На правах рукописи

Гассан Сергей Владимирович

Вычислительные алгоритмы в геометрии чисел

01.01.07 — вычислительная математика

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Владивосток 2011

Работа выполнена в Институте прикладной математики ДВО РАН

Научный руководитель:	доктор физико-математических наук, член-корреспондент РАН Быковский Виктор Алексеевич
Официальные оппоненты:	доктор физико-математических наук, профессор Добровольский Николай Михайлович
	кандидат физико-математических наук Илларионов Андрей Анатольевич
Ведущая организация:	Механико-математический факультет МГУ имени М.В. Ломоносова, г. Москва

Защита состоится 25.01.2012 в 15.00 на заседании диссертационного совета К 212.294.02 в Тихоокеанском государственном университете по адресу: 680035, г. Хабаровск, ул. Тихоокеанская, 136, ауд. 315л.

С диссертацией можно ознакомиться в библиотеке Тихоокеанского государственного университета.

Автореферат разослан "____" декабря 2011 г.

Ученый секретарь
диссертационного совета,
к.ф.-м.н. Э.М. Вихтенко

Общая характеристика работы

Актуальность темы

Обобщением теории непрерывных дробей на многомерный случай занимались многие математики, начиная с Л. Эйлера. Одно из самых удачных было предложено в конце девятнадцотого века Г. Минковским и Г.Ф. Вороным, независимо друг от друга. Оно основано на фундаментальном понятии "локальный минимум" решетки. Построение и анализ алгоритмов для вычисления локальных минимумов, а также изучение их взаимного расположения — одна из важнейших задач в геометрии чисел и целочисленном линейном программировании.

Впервые подобные вопросы были исследованы в работе Валена, опубликованной в 1893 году, для двумерных решеток. Кроме того, в работах В. Быковского эти исследования нашли приложения в теории квадратурных формул, построенных с помощью сеток Коробова. Выяснилось, что у решеток, с помощью которых строятся сетки Коробова, локальные минимумы определяют величину погрешности квадратурных формул на классах функций с доминирующей производной. Тем самым, алгоритмические аспекты вышеупомянутых задач геометрии чисел играют важную роль при построении конкретных оптимальных сеток Коробова, обеспечивающих наилучшую точность при вычислении многомерных интегралов.

Цель работы

Целью работы является разработка эффективного алгоритма для вычисления множества локальных минимумов решеток и исследование их взаимного расположения.

Методика исследования

При выполнении диссертации использовались теория выпуклого анализа, методы геометрии чисел, диофантовых приближений, аналитической и вычислительной теории чисел.

Научная новизна

- В рамках исследования взаимного расположения локальных минимумов трехмерных решеток получен явный вид трехмерных областей Валена первого и второго типов, что уточняет теорему Валена.
- На основе предложенной В.А. Быковским теоретической схемы разработан алгоритм для вычисления локальных минимумов целочисленных решеток.
- Разработан алгоритм для вычисления параметра Бахвалова и оптимальных коэффициентов параллелепипедальных сеток Коробова с помощью локальных минимумов.
- Построена модификация алгоритма вычисления локальных минимумов, позволяющая вычислять параметр Бахвалова приближенно и существенно ускорить вычисление оптимальных коэффициентов.

Личный вклад автора

Области Валена получены автором самостоятельно. На основе предложенной В.А. Быковским теоретической схемы автор самостоятельно разработал и оптимизировал алгоритмы для вычисления локальных минимумов целочисленных решеток, параметра Бахвалова и оптимальных коэффициентов параллелепипедальных сеток Коробова. Программная реализация построенных алгоритмов и вычислительные эксперименты также выполнены автором.

Достоверность

полученных результатов обеспечивается корректностью применения методов исследования, строгостью проведения доказательств предлагаемых утверждений, а также сопоставлением полученных в результате вычислительных экспериментов значений погрешностей квадратурных формул со значениями, полученными ранее другими исследователями.

Теоретическая и практическая ценность

Результаты работы, полученные при исследовании взаимного расположения локальных минимумов трехмерных решеток, носят теоретический характер и могут быть использованы в геометрии чисел, теории диофантовых приближений и целочисленном линейном программировании.

Разработанные алгоритмы для вычисления локальных минимумов и оптимальных коэффициентов могут быть непосредственно использованы на практике для нахождения оптимальных параллелепипедальных сеток.

Апробация работы

Результаты диссертации докладывались и обсуждались на трех Дальневосточных математических школах-семинарах имени Е.В. Золотова (Владивосток, 2004; Хабаровск, 2005; Владивосток, 2010), на научной конференции “Суперкомпьютеры: вычислительные и информационные технологии” (Хабаровск, 2010), на международной научной конференции “First Russia and Pacific Conference on Computer Technology and Applications” (Vladivostok, 2010), на научно-технической конференции “Математическое, вычислительное и информационное обеспечение технологических процессов и систем” (Комсомольск-на-Амуре, 2010), на семинаре ХО ИПМ ДВО РАН (Хабаровск, 2009).

Публикации

Основные результаты диссертации опубликованы в работах, указанных в конце автореферата.

Структура и объем работы

Диссертация изложена на 71 странице и состоит из введения, трех глав (с разбиением на параграфы) и списка литературы из 32 наименований. Работа включает 10 рисунков и 2 таблицы.

Содержание работы

Во **введении** излагается история и мотивировки вопросов, изучаемых в диссертации, а также вводятся некоторые основные определения.

Пусть $\{\boldsymbol{\gamma}^{(1)}, \ldots, \boldsymbol{\gamma}^{(s)}\}$ — s линейно независимых точек из $\mathbb{R}^s$, рассматриваемые как столбцы невырожденной матрицы $G = (\boldsymbol{\gamma}^{(1)} \ldots \boldsymbol{\gamma}^{(s)}) = (\gamma_i^{(j)})$ с $\gamma_i^{(j)} \in \mathbb{R}$. Множество всех целочисленных линейных комбинаций

$$\Gamma = \Gamma(G) = \left\{\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s) = m_1\boldsymbol{\gamma}^{(1)} + \ldots + m_s\boldsymbol{\gamma}^{(s)} \mid m_1, \ldots, m_s \in \mathbb{Z}\right\}$$

назовем ***s*-мерной решеткой** в $\mathbb{R}^s$ с базисом $\langle\boldsymbol{\gamma}^{(1)}, \ldots, \boldsymbol{\gamma}^{(s)}\rangle$. В случае если все числа $\gamma_i^{(j)}$ являются целыми, то решетка называется ***целочисленной***. Величину $D = D(\Gamma) = |\det(G)|$ назовем ***определителем*** решетки Γ.

Обозначим через $\mathcal{L}(\mathbb{R}^s)$ множество всех решеток в $\mathbb{R}^s$, а через $\mathcal{L}^*(\mathbb{R}^s)$ его подмножество, состоящее из всех решеток "общего положения", у которых для любого ненулевого узла $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s)$ все координаты γ_i отличны от нуля. Другими словами, на координатных гиперплоскостях нет ненулевых узлов Γ.

Назовем две матрицы G и G' ***эквивалентными***, если одна получается из другой путем композиции некоторых преобразований вида: 1) изменение знака у столбца или строки; 2) перестановка двух столбцов или строк.

Ненулевой узел $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s)$ назовем ***локальным минимумом*** решетки Γ, если не существует ненулевого узла $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_s)$ из Γ, для которого

$$|\eta_i| \leqslant |\gamma_i| \quad \text{для всех} \quad i = 1, \ldots, s,$$

и при этом хотя бы одно из этих s неравенств строгое.

Назовем матрицу $G = (\boldsymbol{\gamma}^{(1)} \ldots \boldsymbol{\gamma}^{(s)})$ и определяемый ею базис $\langle\boldsymbol{\gamma}^{(1)}, \ldots, \boldsymbol{\gamma}^{(s)}\rangle$ ***минимальными***, если не существует ненулевого узла $\boldsymbol{\eta}$ из Γ, для которого

$$|\eta_i| < \max\{|\gamma_i^{(1)}|, \ldots, |\gamma_i^{(t)}|\} \quad (i = 1, \ldots, s).$$

Понятно, что для решеток "общего положения" $\Gamma \in \mathcal{L}^*(\mathbb{R}^s)$ каждый узел минимального базиса для Γ является локальным минимумом решетки. Из определения непосредственно следует, что эквивалентные матрицы (и соответствующие им базисы) минимальны только одновременно.

В первой главе **"Трехмерные области Валена"** изучается взаимное расположение векторов минимальных базисов трехмерных решеток.

Согласно работе Минковского [1], невырожденная матрица G, определяющая базис решетки Γ "общего положения", минимальна тогда и только тогда когда она эквивалентна одной из матриц вида

$$M_I = \begin{pmatrix} x_1 & -y_1 & z_1 \\ x_2 & y_2 & -z_2 \\ x_3 & y_3 & z_3 \end{pmatrix}, \qquad M_{II} = \begin{pmatrix} x_1 & -y_1 & -z_1 \\ x_2 & y_2 & -z_2 \\ x_3 & y_3 & z_3 \end{pmatrix} \tag{1}$$

[1] **Minkowski H.** Generalization de la theorie des fraction continues / H. Minkowski // Ann. Sci. École Norm. Sup. — 1896. — Vol. 13, №2. — P. 41-60.

с неотрицательными $x_i, y_i, z_i \in \mathbb{R}$, у которых:

(i) $\max\{x_1, z_1\} \leqslant y_1, \;\; \max\{y_2, z_2\} \leqslant x_2, \;\; \max\{x_3, y_3\} \leqslant z_3$;

(ii) для матрицы M_I *(первый тип)* выполняется по крайней мере одно из неравенств: $z_1 \leqslant x_1, \;\; y_2 \leqslant z_2$;

(iii) для матрицы M_{II} *(второй тип)* выполняются неравенства: $y_3 \leqslant x_3, \;\; x_2 \leqslant y_2 + z_2$.

Матрицы вида (1) будем называть ***матрицами Минковского***, соответственно, первого и второго типа. Базис $\langle \boldsymbol{\gamma^{(1)}}, \boldsymbol{\gamma^{(2)}}, \boldsymbol{\gamma^{(3)}} \rangle$ решетки Γ будем называть ***базисом Минковского***, если соответствующая ему матрица эквивалентна матрице Минковского.

Согласно теореме Минковского о выпуклом теле, для любого локального минимума $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \gamma_3)$ решетки $\Gamma \in \mathcal{L}(\mathbb{R}^3)$

$$|\gamma_1\gamma_2\gamma_3| \leqslant D(\Gamma).$$

Из работы [2] следует, что для каждой пары узлов $\left(\boldsymbol{\gamma^{(i)}}, \boldsymbol{\gamma^{(j)}}\right)$ базиса Минковского

$$\min\left\{ |\gamma_1^{(i)}\gamma_2^{(i)}\gamma_3^{(i)}|, |\gamma_1^{(j)}\gamma_2^{(j)}\gamma_3^{(j)}| \right\} \leqslant \frac{1}{2}D(\Gamma).$$

Это неравенство называют теоремой Валена для трехмерных решеток.

Пусть узлы $\boldsymbol{\gamma^{(1)}}, \boldsymbol{\gamma^{(2)}}, \boldsymbol{\gamma^{(3)}}$ составляют базис Минковского решетки Γ. В работе [3] для таких узлов было доказано неравенство

$$\min\left\{ |\gamma_1^{(1)}\gamma_2^{(1)}\gamma_3^{(1)}|, |\gamma_1^{(2)}\gamma_2^{(2)}\gamma_3^{(2)}|, |\gamma_1^{(3)}\gamma_2^{(3)}\gamma_3^{(3)}| \right\} \leqslant \frac{1}{3}D(\Gamma).$$

Наконец, в [4] последняя оценка была усилена в следующем виде: для узлов $\boldsymbol{\gamma^{(1)}}, \boldsymbol{\gamma^{(2)}}, \boldsymbol{\gamma^{(3)}}$, составляющих базис Минковского

$$|\gamma_1^{(1)}\gamma_2^{(1)}\gamma_3^{(1)}| + |\gamma_1^{(2)}\gamma_2^{(2)}\gamma_3^{(2)}| + |\gamma_1^{(3)}\gamma_2^{(3)}\gamma_3^{(3)}| \leqslant D(\Gamma).$$

В настоящей работе мы уточняем перечисленные выше результаты следующим образом. Рассмотрим трехмерный вектор

$$(x, y, z) = \left(\frac{|\gamma_1^{(1)}\gamma_2^{(1)}\gamma_3^{(1)}|}{D(\Gamma)}, \frac{|\gamma_1^{(2)}\gamma_2^{(2)}\gamma_3^{(2)}|}{D(\Gamma)}, \frac{|\gamma_1^{(3)}\gamma_2^{(3)}\gamma_3^{(3)}|}{D(\Gamma)} \right),$$

составленный из деленных на определитель решетки абсолютных величин произведений координат базиса Минковского. Образы отображения

$$M \to (x, y, z) = \left(\frac{x_1x_2x_3}{\det(M)}, \frac{y_1y_2y_3}{\det(M)}, \frac{z_1z_2z_3}{\det(M)} \right)$$

[2] **Быковский В.А.** Теорема Валена для двумерных подходящих дробей / В.А. Быковский // Математические заметки. — 1999. — Т. 66, №1. — С. 30-37.

[3] **Авдеева М.О.** Аналог теоремы Валена для совместных приближений пары чисел / М.О. Авдеева, В.А. Быковский // Математический сборник. — 2003. — Т. 194, №7. — С. 4-14.

[4] **Авдеева М.О.** Уточнение теоремы Валена для базисов Минковского трехмерных решеток / М.О. Авдеева, В.А. Быковский // Математические заметки. — 2006. — Т. 79, №2. — С. 163-168.

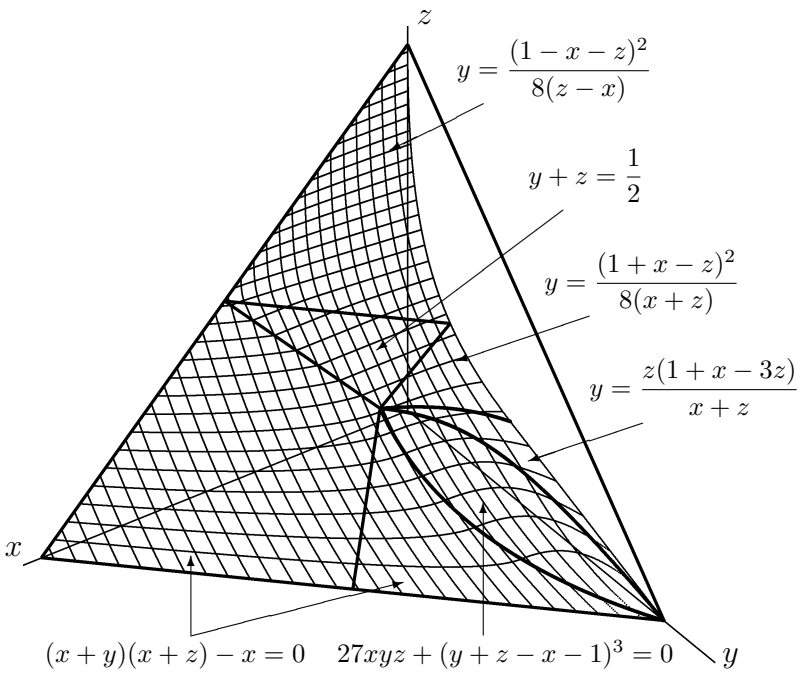

Рис. 1. Область W_I'

для случаев, когда M пробегает все невырожденные матрицы Минковского первого и второго типов, обозначим через $V_I(\mathbb{R}^3)$ и $V_{II}(\mathbb{R}^3)$ и назовем ***трехмерными областями Валена*** соответственно первого и второго типа.

Обозначим через W_I' (рис. 1) область в $\mathbb{R}^3$, состоящую из всех точек (x, y, z) с неотрицательными x, y, z и $x + z \leqslant 1$, для которых:

1) $y \leqslant \dfrac{x}{x+z} - x$ при $x \geqslant \max\{z, \sqrt{z} - z\}$;

2) $y \leqslant \psi(x, z)$ при $0 \leqslant x, z \leqslant \dfrac{1}{4}$; $x \leqslant \sqrt{z} - z$; $z \leqslant \sqrt{x(1+5x)} - 2x$;

3) $y \leqslant \dfrac{z(1+x-3z)}{x+z}$ при $0 \leqslant x, z \leqslant \dfrac{1}{4}$; $\sqrt{x(1+5x)} - 2x \leqslant z \leqslant \dfrac{1+x}{5}$;

4) $y \leqslant \dfrac{(1+x-z)^2}{8(x+z)}$ при $0 \leqslant x, z \leqslant \dfrac{1}{2}$; $x \leqslant \min\{5z-1, 1-3z\}$;

5) $y \leqslant \dfrac{1}{2} - z$ при $0 \leqslant x, z \leqslant \dfrac{1}{2}$; $x \leqslant z$; $x \geqslant \max\{1-3z, 3z-1\}$;

6) $y \leqslant \dfrac{(1-x-z)^2}{8(z-x)}$ при $x \leqslant 3z - 1$,

где через $y_0 = \psi(x, z)$ мы обозначили единственное действительное решение уравнения

$$f(y) = 27xyz + (y + z - x - 1)^3 = 0.$$

Обозначим через W_I'' область в $\mathbb{R}^3$, полученную из W_I' путем циклического сдвига переменных (x, y, z), так что переменным (x, y, z) (область W_I') соответствуют переменные (z, x, y) (область W_I''). Тогда имеет место

Теорема 1. *Область Валена $V_I(\mathbb{R}^3)$ есть объединение областей W_I' и W_I''.*

Обозначим через W_{II} (рис. 2) область в $\mathbb{R}^3$, состоящую из всех точек (x, y, z) с неотрицательными x, y, z, для которых:

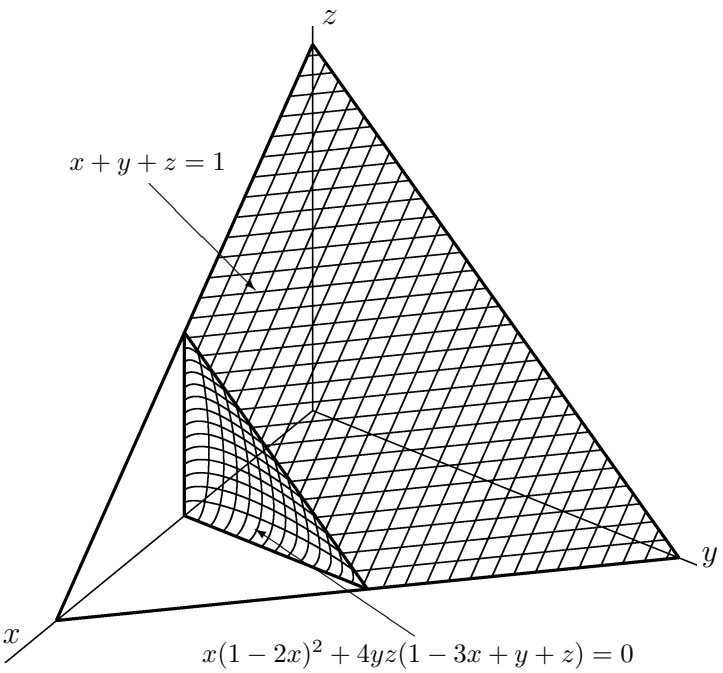

Рис. 2. Область W_{II}

1) $x + y + z \leqslant 1$ при $y + z \geqslant 1/2$;
2) $x \leqslant \varphi(y, z)$ при $y + z < 1/2$,

где через $x_0 = \varphi(y, z)$ мы обозначили решение уравнения

$$f(x) = x(1 - 2x)^2 + 4yz(1 - 3x + y + z) = 0,$$

принадлежащее отрезку $[4/9, 1/2]$. Тогда справедлива

Теорема 2. *Область Валена $V_{II}(\mathbb{R}^3)$ совпадает с W_{II}.*

Во второй главе **"Алгоритм вычисления локальных минимумов целочисленных решеток"** рассматривается построение алгоритма вычисления множества локальных минимумов целочисленных решеток на основе предложенной в работе В.А. Быковского [5] теоретической схеме. Ключевую роль в вычислительной схеме играют приведенные базисы и кратчайшие вектора решеток, алгоритмы вычисления которых обсуждаются в отдельных параграфах. В конце главы предлагается алгоритмическая модель для программной реализации рассмотренных алгоритмов и оценивается асимптотическое время работы.

Пусть $\boldsymbol{\mathcal{L}}$: $\mathbb{Z}^s \to \mathbb{Z}^s$ произвольное невырожденное линейное преобразование

$$\boldsymbol{m} = \begin{pmatrix} m_1 \\ m_2 \\ \dots \\ m_s \end{pmatrix} \to \boldsymbol{\mathcal{L}}(\boldsymbol{m}) = \begin{pmatrix} L_1(\boldsymbol{m}) \\ L_2(\boldsymbol{m}) \\ \dots\dots \\ L_s(\boldsymbol{m}) \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \dots\dots\dots\dots\dots \\ b_{s1} & b_{s2} & \cdots & b_{ss} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \dots \\ m_s \end{pmatrix},$$

где

$$L_i(\boldsymbol{m}) = m_1 b_{i1} + \ldots + m_s b_{is}$$

[5] **Быковский В.А.** Алгоритм вычисления локальных минимумов решеток / В.А. Быковский // Доклады РАН. — 2004. — Т. 399, №5. — С. 587-589.

линейные формы с целочисленными коэффициентами. Оно определяет целочисленную решетку

$$\Gamma = \left\{ \boldsymbol{v} = \boldsymbol{\mathcal{L}}(\boldsymbol{m}) = m_1\boldsymbol{b^{(1)}} + \ldots + m_s\boldsymbol{b^{(s)}} \mid m_1, \ldots, m_s \in \mathbb{Z} \right\}$$

в $\mathbb{R}^s$ с базисом $\langle \boldsymbol{b^{(1)}}, \ldots, \boldsymbol{b^{(s)}} \rangle$, элементы которого являются столбцами матрицы $B = (b_{ij})$ с $b_{ij} \in \mathbb{Z}$. Определитель решетки Γ $N = N(\Gamma) = |\det(B)|$.

Напомним, что ненулевой узел $\boldsymbol{v} = (v_1, \ldots, v_s)$ решетки Γ в $\mathbb{R}^s$ называется ***локальным минимумом***, если не существует другого ненулевого узла $\boldsymbol{u} = (u_1, \ldots, u_s)$ решетки Γ, для которого $|u_i| \leqslant |v_i|$ для всех $i = 1, \ldots, s$ и при этом хотя бы одно из этих s неравенств строгое. Введем обозначение

$$|||\boldsymbol{v}||| = \prod_{i=1}^{s} \max\{1, |v_i|\}.$$

По теореме Минковского о выпуклом теле, для любого локального минимума $\boldsymbol{v}$ целочисленной решетки Γ определителя N выполняется неравенство $|||\boldsymbol{v}||| \leqslant N$. Отсюда непосредственно следует, что множество $\mathfrak{M}(\Gamma)$ локальных минимумов целочисленной решетки Γ конечно. В работе [6] показано, что для количества его элементов выполняется оценка

$$\#\mathfrak{M}(\Gamma) \leqslant C(s)(\log^{s-1} N)$$

с некоторой положительной константой $C(s)$ и $N > 1$.

Пусть Γ — целочисленная решетка в $\mathbb{R}^s$ определителя N. Обозначим через $\mathcal{K}_s(N)$ множество всех наборов неотрицательных целых чисел $K = (k_1, \ldots, k_s)$, для которых

$$k_1 + \ldots + k_s \leqslant s/2 + \log_2 N$$

и при этом хотя бы одно k_i равно нулю. Каждому набору K из $\mathcal{K}_s(N)$ сопоставим положительно определенную квадратичную форму

$$Q^{(K)}(m_1, \ldots, m_s) = \sum_{i=1}^{s} \left(\frac{L_i(\boldsymbol{m})}{2^{k_i}} \right)^2. \tag{2}$$

По определению, величина

$$M^{(K)}(\Gamma) = \min_{\substack{\boldsymbol{m} \in \mathbb{Z}^s \\ \boldsymbol{m} \neq (0,\ldots,0)}} Q^{(K)}(\boldsymbol{m})$$

есть минимум $Q^{(K)}(\boldsymbol{m})$. Определим множество

$$\mathcal{M}(\Gamma) = \bigcup_{K \in \mathcal{K}_s(N)} \left\{ \boldsymbol{\mathcal{L}}(\boldsymbol{m}) \mid \boldsymbol{m} \in \mathbb{Z}^s \,;\, Q^{(K)}(\boldsymbol{m}) \leqslant 4s \cdot M^{(K)}(\Gamma) \right\}.$$

[6] **Быковский В.А.** О погрешности теоретико-числовых квадратурных формул / В.А. Быковский // Доклады РАН. — 2003. — Т. 389, №2. — С. 154-155.

В работе [5] показано, что имеет место включение $\mathfrak{M}(\Gamma) \subset \mathcal{M}(\Gamma)$.

Таким образом, для вычисления множества локальных минимумов $\mathfrak{M}(\Gamma)$ достаточно для каждого набора $K \in \mathcal{K}_s(N)$ перебрать все целочисленные решения $\boldsymbol{m} = (m_1, \ldots, m_s)$ неравенства $Q^{(K)}(\boldsymbol{m}) \leqslant 4s \cdot M^{(K)}(\Gamma)$ и выбрать среди векторов $\boldsymbol{v} = \boldsymbol{\mathcal{L}}(\boldsymbol{m})$ те, которые являются локальными минимумами решетки Γ.

Так выглядит схема алгоритма вычисления локальных минимумов, предложенная в работе В.А. Быковского [5]. Задача настоящей главы заключается в разработке и реализации этого алгоритма.

Для того чтобы все вычисления производить только с целыми числами, мы домножаем выражения вида (2) для квадратичных форм $Q^{(K)}(\boldsymbol{m})$ на множители. Для каждого набора $K = (k_1, \ldots, k_s) \in \mathcal{K}_s(N)$ мы определяем положительно определенную квадратичную форму

$$Q^{(K)}(\boldsymbol{m}) = \sum_{i=1}^{s} \left(2^{l_i} L_i(\boldsymbol{m})\right)^2$$

где $l_i = \max\{k_1, \ldots, k_s\} - k_i$. Все последующие рассуждения остаются без изменений.

Величина $M^{(K)}(\Gamma)$ достигается на кратчайшем ненулевом векторе некоторой решетки и является квадратом его длины. Вычисление кратчайшего вектора представляет собой довольно нетривиальную задачу и имеет тесную связь с нахождением базисов решетки, составленных из коротких векторов.

Для эффективного перечисления целочисленных решений $\boldsymbol{m} = (m_1, \ldots, m_s)$ неравенств

$$Q^{(K)}(\boldsymbol{m}) \leqslant 4s \cdot M^{(K)}(\Gamma) \tag{3}$$

мы используем базисы решеток, состоящие из коротких и почти ортогональных векторов. Такие базисы называются ***приведенными*** (***reduced***). Им соответствуют ***приведенные*** квадратичные формы. При использовании приведенных базисов все целочисленные решения неравенств (3) покоординатно ограничены константой, не завящей от размера задачи N (зависящей только от размерности пространства s).

В предложенной в работе В.А. Быковского [5] схеме алгоритма предлагается использовать базисы решеток, приведенные по Минковскому. Однако, время работы алгоритма построения приведенного по Минковскому базиса возрастает экспоненциально с ростом размерности пространства s. Поэтому, мы используем LLL-приведенные базисы, которые можно вычислить за полиномиальное время. В отличие от базиса, приведенного по Минковскому, LLL-приведенный базис не обязательно содержит среди своих векторов кратчайший вектор решетки, однако позволяет аппроксимировать его с точностью до множителя $2^{(s-1)/2}$. Для вычисления кратчайшего вектора мы используем алгоритм перечисления Fincke-Pohst, который принимает на входе LLL-приведенный базис.

Оценим время работы алгоритма. Для каждого из $O(\log^{s-1} N)$ наборов $K = (k_1, \ldots, k_s)$ нам требуется $O(s^4(s+\log N))$ времени для построения LLL-приведенного базиса и $2^{O(s^2)}$ времени для вычисления кратчайшего вектора. Тогда общее время работы алгоритма оценивается выражением

$$O(\log^{s-1} N) \cdot \left(O(s^4(s+\log N)) + 2^{O(s^2)}\right). \tag{4}$$

В третьей главе **"Параметр Бахвалова и оптимальные коэффициенты"** рассматривается применение алгоритма вычисления локальных минимумов решетки к нахождению параметров и оптимальных коэффициентов параллелепипедальных сеток Коробова. Для оптимизации вычислений вводится понятие эллиптических минимумов решетки и предлагается алгоритм для их вычисления. Этот алгоритм позволяет существенно ускорить вычисление оптимальных коэффициентов. В конце главы приводятся результаты вычислений оптимальных коэффициентов для размерностей $s = 2, 3$.

Для приближенного вычисления кратных интегралов функций на единичном s-мерном кубе $\mathcal{G}_s = [0,1]^s$ используются квадратурные формулы

$$\int\limits_{\mathcal{G}_s} f(\boldsymbol{x})\, \boldsymbol{dx} = \frac{1}{N} \sum_{k=1}^{N} f(\boldsymbol{x^{(k)}}) - R_N(f), \tag{5}$$

где $N \in \mathbb{N}$. Точки $\boldsymbol{x^{(1)}}, \ldots, \boldsymbol{x^{(N)}}$ называются ***узлами***, их совокупность — ***сеткой***, а величина $R_N(f)$ — ***погрешностью*** квадратурной формулы.

Пусть $a_1, \ldots, a_s$ — целые числа, для которых НОД$(a_1, \ldots, a_s, N) = 1$. Н.М. Коробов [7] предложил использовать параллелепипедальные сетки

$$\boldsymbol{x}^{(k)} = \left(\left\{\frac{a_1 k}{N}\right\}, \ldots, \left\{\frac{a_s k}{N}\right\}\right) \quad (k = 1, \ldots, N) \tag{6}$$

для подынтегральных функций, непрерывных в единичном s-мерном кубе и имеющих период 1 по каждой из переменных $x_1, \ldots, x_s$.

Будем говорить, что функция

$$f(\boldsymbol{x}) = \sum_{v_1,\ldots,v_s=-\infty}^{\infty} c(\boldsymbol{v})\, e^{2\pi i(\boldsymbol{v}\cdot\boldsymbol{x})}, \quad \text{где} \quad c(\boldsymbol{v}) = \int\limits_{\mathcal{G}_s} f(\boldsymbol{x})\, e^{-2\pi i(\boldsymbol{v}\cdot\boldsymbol{x})}\, \boldsymbol{dx}$$

принадлежит классу E_s^α, если для ее коэффициентов Фурье

$$|c(\boldsymbol{v})| \leqslant \frac{C}{|||\boldsymbol{v}|||^\alpha},$$

где $\alpha > 1$ — действительное число. Для погрешности квадратурной формулы (5) на классе E_s^α справедлива оценка

$$|R_N(f)| \leqslant C \sum_{\substack{\boldsymbol{v}\in\mathbb{Z}^n \\ N \,|\, \boldsymbol{a}\cdot\boldsymbol{v}}}{}' \frac{1}{|||\boldsymbol{v}|||^\alpha}.$$

[7] **Коробов Н.М.** Приближенное вычисление кратных интегралов с помощью методов теории чисел / Н.М. Коробов // Доклады Академии наук СССР. — 1957. — Т. 115, №6. — С. 1062-1065.

Суммирование здесь ведется по всем ненулевым целочисленным решениям $\boldsymbol{v} = (v_1, \ldots, v_s)$ сравнения

$$a_1 v_1 + \ldots + a_s v_s \equiv 0 \pmod{N}. \tag{7}$$

Задача состоит в том чтобы найти вектор $\boldsymbol{a} = (a_1, \ldots, a_s)$, минимизирующий сумму в правой части оценки для $|R_N(f)|$. Наибольшие слагаемые в этой сумме соответствуют решениям $\boldsymbol{v}$ сравнения (7) с наименьшими значениями $|||\boldsymbol{v}|||$. Так возникает идея о нахождении вектора $\boldsymbol{a}$, который делает величину

$$q(\boldsymbol{a}) = \min_{\substack{\boldsymbol{v}\in\mathbb{Z}^n\setminus\{\mathbf{0}\} \\ \boldsymbol{a}\cdot\boldsymbol{v}\equiv 0 \pmod{N}}} |||\boldsymbol{v}||| \tag{8}$$

как можно больше. Соответствующие значения $a_1, \ldots, a_s$ называются ***оптимальными коэффициентами***. Параметр $q(\boldsymbol{a})$ (***параметр Бахвалова***), определяемый равенством (8), был предложен Н.С. Бахваловым [8] и характеризует равномерную распределенность узлов параллелепипедальной сетки.

Назовем ненулевое целочисленное решение $\boldsymbol{v} = (v_1, \ldots, v_s)$ сравнения (7) ***локально минимальным***, если не существует другого ненулевого решения $\boldsymbol{v'} = (v'_1, \ldots, v'_s)$, такого что $|v'_i| \leqslant |v_i|$ для всех $i = 1, \ldots, s$ и при этом хотя бы одно из этих s неравенств строгое. Заметим, что при определении параметра Бахвалова $q(\boldsymbol{a})$ можно учитывать только локально минимальные решения, количество которых не превосходит $O(\log^{s-1} N)$. Это наблюдение, сделанное В.А. Быковским [5], позволяет свести задачу вычисления параметра Бахвалова к задаче нахождения множества всех локально минимальных решений сравнения (7).

Все целочисленные решения сравнения (7) составляют некоторую целочисленную решетку $\Gamma = \Gamma(\boldsymbol{a})$ в $\mathbb{R}^s$ определителя N. Локально минимальные решения соответствуют локальными минимумами решетки. В связи с этим мы можем рассматривать несколько более общую задачу — о вычислении множества локальных минимумов решетки Γ. Параметр Бахвалова

$$q(\boldsymbol{a}) = q(\Gamma) = \min_{\boldsymbol{v}\in\mathfrak{M}(\Gamma)} |||\boldsymbol{v}|||.$$

Для каждого набора $(k_1, \ldots, k_s)$ мы рассматриваем квадратичную форму

$$Q^{(K)}(\boldsymbol{m}) = \sum_{i=1}^{s} \left(2^{l_i} L_i(\boldsymbol{m})\right)^2 = \sum_{i=1}^{s} \left(2^{l_i} v_i\right)^2 = Q^{(K)}(\boldsymbol{v}).$$

Ее минимум

$$M^{(K)}(\Gamma) = \min_{\substack{\boldsymbol{m}\in\mathbb{Z}^s \\ \boldsymbol{m}\neq(0,\ldots,0)}} Q^{(K)}(\boldsymbol{m}) = \min_{\substack{\boldsymbol{v}\in\Gamma \\ \boldsymbol{v}\neq(0,\ldots,0)}} \sum_{i=1}^{s} \left(2^{l_i} v_i\right)^2 = \sum_{i=1}^{s} \left(2^{l_i} \overline{v}_i\right)^2$$

[8] **Бахвалов Н.С.** О приближенном вычислении кратных интегралов / Н.С. Бахвалов // Вестн. Моск. ун-та. Сер. Матем., мех., астрон., физ., хим. — 1959. — №4. — С. 3-18.

достигается на кратчайшем векторе "растянутой" решетки $\Gamma^{(K)}$ с координатами $\left(2^{l_1}\overline{v}_1,\ldots,2^{l_s}\overline{v}_s\right)$, определяющем узел $\overline{\boldsymbol{v}}$ исходной решетки Γ.

В пространстве переменных $(v_1,\ldots,v_s)$ — узлов решетки Γ неравенство

$$\sum_{i=1}^{s}\left(2^{l_i}v_i\right)^2 \leqslant M^{(K)}(\Gamma)$$

определяет эллипсоид с центром в начале координат, "вытянутый" вдоль некоторых координатных осей. Тот факт, что форма $Q^{(K)}(\boldsymbol{v})$ достигает минимума в узле $\overline{\boldsymbol{v}}$, говорит о том что внутри этого эллипсоида нет ненулевых узлов решетки Γ. Это означает, что для узла $\overline{\boldsymbol{v}}$ (назовем такой узел ***эллиптическим минимумом*** решетки Γ) выполняются условия из определения локального минимума. Мы можем ограничиться включением вектора $\overline{\boldsymbol{v}}$ в список локальных минимумов и не перебирать с помощью алгоритма Fincke-Pohst все решения неравенства

$$Q_L^{(K)}(\boldsymbol{m}) \leqslant 4s\cdot M^{(K)}(\Gamma).$$

В результате, мы избавимся от экпоненциального вклада во времени работы алгоритма (см. оценку (4)), но получим лишь множество эллиптических минимумов $\widetilde{\mathfrak{M}}(\Gamma)$.

Для ***приближенного параметра Бахвалова***

$$\widetilde{q}(\Gamma) = \min_{\boldsymbol{v}\in\widetilde{\mathfrak{M}}(\Gamma)} |||\boldsymbol{v}|||$$

справедлива

Теорема 3. *Для любой s-мерной целочисленной решетки* Γ

$$q(\Gamma) \leqslant \widetilde{q}(\Gamma) \leqslant 8^{s/2}q(\Gamma).$$

С помощью алгоритма приближенного вычисления параметра Бахвалова можно существенно ускорить вычисление оптимальных коэффициентов. Для некоторого множества S решеток Γ вычисление

$$Q(S) = \max_{\Gamma\in S} q(\Gamma)$$

можно организовать в два шага. Учитывая только эллиптические минимумы, с помощью "быстрого" варианта алгоритма находим значение

$$\widetilde{Q}(S) = \max_{\Gamma\in S} \widetilde{q}(\Gamma).$$

Затем для небольшого числа "экстремальных" решеток $\Gamma\in S$, на которых достигается максимум $\widetilde{Q}(S)$, вычисляем значения $q(\Gamma)$, учитывая *все* локальные минимумы. Если хотя бы для одной "экстремальной" решетки Γ выполняется равенство $q(\Gamma)=\widetilde{q}(\Gamma)$, то вычисленный на первом шаге максимум $\widetilde{Q}(S)$ совпадает с искомым значением $Q(S)$. Числа $a_1,\ldots,a_s$, определяющие любую "экстремальную" решетку Γ, будут оптимальными коэффициентами.

Предложенная схема вычислений позволяет существенно сократить время вычисления оптимальных коэффициентов. Перебор всех локальных минимумов мы осуществляем только для небольшого числа "экстремальных" решеток, в то время как для остальных решеток мы ограничиваемся рассмотрением лишь эллиптических минимумов.

Отметим, что для набора $K \in \mathcal{K}_s(N)$ LLL-приведенный базис соответствующей "растянутой" решетки $\Gamma^{(K)}$ не всегда содержит среди своих элементов кратчайший вектор решетки $\Gamma^{(K)}$, определяющий эллиптический минимум $\overline{\boldsymbol{v}}$ исходной решетки Γ. Поэтому, используя LLL-приведенные базисы, мы можем упустить некоторые эллиптические минимумы. Однако, это не является существенным. Основная идея рассмотренной схемы состоит в вычислении

$$\max_{\Gamma \in S} q(\Gamma),$$

учитывая только вектора некоторого легко вычисляемого подмножества множества локальных минимумов (например, множества эллиптических минимумов) и последующей проверки того что для "экстремальных" решеток значение $q(\Gamma)$ не уменьшается при учете всех локальных минимумов.

В конце третьей главы приводятся результаты вычислений оптимальных коэффициентов для размерностей $s = 2, 3$. Пусть $N = 2^r$, где r — натуральное число. Наиболее привлекательны с практической точки зрения параллелепипедальные сетки вида (6) с коэффициентами $a_i = l^{i-1} \bmod N$ $(1 \leqslant i \leqslant s)$, где целое l принимает нечетные значения от 1 до $2^{r-1} - 1$.

В этом случае все целочисленные решения $\boldsymbol{v} = (v_1, \ldots, v_s)$ сравнения (7) составляют целочисленную решетку $\Gamma_{2^r}(l)$ определителя N с базисом

$$B_{2^r} = \begin{pmatrix} N & -a_2 & \cdots & -a_s \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Наша задача состоит в нахождении значения параметра l, для которого величина $q(\Gamma_{2^r}(l))$ достигает наибольшего значения

$$\max_{l} q(\Gamma_{2^r}(l)).$$

Для проведения вычислений разработана программная реализация рассмотренных в работе алгоритмов с использованием языка программирования C++. Для работы с большими числами используется библиотека NTL (Number Theory Library). Для лучшей производительности библиотека NTL используется вместе с GMP (GNU Multi-Precision library). Разработана программная реализация для проведения вычислений на многопроцессорных вычислительных комплексах с использованием интерфейса MPI (Message Passing Interface). Вычислительные эксперименты проводились на Linux кластере в Институте прикладной математике ДВО РАН в городе Владивостоке.

Автор выражает искреннюю благодарность своему научному руководителю В.А. Быковскому за всестороннюю поддержку на всех этапах выполнения работы.

Основные результаты диссертации

- Получен явный вид трехмерных областей Валена первого и второго типов, что уточняет теорему Валена.
- При нахождении областей Валена разработана методика, позволяющая легко получить известные ранее оценки для локальных минимумов, составляющих базис Минковского.
- На основе предложенной В.А. Быковским теоретической схемы разработан алгоритм для вычисления локальных минимумов целочисленных решеток.
- Разработан алгоритм для вычисления параметра Бахвалова и оптимальных коэффициентов параллелепипедальных сеток Коробова с помощью локальных минимумов.
- Построена модификация алгоритма вычисления локальных минимумов, позволяющая вычислять параметр Бахвалова приближенно и существенно ускорить вычисление оптимальных коэффициентов.
- Разработана программная реализация построеных алгоритмов.
- Вычислены значения оптимальных коэффициентов параллелепипедальных сеток Коробова для размерностей пространства $s = 2, 3$.

Публикации по теме диссертации

1. **Гассан С.В. О параметре оптимальности параллелепипедальных сеток Коробова для кубатурных формул / В.А. Быковский, С.В. Гассан // Журнал вычислительной математики и математической физики. — 2011. — Т. 51. — №8. — С. 1363-1369.**

2. **Гассан С.В. Алгоритм вычисления локальных минимумов целочисленных решеток и его приложения / В.А. Быковский, С.В. Гассан // Вестник Тихоокеанского государственного университета. — 2011. — №1(20). — С. 39-48.**

3. **Гассан С.В.** Структура областей Валена для трехмерных решеток / С.В. Гассан // Чебышевский сборник. — 2005. — Т. VI. — Вып. 3(15). — Тула: Изд-во Тул. гос. пед. ун-та им. Л.Н. Толстого, 2005. — С. 51-84.

4. **Гассан С.В.** Алгоритм вычисления локальных минимумов целочисленных решеток и его приложения / В.А. Быковский, С.В. Гассан // Суперкомпьютеры: вычислительные и информационные технологии: материалы международной научно-практической конференции. — Хабаровск: Изд-во Тихоокеан. гос. ун-та, 2010. — С. 21-29.

5. **Гассан С.В.** О вычислении дискретных эллиптических минимумов целочисленных решеток / С.В. Гассан // XXXV Дальневосточная мате-

матическая школа-семинар имени академика Е.В. Золотова: сб. докл. (электронный ресурс). — Владивосток: ИАПУ ДВО РАН, 2010. — С. 56-62.

6. **Гассан С.В.** О вычислении локальных минимумов целочисленных решеток / С.В. Гассан // Международный симпозиум "Образование, наука и производство: проблемы, достижения и перспективы": материалы Всероссийской конференции "Школа по фундаментальным основам моделирования обработки материалов" и научно-технической конференции "Математическое, вычислительное и информационное обеспечение технологических процессов и систем": В 5т. Т.4. — Комсомольск-на-Амуре: ГОУВПО "КнАГТУ", 2010. — С. 265-268.

7. **Gassan S.V.** Parallel implementation of the algorithm for calculating local minima of integral lattices / S.V. Gassan // First Russia and Pacific conference on computer technology and applications: electronic conference proceedings. — Vladivostok: IACP FEB RAS, 2010. — P. 183-187.

Гассан Сергей Владимирович

Вычислительные алгоритмы в геометрии чисел

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Подписано в печать 05.12.2011.
Формат 60x84/16. Усл. п. л. 1. Уч.-изд. л. 1.1.
Тираж 100 экз.

Отпечатано в ИПМ ДВО РАН.
690041, г. Владивосток, ул. Радио, 7.