УДК 511.36+511.9

СМЕЖНЫЕ МИНИМУМЫ РЕШЕТОК [1]

В. А. Быковский, О. А. Горкуша (г. Хабаровск)

Аннотация

Вороной доказал, что для трехмерных полных решеток любые два смежных минимума можно дополнить до базиса некоторым третьим узлом. В этой работе мы доказываем s — мерное обобщение теоремы Вороного для $s \geq 4$.

Всюду далее через s $(s = 2, 3, \dots)$ будем обозначать размерность пространства $\mathbb{R}^s$. Для $x = (x_1, \dots, x_s) \in \mathbb{R}^s$ положим $\Pi(x) = \left\{x' \in \mathbb{R}^s \middle| |x'_i| \leq |x_i|; i = 1, \dots, s\right\}$. Если T — непустое конечное подмножество в $\mathbb{R}^s$, то введем обозначение

$$\Pi(T) = \Pi(|T|_1, \dots, |T|_s),$$

где $|T|_i = max\left\{|x_i| \middle| x = (x_1, \dots, x_i, \dots, x_s) \in T\right\}$. Пусть $\mathfrak{L}_s(\mathbb{R})$ — множество всех полных решеток (в дальнейшем просто решеток) в $\mathbb{R}^s$, а $\mathfrak{M}(\Gamma)$ — множество всех относительных минимумов решетки Γ (в дальнейшем просто минимумов), состоящее из ненулевых узлов $\gamma \in \Gamma$, для которых не существует ненулевых $\gamma' \in \Gamma$ со строгим включением $\Pi(\gamma') \subset \Pi(\gamma)$.

Напомним, что произвольная решетка Γ из $\mathfrak{L}_s(\mathbb{R})$ имеет вид

$$\Gamma = \{m_1\gamma^{(1)} + \dots + m_s\gamma^{(s)} \big| m_1, \dots, m_s \in \mathbb{Z}\}$$

с линейно независимыми узлами $\gamma^{(1)}, \dots, \gamma^{(s)}$, составляющими целочисленный базис Γ (см. [1]). Пусть

$$\alpha = [0; q_1, \dots, q_i, \dots] \tag{1}$$

— разложение $\alpha \in (0, 1/2]$ в цепную дробь с неполными частными $q_i \in \mathbb{N}$, и для $i = 1, 2, \dots$

$$P_i/Q_i = [0; q_1, \dots, q_i] \tag{2}$$

— несократимые подходящие дроби к α с натуральными P_i и Q_i. Удобно положить $P_0 = 1, Q_0 = 0$. Определим решетку (из $\mathfrak{L}_2(\mathbb{R})$)

$$\Gamma_\alpha = \{m_1(1, 0) + m_2(-\alpha, 1) \big| m_1, m_2 \in \mathbb{Z}\}. \tag{3}$$

По теореме Лагранжа о наилучших приближениях

$$\mathfrak{M}(\Gamma_\alpha) = \{\pm(P_i - \alpha Q_i, Q_i) \big| i = 0, 1, \dots\}. \tag{4}$$

Пусть теперь Γ произвольная решетка из $\mathfrak{L}_s(\mathbb{R})$, порожденная базисом $\gamma^{(1)}, \dots, \gamma^{(s)}$. Поскольку в соответствии с (4)

$$\{(m_1, m_2) \in \mathbb{Z}^2 \big| m_1(1, 0) + m_2(-\alpha, 1) \in \mathfrak{M}(\Gamma_\alpha)\} =$$

[1] Работа выполнена при финансовой поддержке ФЦП "Интеграция"(проект К 0560).

$$= \{\pm(P_i, Q_i)\big| i = 0, 1, \dots\},$$

то целочисленные наборы из

$$\{(m_1, \dots, m_s) \in \mathbb{Z}^s \big| m_1\gamma^{(1)} + \dots + m_s\gamma^{(s)} \in \mathfrak{M}(\Gamma)\} \tag{5}$$

можно рассматривать в качестве аналога подходящих дробей для произвольных решеток Γ. Разумеется, множество (5) зависит от выбора конкретного базиса решетки Γ. Эту конструкцию предложили Вороной [2] и Минковский в конце девятнадцатого века независимо друг от друга.

Особенности взаимного расположения минимумов решетки играют большую роль при построении многомерных обобщений алгоритма разложения чисел в цепную дробь. Следуя [2] и [3] назовем минимумы $\gamma^{(1)}$ и $\gamma^{(2)}$ из $\mathfrak{M}(\Gamma)$ с $\gamma^{(1)} \neq \pm\gamma^{(2)}$ смежными, если не существует отличный от нулевого узел $\gamma \in \Gamma$, для которого:
а) $\gamma_i = 0$ при всех i с $|\{\gamma^{(1)}, \gamma^{(2)}\}|_i = 0$;
б) $|\gamma_i| < |\{\gamma^{(1)}, \gamma^{(2)}\}|_i$ при всех i с $|\{\gamma^{(1)}, \gamma^{(2)}\}|_i > 0$.
Вороной в [2] доказал:
(I) для решеток $\Gamma \in \mathfrak{L}_2(\mathbb{R})$ любая пара смежных минимумов Γ составляет базис Γ;
(II) для решеток $\Gamma \in \mathfrak{L}_3(\mathbb{R})$ любую пару смежных минимумов Γ можно дополнить некоторым третьим узлом до базиса Γ.
В настоящей работе мы обобщаем этот результат на остальные размерности в следующем виде.

Теорема 1. *Пусть $s \geq 4$ и $\gamma^{(1)}, \gamma^{(2)}$ произвольная пара смежных минимумов решетки $\Gamma \in \mathfrak{L}_s(\mathbb{R})$ с $(\gamma^{(1)} \pm \gamma^{(2)})/2 \notin \Gamma$. Тогда $\gamma^{(1)}$ и $\gamma^{(2)}$ можно дополнить некоторыми узлами $\gamma^{(3)}, \dots, \gamma^{(s)}$ (не обязательно минимумами!) до базиса Γ.*

Для доказательства теоремы нам потребуются следующие два утверждения.

Лемма 1. *Пусть $\gamma^{(1)}, \dots, \gamma^{(s)}$ — базис решетки $\Gamma \in \mathfrak{L}_s(\mathbb{R})$ и для относительного минимума γ разложение по базису имеет вид:*

$$\gamma = m_1\gamma^{(1)} + \dots + m_s\gamma^{(s)}.$$

Тогда $(m_1, \dots, m_s) = 1$.

Доказательство. Если $\mathrm{H}(m_1, \dots, m_s) = d > 1$, то $\gamma = d\gamma'$ с $\gamma' \in \Gamma$. Но тогда $\Pi(\gamma') \subset \Pi(\gamma)$, что нарушает условие минимальности γ. Лемма доказана. □

Лемма 2 (см.[1], гл.1, §2). *Пусть $\gamma^{(1)}, \dots, \gamma^{(s)}$ — базис решетки $\Gamma \in \mathfrak{L}_s(\mathbb{R})$ и для некоторых целых $m_1, \dots, m_s$, $n_1, \dots, n_s$*

$$\gamma = m_1\gamma^{(1)} + \dots + m_s\gamma^{(s)}, \gamma' = n_1\gamma^{(1)} + \dots + n_s\gamma^{(s)}.$$

Тогда узлы γ и γ' можно дополнить до базиса Γ тогда и только тогда, когда наибольший общий делитель всех целых чисел

$$D_{ij} = det\begin{pmatrix} m_i & m_j \\ n_i & n_j \end{pmatrix} = m_i n_j - m_j n_i \tag{6}$$

с $1 \le i < j \le s$ *равен* 1.

Доказательство теоремы. Пусть $\zeta^{(1)}, \ldots, \zeta^{(s)}$ — базис Γ. Тогда для некоторых целых $m_j, n_j (j = 1, \ldots, s)$

$$\gamma^{(1)} = m_1\zeta^{(1)} + \cdots + m_s\zeta^{(s)}, \gamma^{(2)} = n_1\zeta^{(1)} + \cdots + n_s\zeta^{(s)}.$$

Согласно лемме 2 достаточно доказать, что наибольший общий делитель всех чисел D_{ij} из (6) равен 1. Пусть это не так. То есть, найдется натуральное $q \neq 1$, для которого все D_{ij} из (6) делятся на q. Согласно лемме 1 наибольший общий делитель чисел $m_1, \ldots, m_s$ равен 1. Поэтому для некоторого индекса $tm_t \not\equiv 0(modq)$. Определим целые a и b из условий:

$$a \equiv n_t(modq), b \equiv -m_t(modq),$$

$$-q/2 < a, b \le q/2.$$

При этом $b \neq 0$. Поскольку

$$a\gamma^{(1)} + b\gamma^{(2)} = \sum_{j=1}^{s}(am_j + bn_j)\zeta^{(j)}$$

и для любого j, согласно предположению и выбору a с b,

$$am_j + bn_j \equiv n_t m_j - m_t n_j \equiv 0(modq),$$

то $a\gamma^{(1)} + b\gamma^{(2)} = q\gamma$ с $\gamma \in \Gamma$ и $\gamma \neq (0, \ldots, 0)$. При этом для всех $j = 1, \ldots, s$

$$|\gamma_j| \le (|\gamma_j^{(1)}| + |\gamma_j^{(2)}|)/2. \tag{7}$$

Если $|\gamma_j^{(1)}| \neq |\gamma_j^{(2)}|$, то из (7) следует строгое неравенство

$$|\gamma_j| < max\{|\gamma_j^{(1)}|, |\gamma_j^{(2)}|\} = |\{\gamma^{(1)}, \gamma^{(2}\}|_j. \tag{8}$$

Также $\gamma_j = 0$ при $\gamma_j^{(1)} = \gamma_j^{(2)} = 0$. Предположим, что имеются индексы j с $|\gamma_j^{(1)}| = |\gamma_j^{(2)}| \neq 0$. Тогда равенство в (7) возможно только для $a = b = q/2$. А этого не может быть, поскольку по условию теоремы точки $(\gamma^{(1)} \pm \gamma^{(2)})/2$ из $\mathbb{R}^s$ не являются узлами Γ. Теорема полностью доказана.

Пусть Γ решетка из $\mathfrak{L}_4(\mathbb{R})$, порожденная базисом

$$(1, 1, 0, 1), (1, 0, 1, -1), (4, 0, 0, 0), (0, 0, 0, 4).$$

Положим

$$\gamma^{(1)} = (2, 1, 1, 0), \gamma^{(2)} = (0, 1, -1, 2).$$

Тогда $\gamma^{(1)}$ и $\gamma^{(2)}$ минимумы Γ и не дополняются до базиса. При этом

$$(\gamma^{(1)} + \gamma^{(2)})/2 = (1, 1, 0, 1), (\gamma^{(1)} - \gamma^{(2)})/2 = (1, 0, 1, -1)$$

— узлы Γ. Следовательно, условие $(\gamma^{(1)} \pm \gamma^{(2)})/2 \notin \Gamma$ не может быть опущено.

Список литературы

[1] *Cassels J.* An introduction to the geometry of numbers. Cambridge: , 1959; (Русский перевод: Введение в геометрию чисел. М.: Мир, 1965)

[2] *Вороной Г. Ф.* Собрание сочинений. Т. 1., Киев:, 1952.

[3] *Buchmann J.* On the Computation of Units and Class Numbers by a Generalization of Lagrange's Algorithm. // Journal of Number Theory. 1987. V. 26. P. 8–30.