УДК 519.644.7+511.9

АЛГОРИТМ ВЫЧИСЛЕНИЯ ЛОКАЛЬНЫХ МИНИМУМОВ ЦЕЛОЧИСЛЕННЫХ РЕШЕТОК И ЕГО ПРИЛОЖЕНИЯ

Быковский В. А. – чл.-корр. РАН, профессор, директор Хабаровского отделения Института прикладной математики ДВО РАН, тел. (4212) 32-46-76, e-mail: vab@iam.khv.ru; *Гассан С. В.* – мл. науч. сотрудник, тел. (4232) 31-19-18, e-mail: svgas@dvo.ru (Институт прикладной математики ДВО РАН)

Рассматривается алгоритм вычисления множества локальных минимумов целочисленных решеток. Обсуждаются детали программной реализации и варианты оптимизации. Предлагается модификация алгоритма для вычисления множества эллиптических минимумов. Рассматривается применение предложенных алгоритмов для вычисления параметров теории многомерных квадратурных формул Коробова.

In the paper we consider the algorithm for finding local minima of integral lattices. We discuss the details of the software implementation and the ways of optimization. We also propose the modification of the algorithm allowing to calculate elliptic minima and consider the application of these algorithms to computing parameters from the theory of Korobov's multidimensional quadrature formulas.

Ключевые слова: целочисленные решетки, локальные минимумы, приведенные квадратичные формы.

Введение

В геометрии чисел *решеткой* называют множество всех целочисленных линейных комбинаций произвольно заданных линейно независимых векторов пространства, являющихся *базисом* решетки. В случае, когда координаты векторов базиса также являются целыми числами, мы говорим о *целочисленных решетках*. Более формально любую целочисленную решетку в R^n можно записать в виде:

$$\Gamma = \left\{ v = L(m) = m_1 b^{(1)} + \ldots + m_n b^{(n)} \;\middle|\; m_1, \ldots, m_n \in Z \right\}$$

(символ Z обозначает множество всех целых чисел 0, ±1, ±2, …), где элементы базиса $<b^{(1)},\ldots,b^{(n)}>$ составлены из соответствующих столбцов целочисленной матрицы:

$$B = \begin{pmatrix} \begin{pmatrix} b_{11} \\ \cdots \\ b_{n1} \end{pmatrix} & \cdots & \begin{pmatrix} b_{1n} \\ \cdots \\ b_{nn} \end{pmatrix} \end{pmatrix}, \quad b_{ij} \in Z,$$

определяющей невырожденное линейное преобразование:

$$m = \begin{pmatrix} m_1 \\ \cdots \\ m_n \end{pmatrix} \to L(m) = \begin{pmatrix} L_1(m) \\ \cdots \\ L_n(m) \end{pmatrix} = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ & \cdots & \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ \cdots \\ m_n \end{pmatrix},$$

где:

$$L_i(m) = m_1 b_{i1} + \ldots + m_n b_{in}$$

линейные формы с целочисленными коэффициентами. Величину:

$$N = N(\Gamma) = |\det(B)|$$

называют *определителем* решетки.

В теории многомерных квадратурных формул Н. М. Коробова (см. [1]) важную роль играет параметр:

$$Q(\Gamma) = \min_{\substack{v \in \Gamma \\ v \neq (0,\ldots,0)}} \prod_{i=1}^{n} \max\{1, |v_i|\},$$

введенный Н. С. Бахваловым. В работе [2] предложен алгоритм вычисления $Q(\Gamma)$, который основывается на теории приведения положительно определенных квадратичных форм и концепции локальных минимумов решеток, предложенной в конце девятнадцатого века независимо Г. Ф. Вороным [3] и Г. Минковским [4].

По определению, ненулевой узел:

$$\gamma = (\gamma_1, \ldots, \gamma_n)$$

произвольной решетки Γ в R^n (в том числе и целочисленной) называется *локальным минимумом*, если не существует другого ненулевого узла:

$$\eta = (\eta_1, \ldots, \eta_n)$$

решетки Γ, для которого:

$$|\eta_i| \le |\gamma_i|, \quad i = 1, \ldots, n,$$

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

Обозначим через М(Γ) множество всех локальных минимумов решетки Γ. По теореме Минковского о выпуклом теле, для локальных минимумов выполняется неравенство:

$$|\gamma_1 \cdots \gamma_n| \le N(\Gamma).$$

Для локальных минимумов $v = (v_1, \ldots, v_n)$ целочисленных решеток Γ из него непосредственно следует, что:

$$\prod_{i=1}^{n} \max\{1, |v_i|\} \le N(\Gamma).$$

Это означает, что множество M(Γ) конечно. Более того, для количества его элементов выполняется оценка:

$$\#\mathrm{M}(\Gamma) \le C(n) \cdot (\log N)^{n-1}$$

с некоторой положительной константой $C(n)$ и $N>1$. Заметим, что:

$$Q(\Gamma) = \min_{v \in \mathrm{M}(\Gamma)} \prod_{i=1}^{n} \max\{1, |v_i|\}.$$

Поэтому для нахождения величины $Q(\Gamma)$ достаточно вычислить все локальные минимумы из M(Γ).

В настоящей работе мы рассматриваем практическую реализацию алгоритма вычисления множества локальных минимумов, предложенного в [2]. Для эффективного вычисления параметров теории многомерных квадратурных формул Коробова мы предлагаем новую версию алгоритма, основанную на понятии эллиптических минимумов.

Работа выполнена при финансовой поддержке ДВО РАН (проект 09-I-П4-01).

Теоретическая схема алгоритма

Обозначим через $\mathrm{K_n}(N)$ множество всех наборов неотрицательных целых чисел $K = (k_1, \ldots, k_n)$, для которых:

$$k_1 + \ldots + k_n \le n/2 + \log_2 N,$$

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

$$Q^{(K)}(m_1, \ldots, m_n) = \sum_{i=1}^{n} \left(\frac{L_i(m)}{2^{k_i}} \right)^2. \qquad (1)$$

По определению, величина:

$$M^{(K)}(\Gamma) = \min_{\substack{m \in Z^n \\ m \ne (0,\ldots,0)}} Q^{(K)}(m)$$

есть минимум квадратичной формы.

Определим множество:

$$\widetilde{\mathrm{M}}(\Gamma) = \bigcup_{K \in \mathrm{K}_n(N)} \left\{ L(m) \mid m \in Z^n;\ Q^{(K)}(m) \le 4n \cdot M^{(K)}(\Gamma) \right\}. \qquad (2)$$

В работе [2] показано, что имеет место включение:

$$\mathrm{M}(\Gamma) \subset \widetilde{\mathrm{M}}(\Gamma).$$

Здесь возникает вопрос об ограничениях на область изменения целочисленных решений $m = (m_1, \ldots, m_n)$ неравенств:

$$Q^{(K)}(m) \le 4n \cdot M^{(K)}(\Gamma),$$

определяющих множество (2). А именно, ограничены ли они константой, не зависящей от размера задачи N. Легко проверить на конкретных примерах, что интервалы изменения переменных m_i могут увеличиваться с ростом N. Проблему удается решить с помощью теории приведения квадратичных форм.

Приведенные базисы и квадратичные формы

Заметим, что квадратичная форма (1) представляет собой сумму квадратов координат или скалярный квадрат вектора решетки с базисом:

$$B^{(K)} = \begin{pmatrix} \begin{pmatrix} \frac{b_{11}}{2^{k_1}} \\ \cdots \\ \frac{b_{n1}}{2^{k_n}} \end{pmatrix} & \cdots & \begin{pmatrix} \frac{b_{1n}}{2^{k_1}} \\ \cdots \\ \frac{b_{nn}}{2^{k_n}} \end{pmatrix} \end{pmatrix}.$$

Можно записать:

$$Q^{(K)}(m) = \left(B^{(K)} m\right)^T \cdot \left(B^{(K)} m\right) = m^T \left(\left(B^{(K)}\right)^T B^{(K)}\right) m.$$

Базис решетки определен неоднозначно. При размерности $n > 1$ решетка имеет бесконечно много базисов. Например, для произвольной унимодулярной матрицы S произведение $B' = B\,S$ также является базисом решетки.

Однако некоторые базисы представляют больший интерес, чем другие. А именно, наиболее полезными оказываются базисы, которые состоят из коротких и почти ортогональных векторов. Такие базисы называются *приведенными* (*reduced*). Им соответствуют *приведенные* квадратичные формы.

Понятие приведенного базиса не является каноническим. Впервые идея выбора определенных «коротких» векторов появилась в работах Гаусса для 2-мерного случая. Эрмит обобщил определения Гаусса на случай произвольной размерности. Более сильное определение, данное Коркиным и Золотаревым, в литературе обычно приписывается Эрмиту, и соответствующие базисы называются «приведенными по Эрмиту». В конце XIX века Минковский предложил свое определение приведенного базиса, потребовав, чтобы каждый базисный вектор был «как можно короче».

Проблема заключается в том, что не существует такого алгоритма, который находил бы приведенный базис за быстрое время, за исключением случаев размерности 2 и 3 (алгоритмы Гаусса [5] и B. Vallee [6] соответственно).

В 1982 году троим исследователям Lenstra, Lenstra и Lovász удалось осуществить идею построения такого приведенного базиса, чтобы его можно было вычислять за полиномиальное время [7]. Предложенные приведенные базисы получили название LLL-приведенных. Хотя такое определение «приведенности» является более слабым, преимущество в быстродействии позволило алгоритму LLL-приведения получить широкое распространение в приложениях.

Для того, чтобы сформулировать определения приведенных базисов, напомним процесс ортогонализации Грамма-Шмидта. Пусть $b_1,\ldots,b_n$ – линейно независимые векторы в пространстве R^n. Определим по индукции:

$$b_i' = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j' \quad (1 \le i \le n),$$

где:

$$\mu_{i,j} = \frac{(b_i, b_j')}{(b_j', b_j')} \quad (1 \le j < i \le n).$$

Тогда векторы:

$$b_1', \ldots, b_n'$$

попарно ортогональны и представляют собой базис пространства R^n. Здесь (a, b) обозначает скалярное произведение векторов a и b. Заметим также, что вектор b'_i представляет собой проекцию b_i на ортогональное дополнение пространства:

$$\sum_{j=1}^{i-1} \mathrm{R}\ b_j = \sum_{j=1}^{i-1} \mathrm{R}\ b_j'.$$

Процесс ортогонализации Грамма-Шмидта позволяет для данного базиса $B = (b_1,\ldots,b_n)$ решетки Γ находить его ортогональную проекцию $(b'_1,\ldots,b'_n)$. Понятно, что получаемые при этом ортогональные векторы, вообще говоря, не являются точками решетки Γ.

Базис $B = (b_1,\ldots,b_n)$ решетки Γ будем называть *собственным*, если для получаемых в процессе ортогонализации Грамма-Шмидта коэффициентов выполняются неравенства:

$$\left|\mu_{i,j}\right| \le \frac{1}{2} \quad (1 \le j < i \le n).$$

Сформулируем теперь определение приведенных базисов. Базис $(b_1,\ldots,b_n)$ решетки Γ в R^n называется:

– *LLL приведенным*, если он является собственным и для $i = 2,\ldots,n$ выполняются неравенства:

$$\frac{3}{4}\left|b_{i-1}'\right|^2 \le \left|b_i' + \mu_{i,i-1} b_{i-1}'\right|^2 \quad (1 < i \le n);$$

– *приведенным по Эрмиту*, если он является собственным, и для $i = 1,\ldots,n$, b'_i является кратчайшим вектором среди векторов проекции решетки Γ на ортогональное дополнение пространства:

$$\sum_{j=1}^{i-1} \mathrm{R}\ b_j;$$

– *приведенным по Минковскому*, если для $i = 1,\ldots,n$, b_i является кратчайшим вектором решетки Γ, который может быть дополнен до базиса $(b_1,\ldots,b_i)$ решетки Γ.

В рассматриваемом нами алгоритме вычисления локальных минимумов приведенные базисы нужны по двум причинам.

1. Для того, чтобы ограничить интервалы изменения переменных в неравенствах, определяющих множество (2). Можно показать, что в случае приведенных базисов все целочисленные решения этих неравенств покоординатно ограничены константой, зависящей только от размерности пространства n.

2. Для нахождения минимума $M^{(K)}(\Gamma)$ – квадрата длины кратчайшего ненулевого вектора решетки. В случае базисов, приведенных по Минковскому или Эрмиту, первый базисный элемент представляет собой кратчайший вектор решетки.

В представленной в работе [2] теоретической схеме алгоритма предлагается использовать базисы, приведенные по Минковскому. В работе [8] описан алгоритм для нахождения такого базиса в случае размерности $n = 2,\ldots,6$. Для исходного базиса вначале выполняется LLL-приведение. Очень часто LLL-приведенный базис является также приведенным по Минковскому. Если нет, то обычно остается только один-два шага-итерации, чтобы «привести» его окончательно.

В случае произвольной размерности n вычисление приведенного по Минковскому базиса требует наибольших временных затрат по сравнению с двумя другими вариантами приведения. Хотя алгоритм вычисления базиса, приведенного по Эрмиту менее трудоемкий, время его работы также возрастает экспоненциально с ростом размерности пространства n.

Алгоритм построения LLL-приведенного базиса, наиболее привлекательный с точки зрения быстродействия, позволяет аппроксимировать кратчайший вектор решетки с точностью до множителя $2^{(n-1)/2}$. Очень часто LLL-приведенный базис содержит среди своих элементов кратчайший вектор решетки. Однако в общем случае это не так.

Вычисление кратчайшего вектора решетки

Алгоритмы нахождения кратчайшего вектора решетки можно разделить на две группы: алгоритмы перечисления и алгоритмы просеивания. Хотя алгоритмы просеивания имеют лучшую асимптотическую оценку $2^{O(n)}$, на практике они уступают алгоритмам перечисления с оценкой $2^{O(n^2)}$, по крайней мере, до размерности $n = 50$. А для таких размерностей рассматриваемые алгоритмы уже неосуществимы за приемлемое время на современной вычислительной технике.

Алгоритмы перечисления систематически исследуют область пространства (с центром в начале координат), которая гарантированно содержит кратчайший вектор. Время работы таких алгоритмов пропорционально количеству точек решетки в области, что, в свою очередь, зависит от качества входного базиса.

Мы будем использовать алгоритм перечисления Fincke-Pohst [9], который, принимая на входе LLL-приведенный базис, соответствующий квадра-

тичной форме $Q(x)$, работает следующим образом. Для заданной константы C мы перебираем все векторы решетки, удовлетворяющие неравенству:

$$Q(x) \le C .$$

В случае, если матрица квадратичной формы является диагональной:

$$Q(x) = q_{11} x_1^2 + q_{22} x_2^2 + \ldots + q_{nn} x_n^2 ,$$

мы выбираем:

$$|x_1| \le \sqrt{C / q_{11}} .$$

После каждого выбора x_1 выбираем:

$$|x_2| \le \sqrt{(C - q_{11} x_1^2)/ q_{22}} ,$$

и т. д. В общем случае мы используем разложение Холеского, чтобы привести квадратичную форму к виду:

$$Q(x) = \sum_{i=1}^{n} q_{ii} \left(x_i + \sum_{j=i+1}^{n} q_{ij} x_j \right)^2 .$$

После этого действуем аналогично случаю диагональной матрицы, начиная с выбора переменной x_n.

Алгоритмическая модель

Каждому набору K из $K_n(N)$ (см. раздел 2) сопоставим положительно определенную квадратичную форму:

$$Q^{(K)}(m_1,\ldots,m_n) = \sum_{i=1}^{n} \left(2^{l_i} L_i(m)\right)^2 ,$$

где:

$$l_i = \max\{k_1,\ldots,k_n\} - k_i .$$

Ей соответствует решетка с целочисленным базисом:

$$B^{(K)} = \begin{pmatrix} \begin{pmatrix} 2^{l_1} b_{11} \\ \cdots \\ 2^{l_n} b_{n1} \end{pmatrix} & \cdots & \begin{pmatrix} 2^{l_1} b_{1n} \\ \cdots \\ 2^{l_n} b_{nn} \end{pmatrix} \end{pmatrix}.$$

Находим LLL-приведенный базис:

$$B_L^{(K)} = B^{(K)} \cdot S = \begin{pmatrix} \begin{pmatrix} 2^{l_1} b'_{11} \\ \cdots \\ 2^{l_n} b'_{n1} \end{pmatrix} & \cdots & \begin{pmatrix} 2^{l_1} b'_{1n} \\ \cdots \\ 2^{l_n} b'_{nn} \end{pmatrix} \end{pmatrix}$$

(S – некоторая унимодулярная матрица), который соответствует приведенной квадратичной форме:

$$Q_L^{(K)}(m) = \sum_{i=1}^{n}\left(2^{l_i}\left(m_1 b'_{i1} + \ldots + m_n b'_{in}\right)\right)^2 = \sum_{i=1}^{n}\left(2^{l_i} L_i^{(K)}(m)\right)^2 .$$

Обозначим через v_L кратчайший вектор среди элементов базиса $B_L^{(K)}$ и через $M_L = |v_L|^2$ квадрат его длины. Положим, $M = M_L$. Для базиса $B_L^{(K)}$ выполняем алгоритм Fincke-Pohst с константой $C = M_L$. Для каждого вектора v, выдаваемого алгоритмом:

1. Если $|v|^2 < |v_L|^2$, то $M = |v|^2$;
2. рассматривая v в качестве кандидата на локальный минимум, проверяем, можно ли его включить в список локальных минимумов.

В случае, если $M_L < 4n \cdot M$, выполняем алгоритм Fincke-Pohst с константой $C = 4n \cdot M$, не перебирая при этом уже рассмотренные векторы. Для каждого вектора v рассматриваем возможность включения его в список локальных минимумов.

Эллиптические минимумы

Для каждого набора K из $K_n(N)$ минимум квадратичной формы:

$$Q^{(K)}(m) = \sum_{i=1}^{n}\left(2^{l_i} L_i(m)\right)^2 = \sum_{i=1}^{n}\left(2^{l_i} u_i\right)^2 = Q^{(K)}(u),$$

$$M^{(K)}(\Gamma) = \min_{\substack{m \in Z^n \\ m \neq (0,\ldots,0)}} Q^{(K)}(m) = \min_{\substack{u \in \Gamma \\ u \neq (0,\ldots,0)}} \sum_{i=1}^{n}\left(2^{l_i} u_i\right)^2 = \sum_{i=1}^{n}\left(2^{l_i} \bar{u}_i\right)^2$$

достигается на кратчайшем векторе с координатами:

$$\left(2^{l_1}\bar{u}_1, \ldots, 2^{l_n}\bar{u}_n\right),$$

определяющими узел $\bar{u}$ решетки Г. В пространстве переменных ($u_1, \ldots, u_n$) – узлов решетки неравенство:

$$\sum_{i=1}^{n}\left(2^{l_i} u_i\right)^2 \leq M^{(K)}(\Gamma)$$

определяет эллипсоид с центром в начале координат, «вытянутый» вдоль некоторых координатных осей. Тот факт, что форма $Q^{(K)}(u)$ достигает минимума в узле $\bar{u}$, говорит о том, что внутри этого эллипсоида нет ненулевых узлов решетки. Это означает, что для узла $\bar{u}$ выполняются условия из определения локального минимума: не существует другого ненулевого узла $v = (v_1, \ldots, v_n)$ решетки, для которого:

$$|v_i| \leq |\bar{u}_i|, \quad i = 1, \ldots, n,$$

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

Назовем ненулевой узел:

$$\gamma = (\gamma_1, \ldots, \gamma_n)$$

произвольной решетки Γ в R^n (в том числе и целочисленной) *эллиптическим минимумом*, если можно указать проходящий через него эллипсоид с центром в начале координат и осями, совпадающими с координатными осями, – такой, что внутри него нет ненулевых узлов решетки Γ. Рассматриваемый нами узел $\bar{u}$ как раз и является эллиптическим минимумом. Поскольку любой эллиптический минимум является также локальным минимумом, множество эллиптических минимумов решетки Γ является подмножеством множества локальных минимумов M(Γ).

Сделанные наблюдения позволяют упростить рассматриваемый нами алгоритм вычисления локальных минимумов. Для каждого набора K из $K_n(N)$ кратчайший вектор соответствующей «растянутой» решетки гарантированно определяет локальный минимум $\bar{u}$ исходной решетки Γ. Мы можем ограничиться включением вектора $\bar{u}$ в список локальных минимумов и не перебирать решения неравенств, определяющих множество (2). Как уже было сказано, получаемое в таком случае множество будет подмножеством множества M(Γ).

В теории многомерных квадратурных формул Н. М. Коробова представляют интерес максимальные значения параметра:

$$Q(\Gamma) = \min_{\substack{v\in\Gamma \\ v\neq(0,\ldots,0)}} \prod_{i=1}^{n} \max\{1, |v_i|\}$$

на определенных множествах решеток. Для множества S решеток Γ вычисление:

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

можно выполнить в два шага. Используя «упрощенную» версию алгоритма вычисления локальных минимумов, находим значение максимума $M_e(\mathrm{S})$.

Затем для небольшого числа «экстремальных» решеток Γ, на которых достигается максимум $M_e(\mathrm{S})$, вычисляем значения $Q(\Gamma)$, учитывая *все* локальные минимумы. Если хотя бы для одной «экстремальной» решетки Γ значение $Q(\Gamma)$ не изменилось, то вычисленный на первом шаге максимум $M_e(\mathrm{S})$ совпадает с искомым $M(\mathrm{S})$.

Из эвристических соображений можно предположить, что внутренний минимум, с большой вероятностью, достигается именно на эллиптических минимумах, и, поэтому, значение внешнего максимума не уменьшается. В данном случае это легко проверить.

Заключение

Для рассмотренных алгоритмов разработана программная реализация на языке C++. Для работы с большими числами используется библиотека Number Theory Library (NTL) [10]. Разработана программная реализация алгоритмов для проведения вычислений на многопроцессорных вычислительных комплексах с использованием интерфейса MPI [11].

Библиографические ссылки

1. *Коробов Н. М.* О приближенном вычислении кратных интегралов // Докл. АН СССР. 1959. – Т. 124. – № 6.

2. *Быковский В. А.* Алгоритм вычисления локальных минимумов решеток. // Докл. РАН. – 2004. – Т. 399, № 5.

3. *Вороной Г. Ф.* Собрание сочинений. – Т. 1. – Киев: 1952.

4. *H. Minkowski.* Generalisation de la theorie des fractions continues, Ann. de lEcole Norm. (3), 13:2 (1896).

5. *H. Cohen.* A Course in Computational Algebraic Number Theory, Graduate Texts in Math., vol. 138, Springer-Verlag, Berlin Heidelberg, 1993. (Algorithm 1.3.14.).

6. *B. Vallee.* Une approche géométrique des algorithmes de réduction en petite dimension, Thesis, Univ. of Caen, 1986.

7. *A. K. Lenstra, H. W. Lenstra and L. Lovász.* Factoring polynomials with rational coefficients, Math. Ann. 261 (1982).

8. *Рышков С. С.* К теории приведения положительных квадратичных форм по Эрмиту-Минковскому, Исследования по теории чисел // 2, Зап. научн. сем. ЛОМИ, 33, Наука, Л., 1973.

9. *U. Fincke and M. Pohst.* Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, Math. Comp. 44 (1985).

10. http://www.shoup.net/ntl/

11. http://www.mcs.anl.gov/research/projects/mpi/