中国科学: 数学 2010 年 第 40 卷 第 8 期: 723～730
www.springerlink.com math.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

格中依次最短无关组与 Minkowski 约化基等价的充分条件

王源华[①*], 尚士魁[②], 高峰[③], 黄民强[④]

① 中国科学院数学与系统科学研究院数学研究所, 北京 100190;
② 中国科学技术大学数学系, 合肥 230026;
③ 中国科学技术大学电子工程与信息科学系, 合肥 230027;
④ 中国科学院数学与系统科学研究院系统科学研究所, 北京 100190
E-mail: wangyh@amss.ac.cn

收稿日期: 2010-05-04; 接受日期: 2010-06-29; * 通信作者

摘要 本文讨论了格中基子集、依次最短无关组及 Minkowski 约化基之间的向量长度关系, 利用无关组与基之间的一些制约性质, 给出了 Minkowski 约化基达到依次最短长度, 以及依次最短无关组成为 Minkowski 约化基的一些充分条件.

关键词 格 依次最短长度 依次最短无关组 Minkowski 约化基

MSC (2000) 主题分类 11H50,11H55

1 引言

欧氏空间 $\mathbb{R}^m$ 中一个 n 维格 Λ 是线性无关向量组 $B=\{b_1,\ldots,b_n\}$ 的整系数线性组合的集合, 即 $\Lambda=\mathbb{Z}b_1\oplus\cdots\oplus\mathbb{Z}b_n=\{\sum_{i=1}^n x_ib_i \mid x_i\in\mathbb{Z}, 1\leqslant i\leqslant n\}$, B 称为 Λ 的一组基. 当 $n>1$ 时，格 Λ 有无穷多组基, 它们之间的变换矩阵构成了整系数一般线性群 $\mathrm{GL}_n(\mathbb{Z})$.

近年来, 随着对格中计算问题的研究不断深入, 格模型越来越广泛地应用于计算科学的众多领域之中. 例如在计算代数、计算数论以及密码学中, 一些困难问题的构造与求解都基于对格的性质的深刻理解 (详见 [1–3] 等). 其中的核心问题之一, 就是寻找具有较好性质的格基 (即格基约化), 通常是选择基向量长度较短以及基向量之间接近正交的格基.

为方便讨论, 下面列出文中涉及的有关格的一些重要概念和基本事实.

依次最短长度 (Successive Minima) n 维格 Λ 的依次最短长度 $\lambda_1(\Lambda),\ldots,\lambda_n(\Lambda)$ 定义为 (可参见 [4] 或 [1, 第 1 章])

$$\lambda_i(\Lambda):=\inf\{r>0 \mid \overline{B}(0,r)\text{中包含}\Lambda\text{的线性无关向量组}S,\text{满足}|S|\geqslant i\},\quad 1\leqslant i\leqslant n,$$

即 $\lambda_i(\Lambda)$ 是以原点为中心的包含 Λ 中至少 i 个线性无关向量的闭球的最短半径. 依次最短长度是格 Λ 的主要特征之一. 由定义可得, $\lambda_1(\Lambda)\leqslant\cdots\leqslant\lambda_n(\Lambda)$.

依次最短无关组 (SMIV) n 维格 Λ 中的一个有序线性无关组 $S=\{s_1,\ldots,s_k\}$ 称为依次最短无关组, 如果

$$\|s_i\|=\min\{\|s_i'\| \mid s_i'\in\Lambda\text{且与}s_1,\ldots,s_{i-1}\text{线性无关}\},\quad 1\leqslant i\leqslant k.$$

引用格式: Wang Y H, Shang S K, Gao F, et al. Some sufficient conditions of the equivalence between successive minimal independent vectors and Minkowski-reduced basis in lattices (in Chinese). Sci Sin Math, 2010, 40(8): 723–730

由定义易知, $\|s_1\| \leqslant \cdots \leqslant \|s_k\|$. 并且, 显然有

$$\lambda_i(\Lambda) \leqslant \max\{\|s_1\|, \ldots, \|s_i\|\} = \|s_i\|.$$

另一方面, 对 $\forall \varepsilon > 0$, 取 $r = \lambda_i(\Lambda) + \varepsilon$, 由 $\lambda_i(\Lambda)$ 的定义, $\overline{B}(0, r)$ 中包含线性无关的向量组 $\{t_1, \ldots, t_i\}$, 其中必有某个 t_j 与 $s_1, \ldots, s_{i-1}$ 线性无关. 由 SMIV 的定义, 可知 $\|s_i\| \leqslant \|t_j\| \leqslant r = \lambda_i(\Lambda) + \varepsilon$. 令 $\varepsilon \to 0$, 我们得到 $\|s_i\| \leqslant \lambda_i(\Lambda)$, 从而有

命题 1.1 SMIV 中向量的长度是唯一确定的. 若 $\{s_1, \ldots, s_k\}$ 是格 Λ 的一组 SMIV, 则

$$\|s_i\| = \lambda_i(\Lambda), \quad 1 \leqslant i \leqslant k.$$

基子集 格 Λ 中线性无关向量组 $B' = \{b_1, \ldots, b_k\}$ 称为基子集, 如果 B' 能扩张为 Λ 的一组基. 在 [4] 中, 基子集也被称为本原 (primitive) 的向量组. 值得注意的是, Λ 中的线性无关向量组未必构成基子集.

依次最短基子集长度 类似于依次最短长度, 我们定义依次最短基子集长度为

$$\mu_i(\Lambda) := \inf\{r > 0 \mid \bar{B}(0, r)\text{中包含}\Lambda\text{的基子集}S, \text{满足}|S| \geqslant i\}, \quad 1 \leqslant i \leqslant n.$$

这也是格 Λ 的重要特征, 并且显然有 $\mu_1(\Lambda) \leqslant \cdots \leqslant \mu_n(\Lambda)$.

Minkowski 约化基 类似于 SMIV 的定义, n 维格 Λ 的一组有序基 $B = \{b_1, \ldots, b_n\}$ 称为 Minkowski 约化基 (简称为 M- 基), 如果

$$\|b_i\| = \min\{\|b_i'\| \mid b_i' \in \Lambda\text{且}\{b_1, \ldots, b_{i-1}, b_i'\}\text{构成基子集}\}, \quad 1 \leqslant i \leqslant n.$$

M- 基的前 k 个向量, 称为 M- 基子集. 由定义易见, $\|b_1\| \leqslant \cdots \leqslant \|b_n\|$, 并且

$$\lambda_i(\Lambda) \leqslant \mu_i(\Lambda) \leqslant \|b_i\|, \quad 1 \leqslant i \leqslant n.$$

在 M- 基的构造过程中, 基向量 b_i 的选择可能不唯一, 所以格 Λ 的 M- 基是不唯一的. 不过, 文献 [5] 中给出的下述结果表明, Λ 的 M- 基中前 4 个向量的长度是唯一确定的, 就是 $\lambda_1(\Lambda), \ldots, \lambda_4(\Lambda)$.

命题 1.2 设 $B = \{b_1, \ldots, b_n\}$ 是格 Λ 的一组 M- 基, 则

$$\|b_i\| = \lambda_i(\Lambda) = \mu_i(\Lambda), \quad 1 \leqslant i \leqslant \min\{4, n\}.$$

但当 $i \geqslant 5$ 时, 三个长度却不是无条件相等的 (例 1.3, 见 [1, 第 7 章]). 而且, Ryskov 的工作表明, 当维数 $\geqslant 7$ 时, 存在格 Λ, 其不同 M- 基中对应向量的长度也是不一致的 (详见 [6]).

例 1.3 设 $n \geqslant 4$, Λ 是欧氏空间 $\mathbb{R}^n$ 中由 $b_i = 2e_i\,(1 \leqslant i \leqslant n-1)$ 和 $b_n = (1, \ldots, 1)^{\mathrm{T}}$ 张成的 n 维格. 易知 $B' = \{2e_1, \ldots, 2e_n\}$ 是 Λ 中达到 $\lambda_i(\Lambda) = 2\,(1 \leqslant i \leqslant n)$ 的一组 SMIV, 但却不是 Λ 的基. 另一方面, Λ 的任一组基中必有一个坐标全为奇数的向量 b, 当 $n \geqslant 5$ 时, $\|b\| \geqslant \sqrt{n} > \lambda_n(\Lambda) = 2$.

事实上, 当 $i \geqslant 5$ 时, 格 Λ 中 M- 基中向量 b_i 的长度达到 $\lambda_i(\Lambda)$ 的条件以及 SMIV 成为基子集的条件都是开放性的问题. 本文通过对格中的线性无关组与相关基子集之间关系的研究, 证明了一个关键引理 (Key Lemma). 利用这一结果, 我们给出了 $i \geqslant 5$ 时 M- 基中向量 b_i 能够达到 $\lambda_i(\Lambda)$ 的一些充分条件. 同样基于该引理, 我们讨论了 SMIV 成为 M- 基子集的条件, 证明了由 3 个向量组成的 SMIV 一定是 M- 基子集, 而 4 个向量的 SMIV 若不构成 M- 基子集, 只能是极特殊的一种情况, 并给出了多于 4 个向量的 SMIV 成为 M- 基子集的充分条件. 最后, 综合起来给出 SMIV 与 M- 基子集等价的几个充分条件.

2 关键引理

关键引理的证明中需要用到下面两个引理. 首先, 通过对整系数矩阵做初等行变换, 应用带余除法可得

引理 2.1 ([7, 第 2 章], 满秩整系数方阵的 Hermite 正规型 HNF) 设 $M \in \mathbb{Z}^{n\times n}$ 是一个满秩方阵, 则存在 $U \in \mathrm{GL}_n(\mathbb{Z})$, 使得 $M = UH$, 这里 $H = (h_{ij})$ 是一个非负整数系数上三角方阵, 其非对角元均小于所在列的对角元. 这样, 若对某个 i 有 $h_{ii} = 1$, 则其所在列为 $\mathbb{R}^n$ 的第 i 个单位列向量 e_i. 这样的 H 称为 (方阵 M 的) Hermite 正规型.

引理 2.2 设 $B = \{b_1, \ldots, b_n\}$ 是欧氏空间中一组线性无关向量, $B^* = \{b_1^*, \ldots, b_n^*\}$ 是对 B 作 Gram-Schmidt 正交化后得到的正交向量组, 则对任意 $x \in \mathrm{span}_{\mathbb{R}}(B)$, 存在格点 $a \in \mathrm{span}_{\mathbb{Z}}(B)$, 使得

$$x - a = \sum_{i=1}^{n} \beta_i b_i^*, \quad \beta_i \in \mathbb{R},$$

满足 $|\beta_i| \leqslant 1/2$ 对所有 $1 \leqslant i \leqslant n$ 都成立.

证明 设 $x = \sum_{i=1}^{n} \alpha_i b_i^* \in \mathrm{span}_{\mathbb{R}}(B)$, 令 $a_n = \lceil \alpha_n \rfloor$ 为距 α_n 最近的整数, $x' = x - a_n b_n = \sum_{i=1}^{n} \alpha_i' b_i^*$, 由于 b_n^* 是 b_n 在 $\mathrm{span}_{\mathbb{R}}\{b_1^*, \ldots, b_{n-1}^*\}^{\perp}$ 上的投影, 故有

$$|\alpha_n'| = \left| \frac{\langle x', b_n^* \rangle}{\|b_n^*\|^2} \right| = |\alpha_n - a_n| \leqslant \frac{1}{2}.$$

依次对下标 $i = n-1, n-2, \ldots, 1$ 实施上述逼近, 便得引理结果. □

这种逐步改变目标向量使得它对 Gram-Schmidt 正交基的系数的绝对值 $\leqslant 1/2$ 的方法, 一般叫做规模约化 (size-reduction). 许多格基约化算法中, 例如著名的 LLL 算法, 都需利用该方法对格基进行约化.

下面的引理是证明本文主要结果的基础.

引理 2.3 (关键引理) 设 Λ 是一个 n 维格, $S = \{s_1, \ldots, s_k\}$ 是 Λ 中线性无关的向量组, 则存在 Λ 的一个基子集 $R = \{r_1, \ldots, r_k\}$ 和对角元为正整数的整系数上三角方阵 $T \in \mathbb{Z}^{k\times k}$ 使得 $S = RT$. 进一步, 设 $S^* = \{s_1^*, \ldots, s_k^*\}$ 和 $R^* = \{r_1^*, \ldots, r_k^*\}$ 分别是 S 和 R 做 Gram-Schmidt 正交化得到的正交向量组, 则有 $s_i^* = t_{ii} r_i^*$, 并且对任意的 $1 \leqslant i \leqslant k$,

(1) 若 $t_{ii} = 1$, 则 $r_i = s_i$;

(2) 否则 $t_{ii} \geqslant 2$, 并且

$$\|r_i\| \leqslant \sqrt{\sum_{j=1}^{i-1} \frac{\|s_j^*\|^2}{4} + \frac{\|s_i^*\|^2}{t_{ii}^2}} \leqslant \frac{\sqrt{\sum_{j=1}^{i} \|s_j^*\|^2}}{2} \leqslant \frac{\sqrt{\sum_{j=1}^{i} \|s_j\|^2}}{2}.$$

证明 只需证明 $k = n$ 的情形. 当 $k < n$ 时, 将 S 扩展为 Λ 中 n 个线性无关向量即可.

首先, 任取格 Λ 的一组基 $R' = \{r_1', \ldots, r_n'\}$, 则存在整系数矩阵 $T' \in \mathbb{Z}^{n\times n}$ 使得 $S = R'T'$. 由于 S 是线性无关的, $\det(T') \neq 0$, 即 T' 是满秩的. 根据引理 2.1, 存在 $U \in \mathrm{GL}_n(\mathbb{Z})$, 使得 $T' = UT$, T 为方阵 T' 的 Hermite 正规型. 令 $R = R'U$, 则 $R = \{r_1, \ldots, r_n\}$ 也是格 Λ 的基, 并且有

$$S = R'T' = R'UT = RT.$$

这样,

$$\mathrm{span}_{\mathbb{R}}\{s_1, \ldots, s_i\} = \mathrm{span}_{\mathbb{R}}\{r_1, \ldots, r_i\}, \quad 1 \leqslant i \leqslant n.$$

而 S^* 和 R^* 是由 S 和 R 做 Gram-Schmidt 正交化得到的, 所以

$$\mathrm{span}_{\mathbb{R}}\{s_1^*,\dots,s_i^*\}=\mathrm{span}_{\mathbb{R}}\{r_1^*,\dots,r_i^*\},\quad 1\leqslant i\leqslant n.$$

由于 s_i^* 和 r_i^* 分别为 s_i 和 r_i 在 $\mathrm{span}_{\mathbb{R}}\{r_1^*,\dots,r_{i-1}^*\}^{\perp}$ 中的投影, 故对所有的 $1\leqslant i\leqslant n$, 有 $s_i^*=t_{ii}r_i^*$. 依次对 $i=1,\dots,n$, 根据 T 的对角元的情况, 调整基向量 r_i 如下:

(1) 当 $t_{ii}=1$ 时, 由引理 2.1, T 的第 i 列为单位向量 e_i, 即 $r_i=s_i$. 此时不做调整.

(2) 否则, 便有 $t_{ii}\geqslant 2$. 设 $u=r_i-r_i^*$, 则 $u\in\mathrm{span}_{\mathbb{R}}\{s_1,\dots,s_{i-1}\}$. 由引理 2.2, 存在格点

$$v\in\mathbb{Z}s_1\oplus\cdots\oplus\mathbb{Z}s_{i-1}\subseteq\mathbb{Z}r_1\oplus\cdots\oplus\mathbb{Z}r_{i-1},$$

使得 $u-v=\sum_{j=1}^{i-1}\beta_j s_j^*$, 满足 $|\beta_j|\leqslant 1/2$. 从而

$$\|u-v\|^2=\sum_{j=1}^{i-1}\beta_j^2\|s_j^*\|^2\leqslant\sum_{j=1}^{i-1}\frac{\|s_j^*\|^2}{4}.$$

令 $r_i'=r_i-v$, 由 $r_i^*\perp(u-v)$ 知

$$\|r_i'\|^2=\|r_i^*+u-v\|^2=\|u-v\|^2+\|r_i^*\|^2\leqslant\sum_{j=1}^{i-1}\frac{\|s_j^*\|^2}{4}+\frac{\|s_i^*\|^2}{t_{ii}^2}.$$

用 r_i' 代替 r_i, 则 $\{r_1,\dots,r_{i-1},r_i',r_{i+1},\dots,r_n\}$ 仍然是 Λ 的一组基, 不妨仍记为 R. 此时, S 对 R 的坐标矩阵 T 中只有从 i 列起的前 $i-1$ 行的元素可能发生变化, 且第 i 列以后的单位向量所在列不变. 因此, 整系数矩阵 T 对指标 $j\leqslant i$, 都满足了引理结论.

依次而为, 逐步调整基向量, 最终便构造出对所有的 i 都满足条件 (1) 和 (2) 的 Λ 的一组基. □

推论 2.4 在关键引理中, 若向量组 $S=\{s_1,\dots,s_k\}$ 的前 $k-1$ 个向量构成基子集, 则可取基子集 $R=\{s_1,\dots,s_{k-1},r_k\}$ 和前 $k-1$ 列为单位向量的矩阵 T, 使得 $S=RT$, 并满足相应的结论. 进一步地, 若 S 不是基子集, 则

$$\|r_k\|\leqslant\sqrt{\sum_{i=1}^{k-1}\frac{\|s_i^*\|^2}{4}+\frac{\|s_k^*\|^2}{t_{kk}^2}}\leqslant\frac{\sqrt{\sum_{i=1}^{k}\|s_i^*\|^2}}{2}\leqslant\frac{\sqrt{\sum_{i=1}^{k}\|s_i\|^2}}{2}\leqslant\frac{\sqrt{k}}{2}\max\{\|s_i\|\mid 1\leqslant i\leqslant k\}.$$

证明 在关键引理证明中, 取向量 r_k' 使得 $R=\{s_1,\dots,s_{k-1},r_k'\}$ 是格 Λ 的初始基子集, 则 S 关于 R 的坐标矩阵的前 $k-1$ 列已经是单位向量. 因此, 只需要把最后的 r_k' 调整为 r_k. 这样, 当 S 不是基子集时, $t_{kk}\geqslant 2$, 得到的 r_k 便满足结论. □

注记 由推论 2.4, 即可推得命题 1.2.

3 Minkowski 约化基的向量长度达到 λ_i 的充分条件

由例 1.3 可知, $n\geqslant 5$ 时 M- 基的向量不一定能达到依次最短长度. 而本节的讨论表明, 如果格的依次最短长度有较显著的递增变化, 其 M- 基的向量长度便能达到依次最短长度.

定理 3.1 设 $n\geqslant 5$, 如果 n 维格 Λ 满足 $\sum_{i=1}^{j-1}\lambda_i(\Lambda)^2\leqslant 3\lambda_j(\Lambda)^2$ (记为条件 C_j), 对 $5\leqslant j\leqslant k$ 都成立, 则对 Λ 的任一 M- 基子集 $\{b_1,\dots,b_k\}$, 有

$$\|b_j\|=\lambda_j(\Lambda)=\mu_j(\Lambda),\quad 1\leqslant j\leqslant k.$$

证明 应用归纳法. 由命题 1.2, 当 $1 \leqslant j \leqslant 4$ 时, 结论成立. 假设结论对 $1 \leqslant j \leqslant k-1$ 都成立, 此时 $\{b_1, \ldots, b_{k-1}\}$ 是一组 SMIV, 取 $b'_k \in \Lambda$, 使得 $\{b_1, \ldots, b_{k-1}, b'_k\}$ 也构成一组 SMIV, 则 $\|b'_k\| = \lambda_k(\Lambda)$.

(1) 如果 $\{b_1, \ldots, b_{k-1}, b'_k\}$ 是一个基子集, 则有

$$\|b_k\| \leqslant \|b'_k\| = \lambda_k(\Lambda) \leqslant \mu_k(\Lambda) \leqslant \|b_k\|.$$

(2) 否则, 由推论 2.4 及条件 C_k, 存在基子集 $\{b_1, \ldots, b_{k-1}, r_k\}$ 使得

$$\|r_k\| \leqslant \frac{\sqrt{\sum_{i=1}^{k-1} \|b_i\|^2 + \|b'_k\|^2}}{2} = \frac{\sqrt{\sum_{i=1}^{k} \lambda_i(\Lambda)^2}}{2} \leqslant \frac{\sqrt{4\lambda_k(\Lambda)^2}}{2} = \lambda_k(\Lambda),$$

因此, 由 M- 基的定义得

$$\|b_k\| \leqslant \|r_k\| \leqslant \lambda_k(\Lambda) \leqslant \mu_k(\Lambda) \leqslant \|b_k\|.$$

综合 (1) 和 (2), 当 $j = k$ 时, 结论也成立. 由归纳法可得定理成立. □

进一步, 我们可得更简洁的充分条件如下.

定理 3.2 对 $n \geqslant 5$, 如果 n 维格 Λ 满足 $\frac{\lambda_{j-1}(\Lambda)}{\lambda_j(\Lambda)} \leqslant \frac{\sqrt{3}}{2}$, 对 $5 \leqslant j \leqslant k$ 都成立, 则对 Λ 的任一 M-基子集 $\{b_1, \ldots, b_k\}$, 有

$$\|b_j\| = \lambda_j(\Lambda) = \mu_j(\Lambda), \quad 1 \leqslant j \leqslant k.$$

证明 首先, 当 $j = 5$ 时, 有

$$\sum_{i=1}^{4} \lambda_i(\Lambda)^2 \leqslant 4\lambda_4(\Lambda)^2 \leqslant 3\lambda_5(\Lambda)^2,$$

即条件 C_5 是成立的. 归纳假设当条件 C_{j-1} 成立时, 由 $\frac{\lambda_{j-1}(\Lambda)}{\lambda_i(\Lambda)} \leqslant \frac{\sqrt{3}}{2}$ 可以推出

$$\sum_{i=1}^{j-1} \lambda_i(\Lambda)^2 = \sum_{i=1}^{j-2} \lambda_i(\Lambda)^2 + \lambda_{j-1}(\Lambda)^2 \leqslant 3\lambda_{j-1}(\Lambda)^2 + \lambda_{j-1}(\Lambda)^2 = 4\lambda_{j-1}(\Lambda)^2 \leqslant 3\lambda_j(\Lambda)^2,$$

即条件 C_j 也成立. 这样条件 C_j 对 $5 \leqslant j \leqslant k$ 都成立, 由定理 3.1 可得结论. □

4 依次最短无关组成为 M- 基子集的充分条件

本节我们讨论格中依次最短无关组 SMIV 在什么条件下能成为一个基子集. 首先有下面的简单事实.

命题 4.1 设 $\{b_1, \ldots, b_k\}$ 是 n 维格 Λ 的一组 SMIV, 如果 $\{b_1, \ldots, b_k\}$ 是基子集, 则它一定是 M-基子集, 即是某个 M- 基的前 k 个向量, 并且有

$$\|b_i\| = \lambda_i(\Lambda) = \mu_i(\Lambda), \quad 1 \leqslant i \leqslant k.$$

证明 首先 b_1 是 Λ 中最短的非零向量, 它是某组 Minkowski 约化基中第 1 个向量. 假设 $\{b_1, \ldots, b_{i-1}\}$ 已经是某个 Minkowski 约化基的前 $i-1$ 个向量, 取 $b'_i \in \Lambda$ 使得 $\{b_1, \ldots, b_{i-1}, b'_i\}$ 是某个 Minkowski 约化基的前 i 个向量, 显然它们线性无关. 由于 $\|b_i\| = \lambda_i(\Lambda)$, 可知

$$\|b_i\| = \lambda_i(\Lambda) \leqslant \mu_i(\Lambda) \leqslant \|b'_i\|.$$

又因 $\{b_1,\dots,b_i\}$ 是基子集, 由 Minkowski 约化基的定义, 上式表明 $\{b_1,\dots,b_i\}$ 也是一个 M- 基子集, 且 $\|b_i\|=\lambda_i(\Lambda)=\mu_i(\Lambda)=\|b_i'\|$. 归纳得到结论. □

下面的定理是本节的主要结论.

定理 4.2 设 $\{b_1,\dots,b_k\}$ 是 n 维格 Λ 的一组 SMIV, 则

(1) 当 $1\leqslant k\leqslant 3$ 时, $\{b_1,\dots,b_k\}$ 是 M- 基子集, 此时 $\|b_i\|=\lambda_i(\Lambda)=\mu_i(\Lambda)$ $(1\leqslant i\leqslant k)$.

(2) 当 $k=4$ 时, 存在格向量 $b_4'\in\Lambda$, 使得 $\{b_1,b_2,b_3,b_4'\}$ 构成 M- 基子集, 并且有正整数 d, 使得

$$b_4\in db_4'+\mathrm{span}_{\mathbb{Z}}\{b_1,b_2,b_3\}.$$

(i) 若 $d=1$, 则 $\{b_1,b_2,b_3,b_4\}$ 是 M- 基子集, 此时 $\|b_4\|=\lambda_4(\Lambda)=\mu_4(\Lambda)$;

(ii) 若 $d>1$, 则 $\{b_1,b_2,b_3,b_4\}$ 不是 M- 基子集. 此时 b_1,b_2,b_3,b_4 是互相正交的等长向量, 且

$$b_4'=\frac{1}{2}\Big(\sum_{j=1}^{3}x_jb_j+b_4\Big),$$

其中 $x_j=\pm1$, $\|b_4'\|=\lambda_j(\Lambda)=\mu_j(\Lambda)$, $1\leqslant j\leqslant 4$.

(3) 当 $k\geqslant 4$ 时, 如果 Λ 满足 $\sum_{i=1}^{j-1}\lambda_i(\Lambda)^2<3\lambda_j(\Lambda)^2$ (条件 C_j') 对 $4\leqslant j\leqslant k$ 成立, 则 $\{b_1,\dots,b_k\}$ 是 M- 基子集, 且有 $\|b_j\|=\lambda_j(\Lambda)=\mu_j(\Lambda)$ $(1\leqslant j\leqslant k)$.

证明 (1) 当 $1\leqslant k\leqslant 3$ 时, 若结论不成立, 则有 $j\leqslant k$ 使得 $\{b_1,\dots,b_{j-1}\}$ 是基子集, 而 $\{b_1,\dots,b_j\}$ 不是基子集, 根据推论 2.4 可知, 必有基子集 $\{b_1,\dots,b_{j-1},r_j\}$ 满足

$$\|r_j\|\leqslant\frac{\sqrt{j}}{2}\|b_j\|<\|b_j\|.$$

另一方面, 显然有 $\|b_j\|=\lambda_j(\Lambda)\leqslant\|r_j\|$, 得出矛盾.

(2) 由 (1) 知, $\{b_1,b_2,b_3\}$ 是 Λ 的一个基子集. 对于 $\{b_1,\dots,b_4\}$, 由关键引理, 存在基子集 $\{b_1,\dots,b_3,b_4'\}$ 和正整数 t_{44}, 使得 $b_4\in t_{44}b_4'+\mathrm{span}_{\mathbb{Z}}\{b_1,\dots,b_3\}$. 令 $d=t_{44}$, 则有:

(i) 若 $d=1$, 则有 $b_4'\in db_4+\mathrm{span}_{\mathbb{Z}}\{b_1,b_2,b_3\}$, 故 $\{b_1,\dots,b_4\}$ 也是基子集, 结论成立.

(ii) 若 $d>1$. 此时, 由 $\|b_1\|\leqslant\|b_2\|\leqslant\|b_3\|\leqslant\|b_4\|$, 得到

$$\|b_4\|=\lambda_4(\Lambda)\leqslant\|b_4'\|\leqslant\sqrt{\sum_{j=1}^{3}\frac{\|b_j^*\|^2}{4}+\frac{\|b_4^*\|^2}{d^2}}\leqslant\frac{\sqrt{\sum_{j=1}^{4}\|b_j^*\|^2}}{2}\leqslant\frac{\sqrt{\sum_{j=1}^{4}\|b_j\|^2}}{2}\leqslant\|b_4\|.$$

因此, 上面不等式中的每一项都相等, 这意味着 $\|b_4'\|=\|b_1\|=\cdots=\|b_4\|$, 并且 $d=2$, $\|b_j^*\|=\|b_j\|$, 对 $1\leqslant j\leqslant 4$ 都成立, 这里 $\{b_1^*,\dots,b_4^*\}$ 是 $\{b_1,\dots,b_4\}$ 做 Gram-Schmidt 正交化得到的向量组. 因此, 对每个 $1\leqslant j\leqslant 4$, $b_j^*=b_j$. 这样得到, $b_1,\dots,b_4$ 是彼此正交的等长向量. 由于 $d=2$, 不妨设

$$2b_4'=\sum_{j=1}^{3}x_jb_j+b_4,\quad x_j\in\mathbb{Z}.$$

计算模长可得,

$$4\|b_4'\|^2=\sum_{j=1}^{3}x_j^2\|b_j\|^2+\|b_4\|^2,$$

即 $x_1^2+x_1^2+x_2^2+x_3^2=3$, 从而 $x_j^2=1,x_j=\pm1,1\leqslant j\leqslant 3$. 结论获证.

(3) 同样由推论 2.4, 若 $\{b_1,\dots,b_4\}$ 不是基子集, 则存在基子集 $\{b_1,\dots,b_3,b_4'\}$, 使得

$$\|b_4\|=\lambda_4(\Lambda)\leqslant\|b_4'\|\leqslant\frac{\sqrt{\sum_{j=1}^3\|b_j\|^2+\|b_4\|^2}}{2}<\frac{\sqrt{3\|b_4\|^2+\|b_4\|^2}}{2}=\|b_4\|,$$

得到矛盾. 因此 $\{b_1,\dots,b_4\}$ 是 M- 基子集. 对 $5\leqslant j\leqslant k$, 利用条件 C_j' 和同样的推理, 由归纳法可得 $\{b_1,\dots,b_k\}$ 是 Λ 的 M- 基子集. □

注记 定理 4.2(2) 的 (ii) 表明, 由 4 个向量组成的 SMIV 如果不是基子集, 本质上只能是第 1 节中给出的例子. 当 $n=4$ 时, $\{2e_1,2e_2,2e_3,2e_4\}$ 是格 Λ 的一组 SMIV, 但却不是 Λ 的基. 而格基 $\{2e_1,2e_2,2e_3,\mathbf{1}\}$ 中 $\mathbf{1}=(1,1,1,1)^{\mathrm{T}}$ 恰好是 $\frac{1}{2}\sum_{i=1}^4 2e_i$.

类似于定理 3.2, 我们有

定理 4.3 设 $n\geqslant 5$, 若 5 维格 Λ 满足 $\sum_{i=1}^3\lambda_i(\Lambda)^2<3\lambda_4(\Lambda)^2$, 并且 $\frac{\lambda_{j-1}(\Lambda)}{\lambda_j(\Lambda)}\leqslant\frac{\sqrt{3}}{2}$ 对 $5\leqslant j\leqslant k$ 都成立, 则 Λ 中的 SMIV$\{b_1,\dots,b_k\}$ 必是 M- 基子集, 且有 $\|b_j\|=\lambda_j(\Lambda)=\mu_j(\Lambda),1\leqslant j\leqslant k$.

证明 根据定理 4.2(3), 我们只需验证条件 C_j' 对 $5\leqslant j\leqslant k$ 都成立. 当 $j=5$ 时,

$$\sum_{i=1}^4\lambda_i(\Lambda)^2=\sum_{i=1}^3\lambda_i(\Lambda)^2+\lambda_4(\Lambda)^2<4\lambda_4(\Lambda)^2\leqslant 3\lambda_5(\Lambda)^2,$$

即条件 C_5' 成立. 假设条件直到条件 C_{j-1}' 成立, 则

$$\sum_{i=1}^{j-1}\lambda_i(\Lambda)^2=\sum_{i=1}^{j-2}\lambda_i(\Lambda)^2+\lambda_{j-1}(\Lambda)^2<4\lambda_{j-1}(\Lambda)^2\leqslant 3\lambda_j(\Lambda)^2,$$

由归纳得到, 条件 C_j' 对 $5\leqslant j\leqslant k$ 都成立. □

最后, 结合上一节中定理 3.1 和 3.2, 我们得到格中 SMIV 与 M- 基子集等价的充分条件.

定理 4.4 设 $B=\{b_1,\dots,b_k\}$ 是 n 维格 Λ 中的线性无关向量组,

(1) 当 $1\leqslant k\leqslant\min\{3,n\}$ 时, 则 B 是 SMIV$\Leftrightarrow$ B 是 M- 基子集;

(2) 当 $k\geqslant 4$ 时,

(i) 条件 (C_j') 对 $4\leqslant j\leqslant k$ 都成立, 则 B 是 SMIV$\Leftrightarrow$ B 是 M- 基子集.

(ii) 若条件 (C_4') 成立, 并且若

$$\frac{\lambda_{j-1}(\Lambda)}{\lambda_j(\Lambda)}\leqslant\frac{\sqrt{3}}{2}$$

对 $5\leqslant j\leqslant k$ 成立, 则 B 是 SMIV$\Leftrightarrow$ B 是 M- 基子集. □

参考文献

1 Micciancio D, Goldwasser S. Complexity of Lattice Problems: A Crytographic Perspective. Boston-Dordrent-London: Kluwer, 2002

2 Nguyen P, Stern J. The two faces of lattices in cryptology. In: Proceedings of the 2001 Cryptography and Lattices Conference (CALC'01). Lecture Notes in Computer Science, vol. 2146. Berlin: Springer-Verlag, 2001, 146–180

3 Lenstra A, Lenstra H, Lovász L. Factoring ploynomials with rational coefficients. Math Ann, 1982, 261: 551–534

4 Gama N, Howgrave-Graham N, Koy H, et al. Rankin's constant and blockwise lattice reduction. In: Proceedings of Crypto '06. Lecture Notes in Computer Science, vol. 4117. Heidelberg: Springer-Verlag, 2006, 112–130

5 Waerden V. Die Reduktionstheorie der positiven quadratischen Formen. Acta Math, 1956, 96: 265–309

6 Ryskov S. On Hermite, Minkowski and Venkov reduction of positive quadratic forms in n variables. Soviet Math Doklady, 1972, 13: 1676–1679

7 Cohen H. A Course in Computational Algebra Number Theory. In: Graduate Texts in Math, vol. 138. Berlin: Springer-Verlag, 1996

Some sufficient conditions of the equivalence between successive minimal independent vectors and Minkowski-reduced basis in lattices

WANG YuanHua, SHANG ShiKui, GAO Feng & HUANG MingQiang

Abstract In this paper, we discuss the relationship of vector length among the subsets of basis, successive minima independent vectors and Minkowski-reduced basis. We get some sufficient conditions under which the length of Minkowski-reduced basis reaches successive minima. Furthermore, some sufficient conditions are given under which successive minima independent vectors become Minkowski-reduced basis.

Keywords: **lattice, successive minima, successive minimal independent vectors, Minkowski-reduced basis**
MSC(2000): **11H50, 11H55**