C Lagarias, H W Lenstra, C P Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice[J]. Combinatorica, 1990, 10(4): 333– 348.

[8] A K Lenstra, H W Lenstra, L Lovász. Factoring polynomials with rational coefficients[J]. Math Ann, 1982, 261: 515– 534.

[9] C P Schnorr. Block reduced lattice bases and successive minima [J]. Combinatorics, Probability and Computing, 1994, (3): 507– 533.

[10] L Babai. On Lovász lattice reduction and the nearest lattice point broblem[J]. Combinatorica, 1986, 6(1): 1– 13.

[11] H Cohen. A Course in Computational Algebraic Number Theory[M]. Berlin: Springer-Verlag, 1995. 84– 90.

[12] P van Emde Boas. Another NP-Complete Problem and the Complexity of Computing Short Vectors in a Lattice[R]. Amsterdam: Mathematics Department, University of Amsterdam, 1981.

[13] Micciancio D. The hardness of the closest vector problem with preprocessing[J]. IEEE Transactions on Information Theory, 2001, 47(3): 1212– 1215.

[14] N Gama, N Howgrave-Graham, H Koy, et al. Rankin's constant and blockwise lattice reduction[A]. Proc CRYPTO'2006, LNCS[C]. Berlin: Springer-Verlag, 2006. 112– 130.

作者简介:

谢朝海　男, 1973 年生于广西,博士研究生. 主要研究方向为网络信息安全技术、信息安全等级保护理论与技术、密码分析技术.

E-mail: xiech@cspec.gov.cn

陶　然　男,1964 年生于安徽,教授,博士生导师. 主要研究方向为现代信号处理理论及应用、雷达系统与技术、通信系统与技术、高速实时信号处理、信息安全与对抗理论与技术.

王　越　男, 1932 年生于江苏,中国科学院院士,中国工程院院士,博士生导师. 主要研究方向为系统理论与复杂电子系统设计、通信理论与技术、网络信息安全.

李继勇　男,1974 年生于贵州,博士研究生. 主要研究方向为网络信息安全技术、密码技术.