

МИНИМИЗАЦИЯ ЧЁТНЫХ КОНИЧЕСКИХ ФУНКЦИЙ НА ДВУМЕРНОЙ ЦЕЛОЧИСЛЕННОЙ РЕШЁТКЕ

Д. В. Грибанов^а, Д. С. Малышев^б

Национальный исследовательский университет «Высшая школа экономики»,
ул. Большая Печёрская, 25/12, 603155 Нижний Новгород, Россия
E-mail: ^аdimitry.gribanov@gmail.com, ^бdsmalyshev@rambler.ru

Аннотация. Рассматривается задача построения последовательных минимумов двумерной целочисленной решётки относительно порядка, заданного некоторой конической функцией f . Для указанной задачи предлагается алгоритм со сложностью $3,32 \log_2 R + O(1)$ обращений к оракулу сравнения функции f , где R — радиус круговой области поиска, тогда как нижняя оценка сложности на данный момент составляет $3 \log_2 R + O(1)$. В настоящей работе приводится эффективный критерий проверки того, что заданные векторы двумерной решётки являются последовательными минимумами и образуют базис решётки. Также показывается, что аналогичная задача поиска последовательных минимумов для решёток размерности n может быть решена алгоритмом, использующим не более чем $O(n)^{2n} \log R$ обращений к оракулу сравнения. Результаты работы могут быть применены для поиска последовательных минимумов относительно любых выпуклых функций, заданных оракулом сравнения. Ил. 2, библиогр. 24.

Ключевые слова: квазивыпуклая функция, выпуклая функция, коническая функция, квазивыпуклый полином, целочисленная решётка, нелинейное целочисленное программирование, последовательные минимумы решётки, приведённый базис решётки.

Введение

Задача целочисленной минимизации (квази)выпуклых функций при (квази)выпуклых ограничениях является известным и интенсивно изучаемым обобщением задачи целочисленного линейного программирования [1–13].

Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект № 18–31–20001–мол-а-вед).

© Д. В. Грибанов, Д. С. Малышев, 2020

Целевая функция и ограничения могут быть определены явно или с помощью оракулов. В [4, 13] приводятся алгоритмы для решения задачи проверки непустоты множества $K \cap \mathbb{Z}^n$, где K — выпуклое множество, заданное сильным оракулом отделения, включённое в шар радиуса R . Количество обращений к оракулу отделения, производимое данными алгоритмами, зависит полиномиально от $\log R$. Модификация данного результата и хороший обзор приведены в работе [3], где получен алгоритм со сложностью $O(n)^n \text{poly}(\log R)$ обращений к оракулу отделения. Дополнительно в [3] приводится рандомизированный алгоритм со средней сложностью $O(n)^n \text{poly}(\log R)$ обращений к оракулу для задачи минимизации выпуклой функции f , заданной оракулом субградиента, на области $K \cap \mathbb{Z}^n$, где выпуклая область K задана сильным оракулом отделения. В [12, 14] предлагается новый подход, основанный на обобщении понятия центра масс на целочисленный случай.

Основным недостатком оракулов, упомянутых выше, является сложность их реализации. Более удобный путь состоит в использовании оракула сравнения или оракула 0-го порядка, вычисляющего значения функции в точках. Однако в [15] показано, что задача минимизации квазивыпуклой функции f на области $K = R \cdot B_2^n \cap \mathbb{Z}^n$, где $R \cdot B_2^n$ обозначает n -мерный шар радиуса R по евклидовой норме, не может быть решена алгоритмом с полиномиальным по $\log R$ количеством обращений к оракулу сравнения.

Задача целочисленной минимизации для выпуклых (и близких к ним) функций, заданных оракулом сравнения или оракулом 0-го порядка, рассмотрена в [1, 15, 16]. В [1] разработан алгоритм целочисленной минимизации дискретных строго квазивыпуклых функций, заданных оракулом сравнения на решётке \mathbb{Z}^2 . Оракульная сложность алгоритма из [1] не превосходит $2 \log_2^2 R + O(\log_2 R)$. В [16] рассмотрена симметричная версия данной задачи, когда функция f дополнительно является чётной. Полученный в [16] алгоритм имеет сложность $4 \log_2 R + O(1)$ обращений к оракулу 0-го порядка.

В [15] рассмотрен вопрос о построении сужения класса квазивыпуклых функций, оснащённых оракулом сравнения, для которого задача целочисленной минимизации при фиксированной размерности допускала бы решение алгоритмом, оракульная трудоёмкость которого зависит полиномиально от величины $\log R$. Более детально, в [15] введены классы конических и дискретно-конических функций. Класс конических функций содержит выпуклые функции, строго квазивыпуклые функции и квазивыпуклые полиномы как собственные подклассы. Для задачи минимизации конической функции f , оснащённой оракулом сравнения, на области $R \cdot B_2^n \cap \mathbb{Z}^n$ в [15] получен алгоритм с оракульной сложностью $O(n)^{2n} \log R$. Кроме того, в [15] доказана нижняя оценка на необходимое

количество обращений к оракулу $3^{n-1} \log_2(2R - 1)$. В предположении, что минимизируемая функция f дополнительно является чётной, дана нижняя оценка оракульной сложности $(2^n - 1) \log_2(R - 1)$.

Важной задачей, которая может быть сведена к задаче целочисленной нелинейной оптимизации, является задача построения векторов, образующих последовательные минимумы решётки относительно некоторой векторной нормы. Результаты работ [17, 18] показывают, что для евклидовой нормы данная задача может быть решена алгоритмом с общей трудоёмкостью $4^n \text{poly}(\text{size}(R))$, где $\text{size}(R)$ — длина битовой кодировки R . В [19, 20] разработан подход, который вместе с результатами из [17] позволяет решать рассматриваемую задачу рандомизированным алгоритмом со сложностью $2^{n+o(n)} \text{poly}(\text{size}(R))$. Отметим, что результаты указанных работ могут быть распространены и на более широкие классы норм.

В настоящей работе исследуем обобщённую задачу построения векторов, образующих последовательные минимумы решётки, относительно порядка, задаваемого произвольной конической функцией f . Для задачи произвольной размерности n будет получен алгоритм с трудоёмкостью $O(n)^{2n} \log R$ обращений к оракулу сравнения функции f , где R — радиус шара, содержащего векторы последовательных минимумов. Более детально будет рассмотрен случай $n = 2$ при дополнительном условии, что функция f чётная. Для данного случая предложен алгоритм с оракульной сложностью $3,32 \log_2 R + O(1)$, тогда как нижняя оценка сложности, приведённая в [15], составляет $3 \log_2 R + O(1)$.

1. Определения, обозначения и некоторые вспомогательные результаты

Обозначим через B_p^n n -мерный единичный шар по отношению к норме l_p , т. е. $B_p^n = \{x \in \mathbb{R}^n \mid \|x\|_p \leq 1\}$.

Для следующих множеств матриц, порождённых столбцами матрицы $B \in \mathbb{R}^{m \times n}$, будем использовать специальные обозначения и названия:

$$\text{cone}(B) = \{Bt \mid t \in \mathbb{R}_+^n\} — \text{конус},$$

$$\text{conv. hull}(B) = \left\{Bt \mid t \in \mathbb{R}_+^n, \sum_{i=1}^n t_i = 1\right\} — \text{выпуклая оболочка},$$

$$\text{affine}(B) = \left\{Bt \mid t \in \mathbb{R}^n, \sum_{i=1}^n t_i = 1\right\} — \text{аффинная оболочка},$$

$$\text{span}(B) = \{Bt \mid t \in \mathbb{R}^n\} — \text{линейная оболочка},$$

$$\Lambda(B) = \{Bt \mid t \in \mathbb{Z}^n\} — \text{решётка}.$$

Для произвольного множества $D \subseteq \mathbb{R}^n$ через $\text{int}(D)$ и $\text{br}(D)$ обозначим подмножества его *внутренних* и *граничных* точек соответственно. Подмножества *внутренних* и *граничных* точек множества $D \subseteq \mathbb{R}^n$

по отношению к аффинному подпространству $\text{affine}(D)$ обозначим через $\text{rel. int}(D)$ и $\text{rel. br}(D)$ соответственно.

Обозначим через $i : j = \{i, i+1, \dots, j\}$ множество целых чисел, начинающихся с i и заканчивающихся на j . Через x_i обозначим i -ю координату вектора $x \in \mathbb{R}^n$. Интервал между точками $y, z \in \mathbb{R}^n$ будем обозначать через $[y, z] = \{x = ty + (1-t)z \mid 0 \leq t \leq 1\}$. Для обозначения открытого интервала будем использовать символ (y, z) . Множество D называется *выпуклым*, если для любых $x, y \in D$ справедливо $[x, y] \subseteq D$. Через $\text{dom}(f)$ обозначим область определения функции f . Для точки $y \in \text{dom}(f)$ через $H_f^{\leq}(y)$ обозначим множество линий уровня функции f :

$$H_f^{\leq}(y) = \{x \in \text{dom}(f) \mid f(x) \leq f(y)\}.$$

Множества $H_f^{<}(y)$ и $H_f^{\geq}(y)$ определяются аналогичным образом.

Для обозначения индикаторов выполнения логических условий будем использовать нотацию Айверсона (см., например, [21, с. 11, 37]). Для логического условия A положим $[A] = 1$, если A истинно, и $[A] = 0$, если A ложно.

Рассмотрим множество функций $f: \text{dom}(f) \rightarrow \mathbb{R}$ таких, что область определения $\text{dom}(f) \subseteq \mathbb{R}^n$ является выпуклым множеством. Функция f называется *квазивыпуклой*, если

$$\forall x, y \in \text{dom}(f) \quad \forall z \in (x, y) \quad f(z) \leq \max\{f(x), f(y)\}.$$

Функция f называется *строго квазивыпуклой*, если

$$\forall x, y \in \text{dom}(f) \quad \forall z \in (x, y) \quad f(z) < \max\{f(x), f(y)\}.$$

Функция f называется *выпуклой*, если

$$\forall x, y \in \text{dom}(f) \quad \forall t \in (0, 1) \quad f(tx + (1-t)y) \leq tf(x) + (1-t)f(y).$$

Будем обозначать рассмотренные классы функций через QConv_n (quasi-convex), SQConv_n (strictly quasiconvex) и Conv_n (convex) соответственно. Обозначим через QCPoly_n класс квазивыпуклых полиномов ненулевой степени с действительными коэффициентами.

Функцию $f: \text{dom}(f) \rightarrow \mathbb{R}$ будем называть *ограниченной*, если для любого $\alpha \in \mathbb{R}$ множество $\{x \in \text{dom}(f) \mid f(x) \leq \alpha\}$ ограничено.

Для точек $x^{(1)}, x^{(2)}, \dots, x^{(k)} \in \mathbb{R}^n$ через $\text{cone}(x^{(1)}, \dots, x^{(k-1)} \mid x^{(k)})$ обозначим множество

$$x^{(k)} + \text{cone}(x^{(k)} - x^{(1)}, x^{(k)} - x^{(2)}, \dots, x^{(k)} - x^{(k-1)}), \quad (1)$$

которое представляет собой конус, образованный векторами $-x^{(1)}, \dots, -x^{(k-1)}$, дополнительно сдвинутый на $x^{(k)}$.

Определение 1. Пусть на множестве D задан линейный (полный) порядок \preceq . Пусть $f: \text{dom}(f) \rightarrow D$, где множество $\text{dom}(f)$ выпукло.

Функция f называется *конической*, если для всех $y, z \in \text{dom}(f)$ и $t \geq 0$ таких, что $f(y) \preceq f(z)$ и $z + t(z - y) \in \text{dom}(f)$, верно

$$f(z + t(z - y)) \succeq f(z).$$

Класс конических функций будем обозначать через Conic_n .

Замечание 1. Далее практически везде будем полагать $D = \mathbb{R}$ со стандартным порядком. Однако в доказательстве теоремы 5 потребуется использование $D = \mathbb{R}^2$ с лексикографическим порядком. Отметим, что все результаты работы справедливы и для наиболее общего случая.

Замечание 2. Нетрудно видеть, что класс Conic_n конических функций является подклассом класса квазивыпуклых функций, т. е. $\text{Conic}_n \subset \text{QConv}_n$. Включение является строгим: контрпримером является квазивыпуклая функция $\text{sgn}(x_1)$, не являющаяся конической.

Обозначим через $\text{MIN}_f(1)$ множество точек минимума функции f : $\text{MIN}_f(1) = \arg \min_{x \in \text{dom}(f)} f(x)$. Если множество $\text{MIN}_f(1)$ не определено, то положим $\text{MIN}_f(1) = \emptyset$. Аналогичным образом для $k \geq 2$ определим множество $\text{MIN}_f(k)$ точек k -го минимума функции f :

$$\text{MIN}_f(k) = \arg \min_{x \in \text{dom}(f) \setminus M} f(x), \quad \text{где } M = \bigcup_{i=1}^{k-1} \text{MIN}_f(i).$$

Если множество $\text{MIN}_f(k)$ не определено, то положим $\text{MIN}_f(k) = \emptyset$.

Следующая теорема, доказанная в [15], даёт несколько эквивалентных способов определения класса Conic_n .

Теорема 1. Пусть $f: \text{dom}(f) \rightarrow D$, где множество $\text{dom}(f) \subseteq \mathbb{R}^n$ выпуклое, а множество D оснащено отношением \preceq линейного порядка. Следующие определения эквивалентны.

(1) Для любой пары точек $y, z \in \text{dom}(f)$ и всех $t \geq 0$ таких, что $f(y) \preceq f(z)$ и $z + t(z - y) \in \text{dom}(f)$, верно неравенство

$$f(z + t(z - y)) \succeq f(z).$$

(2) Для любых точек $x^{(1)}, x^{(2)}, \dots, x^{(k)}, y \in \text{dom}(f)$ таких, что

$$f(x^{(1)}) \leq \dots \leq f(x^{(k)}), \quad y \in \text{cone}(x^{(1)}, \dots, x^{(k-1)} \mid x^{(k)}),$$

выполнено неравенство $f(y) \geq f(x^{(k)})$. Более того, можно дополнительно потребовать, чтобы точки $x^{(1)}, x^{(2)}, \dots, x^{(k)}$ находились в общем положении (любые $i \leq k$ точек аффинно независимы).

(3) Для любой точки $x \in \text{dom}(f)$ множество $H_f^{\leq}(x)$ выпукло (что эквивалентно квазивыпуклости f) и

$$\forall x \in \text{dom}(f) \setminus \text{MIN}_f(1) \quad H_f^{\leq}(x) \subseteq \text{rel. br}(H_f^{\leq}(x)).$$

Рис. 1 является иллюстрацией определений (1) и (2) из теоремы 1.

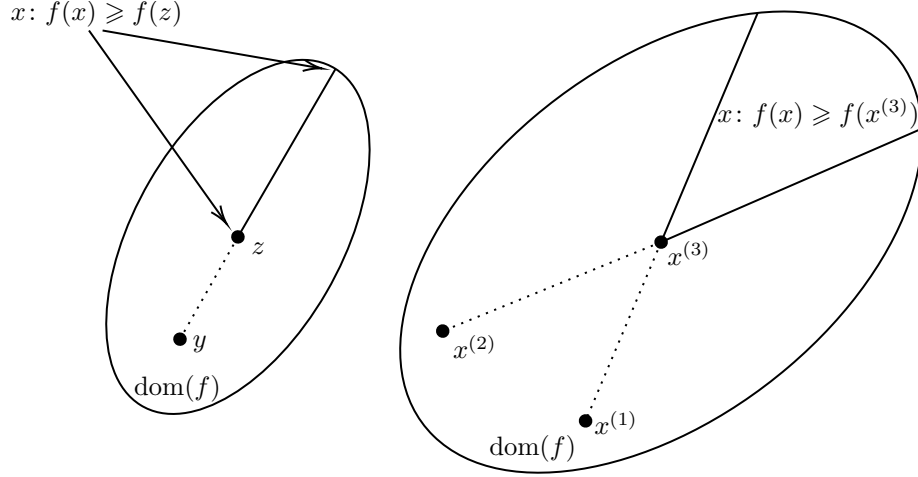


Рис. 1. Иллюстрация к теореме 1:
определение (1) слева и определение (2) справа

Следующие теоремы из [15] утверждают, что класс Conic_n конических функций содержит некоторые важные подклассы функций и замкнут относительно некоторых естественных операций.

Теорема 2. Справедливы следующие включения:

- (1) $\text{SQConv}_n \subset \text{Conic}_n \subset \text{QConv}_n$,
- (2) $\text{QCPoly}_n \subset \text{Conic}_n$,
- (3) $\text{Conv}_n \subset \text{Conic}_n$.

Теорема 3. (1) Пусть $f_i \in \text{Conic}_n$ и $w_i \in \mathbb{R}_+$ для любого $i \in 1:k$. Тогда функция $g(x) = \max_{i \in 1:k} \{w_i f_i(x)\}$ принадлежит классу Conic_n , где $\text{dom}(g) = \bigcap_{i \in 1:k} \text{dom}(f_i)$.

(2) Пусть $f \in \text{Conic}_n$ и $h: \mathbb{R} \rightarrow \mathbb{R}$ — коническая неубывающая функция. Тогда функция $g = h \circ f$ принадлежит классу Conic_n .

(3) Пусть $f \in \text{Conic}_m$, $A \in \mathbb{R}^{m \times n}$ и $b \in \mathbb{R}^m$. Тогда функция $g(x) = f(Ax + b)$, являющаяся аффинным образом $f(x)$, принадлежит классу Conic_n .

(4) Пусть $f_1, f_2 \in \text{Conic}_n$ и $D = \text{dom}(f_1) \cap \text{dom}(f_2)$. Тогда функция $g(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \end{pmatrix}: D \rightarrow \mathbb{R}^2$ является конической по отношению к лексикографическому порядку на \mathbb{R}^2 .

Функция f называется *чётной*, если для всех $x \in \text{dom}(f)$ верно $-x \in \text{dom}(f)$ и $f(x) = f(-x)$. Множество $D \subseteq \mathbb{R}^n$ называется *дискретным*,

если для любого $x \in D$ существует шар $B = x + R \cdot B_2^n$ радиуса $R > 0$ с центром в x такой, что $D \cap B = \{x\}$. Множество $D \subseteq \mathbb{R}^n$ называется *равномерно дискретным*, если существует шар $B = R \cdot B_2^n$ радиуса $R > 0$ такой, что для всех $x \in D$ верно $D \cap (x + B) = \{x\}$.

Определение 2. Пусть $f: \text{dom}(f) \rightarrow D$, где множество $\text{dom}(f) \subset \mathbb{R}^n$ дискретно, а множество D оснащено отношением \preceq линейного порядка. Функция f называется *дискретно-конической*, если для любых точек $y, x^{(1)}, x^{(2)}, \dots, x^{(k)} \in \text{dom}(f)$ таких, что

$$f(x^{(1)}) \leq f(x^{(2)}) \leq \dots \leq f(x^{(k)}), \quad y \in \text{cone}(x^{(1)}, x^{(2)}, \dots, x^{(k-1)} \mid x^{(k)}),$$

верно неравенство $f(y) \geq f(x^{(k)})$. Класс дискретно-конических функций будем обозначать через DConic_n .

Верно ли, что любую функцию класса DConic_n можно естественным образом продолжить до функции из класса Conic_n ? Теорема 4, доказанная в [15], даёт ответ на этот вопрос для ограниченных функций с равномерно дискретной областью определения.

Определение 3. Пусть $f \in \text{DConic}_n$. Функция $g \in \text{Conic}_n$ называется *продолжением функции f* , если

$$\text{dom}(g) = \text{conv.hull}(\text{dom}(f)) \quad \text{и} \quad g(x) = f(x) \quad \text{для} \quad x \in \text{dom}(f).$$

Рассмотрим ограниченную функцию $f \in \text{DConic}_n$ такую, что $\text{dom}(f)$ является равномерно дискретным множеством. Из ограниченности f и равномерной дискретности $\text{dom}(f)$ следует, что множества $\{x \in \mathbb{R}^n \mid f(x) \leq \alpha\}$ конечны, а значит, множества $\text{MIN}_f(i)$ определены однозначно для всех $i \geq 1$. Более того, множества $\text{MIN}_f(i)$ конечны и формируют уникальное разбиение множества $\text{dom}(f)$:

$$\text{dom}(f) = \bigcup_{i \geq 1} \text{MIN}_f(i).$$

Для простоты предположим, что $\text{MIN}_f(i) \neq \emptyset$ для $i \geq 1$. Тогда пусть $z^{(i)}$ есть некоторый представитель множества $\text{MIN}_f(i)$.

Теорема 4. Функция $f \in \text{DConic}_n$ имеет продолжение в терминах определения 3 тогда и только тогда, когда для всех $i \geq 2$ верны следующие включения:

$$\text{MIN}_f(i) \subseteq \text{rel.br}(P_i), \quad \text{где} \quad P_i = \text{conv.hull}(\text{MIN}_f(1) \cup \dots \cup \text{MIN}_f(i)).$$

Так как $P_i = \text{conv.hull}(H_f^{\leq}(z^{(i)}))$, условие может быть переформулировано следующим образом: для всех $z \in \text{dom}(f) \setminus \text{MIN}_f(1)$ верны включения

$$H_f^{\leq}(z) \subseteq \text{rel.br}(\text{conv.hull}(H_f^{\leq}(z))).$$

Следствие 1. Для любой функции $f \in \text{DConic}_n$ существует функция $g \in \text{Conic}_n$ такая, что

$$\begin{aligned} \text{dom}(g) &= \text{conv. hull}(\text{dom}(f)), \quad \text{MIN}_g(1) = \text{MIN}_f(1), \\ \emptyset \neq \text{MIN}_g(2) &\subseteq \text{MIN}_f(2). \end{aligned}$$

2. Постановка задачи

Функция $f: \text{dom}(f) \rightarrow \mathbb{R}$ называется *дискретно-квазивыпуклой*, если множество $\text{dom}(f)$ дискретно и

$$\forall x, y \in \text{dom}(f) \quad \forall z \in (x, y) \cap \text{dom}(f) \quad f(z) \leq \max\{f(x), f(y)\}.$$

Классическими понятиями в геометрии чисел являются понятия кратчайшего вектора решётки и последовательных минимумов решётки (см., например, [22, с. 201–219; 3, с. 35–38; 17–20]) Данные понятия могут быть обобщены для дискретно-квазивыпуклых функций, определённых на точках решётки.

Определение 4. Пусть $\Lambda \subseteq \mathbb{R}^n$ — n -мерная решётка и $f: \Lambda \rightarrow \mathbb{R}$ — дискретно-квазивыпуклая ограниченная функция. Через $\lambda_1(\Lambda, f)$ обозначим минимальное значение f среди ненулевых векторов Λ :

$$\lambda_1(\Lambda, f) = \min_{x \in \Lambda \setminus \{0\}} f(x).$$

Ненулевой вектор v решётки Λ , удовлетворяющий соотношению $f(v) = \lambda_1(\Lambda, f)$, будем называть *минимальным вектором решётки Λ относительно f* . Для $i \in 2 : n$ положим

$$\lambda_i(\Lambda, f) = \min\{\alpha \in \mathbb{R} \mid \dim L(\alpha) \geq i\}, \quad \text{где } L(\alpha) = \text{span}\{x \in \Lambda \mid f(x) \leq \alpha\}.$$

Значения $\lambda_i(\Lambda, f)$ для $i \in 1 : n$ будем называть *последовательными минимумами решётки Λ относительно f* .

Будем говорить, что векторы $b_1, b_2, \dots, b_n \in \Lambda$ образуют *последовательные минимумы решётки Λ относительно f* , если они линейно независимы и $f(b_i) = \lambda_i(\Lambda, f)$ для $i \in 1 : n$.

Для матрицы $A \in \mathbb{Q}^{m \times n}$ через $\text{size}(A)$ обозначим длину двоичной кодировки A . Рассмотрим следующую задачу.

Задача 1. Пусть $B \in \mathbb{Q}^{m \times n}$, $\Lambda = \Lambda(B)$ и $f: \mathbb{R}^n \rightarrow \mathbb{R}$ — коническая функция, оснащённая оракулом сравнения. Пусть также известно, что некоторый вектор решётки Λ , на котором достигается значение $\lambda_n(\Lambda, f)$, находится в шаре $R \cdot B_2^n$ радиуса $R \in \mathbb{Q}_+$.

Задача состоит в построении алгоритма, который на входе, состоящем из матрицы B , числа R и оракула сравнения функции f , позволяет найти векторы, образующие последовательные минимумы решётки Λ относительно f . Количество вызовов к оракулу должно быть ограничено

величиной $C_n \log R$, где C_n — константа, зависящая только от n . Общая трудоёмкость алгоритма должна быть ограничена величиной $C_n \text{poly}(s)$, где $s = \text{size}(B) + \text{size}(R)$.

Замечание 3. Отметим два важных обстоятельства. Во-первых, в [15] показано, что для задачи 1 не существует алгоритма с числом обращений к оракулу $C_n \log R$, если класс функций Conic_n заменить более широким классом квазивыпуклых функций QConic_n . Введение в рассмотрение класса конических функций Conic_n было мотивировано именно этим отрицательным результатом. Существование алгоритма с нужными свойствами для класса Conic_n будет показано далее.

Во-вторых, определение задачи останется осмысленным, если заменить класс конических функций Conic_n классом дискретно-конических функций DConic_n . Но в этом случае теряется возможность задавать вопросы к оракулу сравнения в любых точках \mathbb{Q}^n . Насколько авторам известно, все существующие алгоритмы на базе оракулов, решающие задачу нелинейной целочисленной оптимизации для произвольной размерности n , используют данную возможность. Существование алгоритмов с указанными свойствами, использующих вопросы к оракулу исключительно в точках решётки Λ , известно только для размерности $n \leq 2$. В [1] показано существование алгоритма для строго дискретно-квазивыпуклых функций при $n = 2$ с трудоёмкостью $2 \log_2^2 R + O(\log R)$ обращений к оракулу сравнения. В [16] показано существование алгоритма для той же задачи с трудоёмкостью $4 \log_2 R + O(1)$ обращений к оракулу 0-го порядка при дополнительном условии, что функция является чётной. В настоящей работе последний результат будет обобщён на случай чётных функций класса DConic_2 , трудоёмкость алгоритма составит $3,32 \log_2 R + O(1)$ обращений к оракулу сравнения.

Замечание 4. Так как классы Conic_n и DConic_n инвариантны относительно аффинных преобразований, задача построения векторов, образующих последовательные минимумы решётки $\Lambda(B)$ относительно f , эквивалентна аналогичной задаче для решётки \mathbb{Z}^n относительно $g(x) = f(Bx)$. По данной причине далее в работе будем рассматривать только задачу построения последовательных минимумов решётки \mathbb{Z}^n .

С помощью алгоритмов целочисленной оптимизации (см., например, [3, 15]) несложно получить удовлетворительное решение задачи 1.

Теорема 5. Пусть $f: \mathbb{Z}^n \rightarrow \mathbb{R}$ — дискретно-коническая функция ($f \in \text{DConic}_n$), оснащённая оракулом сравнения. Пусть также известно такое $R \in \mathbb{Q}_+$, что некоторый вектор решётки Λ , на котором достигается значение $\lambda_n(\Lambda, f)$, находится в шаре $R \cdot B_2^n$.

Тогда для задачи построения векторов, образующих последовательные минимумы решётки \mathbb{Z}^n относительно f , существует алгоритм с оракульной сложностью $O(n)^{2n} \log R$. Общая трудоёмкость алгоритма равна $O(n)^{2n} \text{poly}(\text{size}(R))$.

ДОКАЗАТЕЛЬСТВО. Пусть D — некоторое множество с определённым на нём отношением линейного порядка. В [15] доказано существование алгоритма с оракульной сложностью $O(n)^{2n} \log R$ для задачи нахождения вектора, являющегося решением задачи $\min_{x \in \mathbb{Z}^n} g(x)$, где $g: \mathbb{R}^n \rightarrow D$ — коническая функция, заданная оракулом сравнения. При этом дополнительно предполагается, что некоторая точка минимума содержится в шаре радиуса R .

Покажем, как найти некоторые векторы v_1, v_2, \dots, v_n , являющиеся решением задачи. Зафиксируем $k \in 0 : (n-1)$, предположим, что векторы v_1, v_2, \dots, v_{k-1} уже найдены, и покажем как найти вектор v_k . Длины битовой записи векторов v_1, v_2, \dots, v_{k-1} ограничены некоторым полиномом от $\text{size}(R)$. Это означает, что за полиномиальное от $\text{size}(R)$ и n время может быть найдена матрица $A \in \mathbb{Z}^{(n-k+1) \times n}$ полного ранга и вектор $b \in \mathbb{Z}^{n-k+1}$ такие, что

$$\text{span}(v_1, v_2, \dots, v_{k-1}) = \{x \in \mathbb{R}^n \mid Ax = b\}.$$

Для $k = 0$ положим $A = E$ и $b = 0$, где E — единичная матрица. Матрица A и вектор b могут быть найдены, например, методом Гаусса, полиномиальность которого доказана в [23] (см. также [24, с. 37]).

Нетрудно видеть, что v_k является решением одной из $2n$ задач вида

$$\begin{aligned} f(x) &\rightarrow \min, \\ \begin{cases} \pm A_{i*}x \leq \pm b_i - 1, \\ x \in \mathbb{Z}^n, \end{cases} \end{aligned} \quad (2)$$

где $i \in 1 : n$ и A_{i*} обозначает i -ю строку A . Символ \pm означает, что мы отдельно для каждого $i \in 1 : n$ рассматриваем вариант задачи со знаком $+$ и вариант задачи со знаком $-$. Например, при $i = 1$ будут рассмотрены задачи с неравенствами $A_{1*}x \leq b_1 - 1$ и $-A_{1*}x \leq -b_1 - 1$.

Покажем, как решить задачу (2) для $i = 1$ с неравенством $A_{1*}x \leq b_1 - 1$, остальные задачи решаются аналогично. Для этого введём вспомогательную функцию $h(x) = (A_{1*}x - b_1 + 1)_+$, где $(x)_+ = x[x \geq 0]$ обозначает положительную часть числа x . По теореме 3 функция $h(x)$ коническая, так как $h(x)$ является композицией выпуклой и неубывающей конической функций. Положим $\hat{f}(x) = \begin{pmatrix} h(x) \\ f(x) \end{pmatrix}: \mathbb{R}^n \rightarrow \mathbb{R}^2$ и определим на \mathbb{R}^2 лексикографический порядок. По теореме 3 функция $\hat{f}(x)$

коническая, таким образом, рассматриваемая задача эквивалента задаче

$$\operatorname{lexmin}_{x \in \mathbb{Z}^n} \hat{f}(x).$$

При этом оракул лексикографического сравнения легко получается из оракула сравнения функции f и вычисления значений функции $h(x) = (A_{1*}x - b_1 + 1)_+$, последнее делается за полиномиальное от $\operatorname{size}(R)$ время.

Таким образом, задача поиска вектора v_k сводится к $2n$ задачам вида (2). В силу замечания в начале доказательства v_k может быть найден алгоритмом с оракульной сложностью $O(n)^{2n} \log R$. Такова же итоговая трудоёмкость поиска всех векторов v_1, v_2, \dots, v_n . Теорема 5 доказана.

Замечание 5. Трудоёмкость алгоритма можно снизить, если усилить условие теоремы и потребовать, чтобы функция f была выпуклой и оснащённой оракулом субградиента.

В [3, с. 245–255] показано существование рандомизированного алгоритма для решения задачи $\min_{K \cap \mathbb{Z}^n} f(x)$, где K — выпуклое множество, оснащённое оракулом отделения, и f — выпуклая функция, оснащённая оракулом субградиента. Математическое ожидание количества обращений к оракулу у данного алгоритма не превосходит величины $O(n)^n \times (\log R)^{O(1)}$. Аналогичным образом, как и в доказательстве теоремы 5, данный алгоритм может быть применён для построения последовательных минимумов решётки \mathbb{Z}^n относительно функции f . Математическое ожидание количества обращений к оракулу у итогового алгоритма составит $O(n)^n (\log R)^{O(1)}$.

Для наиболее важного случая $f(x) = \|x\|_2$ существуют алгоритмы с трудоёмкостью $2^{O(n)} \operatorname{poly}(\operatorname{size}(R))$ (см., например, [17–20]).

3. Критерий f -приведённого базиса в \mathbb{Z}^2

Рассмотрим задачу построения последовательных минимумов решётки \mathbb{Z}^2 относительно чётной дискретно-конической функции $f: \mathbb{Z}^2 \rightarrow \mathbb{R}$, оснащённой оракулом сравнения. Существенным отличием от задачи 1 является то, что функция f определена только в точках \mathbb{Z}^2 , что исключает вопросы к оракулу в произвольных точках \mathbb{Q}^2 .

По аналогии с определением базиса, приведённого по Минковскому (см., например, [22, с. 26–35]), введём определение f -приведённого базиса решётки \mathbb{Z}^n . Как будет показано далее, для $n = 2$ это определение эквивалентно определению последовательных минимумов \mathbb{Z}^2 .

Определение 5. Пусть $f: \mathbb{Z}^n \rightarrow \mathbb{R}$ — чётная ограниченная функция класса DConic_n . Базис b_1, b_2, \dots, b_n решётки \mathbb{Z}^n называется f -приведённым, если имеет место $f(b_1) = \lambda_1(\mathbb{Z}^n, f)$ и для любого $2 \leq i \leq n$ вектор b_i

является минимальным по значению f вектором таким, что система векторов b_1, b_2, \dots, b_i может быть дополнена до базиса \mathbb{Z}^n .

Следующая теорема и её следствие позволяют сформулировать необходимое и достаточное условие f -приведённости базиса решётки \mathbb{Z}^2 . Отметим, что для любой чётной дискретно-квазивыпуклой функции $f: \mathbb{Z}^2 \rightarrow \mathbb{R}$ точка 0 является точкой минимума: $0 \in \text{MIN}_f(1)$. Согласно замечанию 2 данное свойство выполнено и для класса дискретно-конических функций DConic_n .

Теорема 6. Пусть $f: \mathbb{Z}^2 \rightarrow \mathbb{R}$ — чётная ограниченная функция класса DConic_2 . Точка $y \in \mathbb{Z}^2$ является точкой второго минимума функции f ($y \in \text{MIN}_f(2)$) тогда и только тогда, когда существует вектор $z \in \mathbb{Z}^2$, удовлетворяющий следующим условиям:

- (1) векторы y, z образуют базис решётки \mathbb{Z}^2 ;
- (2) $f(y) \leq f(z) \leq \min\{f(z+y), f(z-y)\}$.

ДОКАЗАТЕЛЬСТВО. ДОСТАТОЧНОСТЬ. Покажем, что для всех $x \in \mathbb{Z}^2 \setminus \{0\}$ верно $f(x) \geq f(y)$. Из теоремы 3 о свойствах конических функций следует, что условия теоремы инвариантны относительно унимодулярных преобразований, а значит, можно считать, что $y = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ и $z = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Рассмотрим следующие конусы:

$$R_1 = \text{cone}(y, z \mid z+y), \quad R_2 = \text{cone}(-y, z \mid z-y), \\ C = \text{cone}(y, -y \mid z), \quad L = \text{cone}(0 \mid y).$$

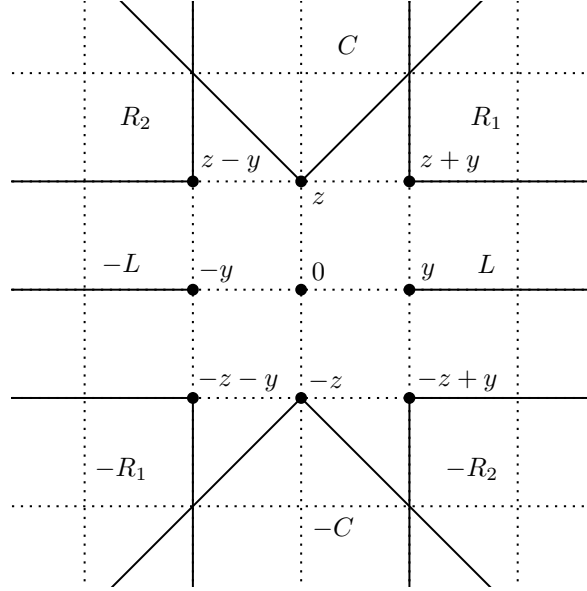
Из рис. 2 видно, что все точки множества $\mathbb{Z}^2 \setminus \{0\}$ покрываются данными конусами и их симметричными версиями.

В силу определения функций класса DConic_2 и неравенств условия (2) получаем, что $f(x) \geq f(y)$ для любых целых точек конусов R_1, R_2, C, L и их симметричных версий.

НЕОБХОДИМОСТЬ. Пусть $y \in \text{MIN}_f(2)$. Покажем, что точка $z \in \mathbb{Z}^2$, удовлетворяющая условиям (1) и (2) теоремы, существует. Пусть $M = \{x \in \mathbb{Z}^2 \mid y, x \text{ образуют базис } \mathbb{Z}^2\}$. Выберем точку $z \in M$ так, что $f(z) = \min\{f(x) \mid x \in M\}$, в силу ограниченности такое z существует. Неравенство $f(y) \leq f(z)$ условия (2), очевидно, выполнено. Остальные неравенства выполнены, поскольку $\{z+y, z-y\} \subseteq M$. Теорема 6 доказана.

Замечание 6. Требование ограниченности функции f нужно лишь при доказательстве необходимости. Также очевидно, что если потребовать $f(y) = f(z)$, то все точки целочисленной решётки будут покрыты конусами $\text{cone}(z, -z \mid y)$, $\text{cone}(y, -y \mid z)$ и их симметричными версиями. Неравенства $f(z) \leq \min\{f(z+y), f(z-y)\}$ в этом случае не нужны.

Следствие 2. Пусть $f: \mathbb{Z}^2 \rightarrow \mathbb{R}$ — чётная функция класса DConic_2 и $y, z \in \mathbb{Z}^2$. Следующие утверждения эквивалентны:

Рис. 2. Покрытие $\mathbb{Z}^2 \setminus \{0\}$

- (1) векторы y, z образуют f -приведённый базис \mathbb{Z}^2 ;
- (2) векторы y, z образуют последовательные минимумы \mathbb{Z}^2 относительно f ;
- (3) векторы y, z образуют базис \mathbb{Z}^2 такой, что верны неравенства

$$f(y) \leq f(z) \leq \min\{f(z+y), f(z-y)\}.$$

4. Алгоритм построения f -приведённого базиса \mathbb{Z}^2

Целью данного раздела является описание алгоритма построения f -приведённого базиса решётки \mathbb{Z}^2 для чётной функции $f: \mathbb{Z}^2 \rightarrow \mathbb{R}$ класса DConic_2 . Отметим, что из результатов работы [15] следует нижняя оценка сложности $3 \log_2 R + O(1)$ на минимальное количество обращений к оракулу, необходимое для поиска точки второго минимума функции f в области, ограниченной кругом радиуса R .

Будем предполагать, что поиск минимума $f(z + ty)$ при $t \in \mathbb{Z}$ производится отдельной процедурой, которая будет рассмотрена позднее. Обозначим через $y^{(k)}$ и $z^{(k)}$ значения переменных y и z после k -й итерации алгоритма 1. Также обозначим через t_k значение переменной t при выполнении поиска минимума функции $f(y + tx)$ на итерации k . Будем считать, что $t_k = 0$ для $k < 1$, а нумерация итераций начинается с 1. Через $y^{(0)}$ и $z^{(0)}$ обозначим значения переменных перед первой итерацией алгоритма.

Алгоритм 1**Вход:** Оракул сравнения функции f .**Выход:** Пара векторов (y, z) , являющихся f -приведённым базисом \mathbb{Z}^2 .

```

1:  $y := e_1, z := e_2$ 
2: repeat
3:   if  $f(y) > f(z)$  then
4:      $y \leftrightarrow z$ 
5:   end if
6:    $t := \arg \min_{t \in \mathbb{Z}} f(z + ty)$ 
7:    $z := z + ty$ 
8: until  $t \neq 0$ 
9: return  $(y, z)$ 

```

Теорема 7. Пусть $f: \mathbb{Z}^2 \rightarrow \mathbb{R}$ — чётная ограниченная функция класса DConic_2 . Тогда алгоритм 1 за конечное число итераций возвращает векторы (y, z) , являющиеся f -приведённым базисом \mathbb{Z}^2 .

ДОКАЗАТЕЛЬСТВО. Отметим, что если $k \geq 2$ и $f(y^{(k)}) \leq f(z^{(k)})$, то алгоритм прервётся на итерации $k + 1$. Действительно, в этом случае будет произведён поиск минимума на прямой, который уже производился на предыдущей итерации, вследствие чего $t_{k+1} = 0$.

При выполнении неравенства $f(y^{(k)}) > f(z^{(k)})$ получим $f(y^{(k+1)}) < f(y^{(k)})$. Таким образом, либо значения $f(y^{(k)})$ строго монотонно убывают, либо алгоритм заканчивает своё выполнение. В силу ограниченности функции f последнее доказывает конечность алгоритма.

На каждой итерации свойство пары векторов $(y^{(k)}, z^{(k)})$ образовывать базис решётки \mathbb{Z}^2 сохраняется, так как от итерации к итерации к ним применяются унимодулярные преобразования вида

$$(yz) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rightarrow (yz), \quad (yz) \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \rightarrow (yz).$$

После завершающей итерации алгоритма имеем неравенства $f(y^{(k)}) \leq f(z^{(k)}) \leq \min\{f(z^{(k)} + y^{(k)}), f(z^{(k)} - y^{(k)})\}$. По следствию 2 получаем, что пара векторов $(y^{(k)}, z^{(k)})$ является f -приведённым базисом \mathbb{Z}^2 . Теорема 7 доказана.

Замечание 7. Сделаем замечание, которое поможет упростить дальнейший анализ алгоритма 1. Если $f(e_1) \leq f(e_2)$, то перестановки значений переменных (yz) не произойдёт на итерации с номером 1, но это может не привести к завершению алгоритма на итерации 2, как это бы происходило на итерациях с номерами, большими двух. Чтобы восстановить однородность хода алгоритма, в случае $f(e_1) < f(e_2)$ поменяем

векторы $(e_1 e_2)$ местами. Если $f(e_1) = f(e_2)$, то по замечанию 6 точки $(e_1 e_2)$ уже образуют f -приведённый базис и алгоритм можно досрочно завершить. Такое изменение никак не влияет на трудоёмкость алгоритма, но существенно упрощает формулы и анализ.

Если итерация с номером $k \geq 1$ завершающая, то либо $(z^{(k-1)} z^{(k)}) = (z^{(k-2)} z^{(k-1)})$, либо $(z^{(k-1)} z^{(k)}) = (z^{(k-1)} z^{(k-2)})$. Если итерация с номером k не является завершающей, то

$$(y^{(k)} z^{(k)}) = (y^{(k-1)} z^{(k-1)}) \begin{pmatrix} 0 & 1 \\ 1 & t_k \end{pmatrix}.$$

Положим $z^{(-1)} = e_1$, тогда для $k \geq 0$ выполнено равенство $y^{(k)} = z^{(k-1)}$, откуда получаем

$$(z^{(k-1)} z^{(k)}) = (z^{(k-2)} z^{(k-1)}) \begin{pmatrix} 0 & 1 \\ 1 & t_k \end{pmatrix}. \quad (3)$$

Положим $a_k = z_2^{(k)}$ для $k \geq -1$, $a_k = 0$ для $k < -1$. Тогда последовательность a_k удовлетворяет равенству

$$a_k = a_{k-1} t_k + a_{k-2} + [k = 0]. \quad (4)$$

Исследуем рост $|a_k|$. Доказательства следующих трёх лемм для случая, когда f является строго дискретно-квазивыпуклой функцией, было проведено в [16]. Часть доказательств для функций класса DConic_n переносится без существенных изменений. Тем не менее, приведём доказательства, чтобы обеспечить полноту и целостность повествования.

Лемма 1. Пусть итерация с номером $k \geq 1$ не является завершающей. Тогда $f(z^{(k)}) \leq \min_{\tau \in \mathbb{Z}} f(\tau z^{(k-1)} \pm z^{(k)})$.

ДОКАЗАТЕЛЬСТВО. Так как итерация с номером $k \geq 1$ не завершающая, то $z^{(k)} = \arg \min_{x \in L} f(x)$, где $L = \{z^{(k-2)} + t z^{(k-1)} \mid t \in \mathbb{Z}\}$, и $z^{(k)} = z^{(k-2)} + t_k z^{(k-1)}$. Очевидно, что точки $\tau z^{(k-1)} \pm z^{(k)}$ лежат на прямых L и $-L$. В силу чётности функции f получаем требуемые неравенства. Лемма 1 доказана.

Лемма 2. Пусть алгоритм 1 произвёл $n \geq 2$ итераций. Тогда

- (1) $|t_1| \geq 1$, $|t_{n-1}| \geq 1$ и $t_n = 0$;
- (2) $|t_k| \geq 2$ для $k \in 2 : (n-2)$;
- (3) если $|t_k| = 2$, то $t_k t_{k+1} > 0$ для $k \in 2 : (n-3)$.

ДОКАЗАТЕЛЬСТВО. П. (1) следует из того, что итерации с номерами 1 и $n-1$ не завершающие. Равенство $t_n = 0$ является условием завершения алгоритма на итерации номер n .

(2) Предположим от противного, что $t_k = \pm 1$. Тогда $z^{(k)} = z^{(k-2)} \pm z^{(k-1)}$, но по лемме 1 имеем $f(z^{(k-1)}) \leq f(z^{(k-2)} \pm z^{(k-1)}) = f(z^{(k)})$. Последнее неравенство означает, что итерация с номером $k+1$ будет завершающей, что возможно только при $k = n-1$.

(3) Рассмотрим конусы $R_1 = \text{cone}(-z^{(k-1)}, z^{(k-1)} \mid z^{(k-1)} + z^{(k-2)})$ и $R_2 = \text{cone}(-z^{(k-1)}, z^{(k-1)} \mid -z^{(k-1)} + z^{(k-2)})$. Так как итерация с номером $k-1$ не является завершающей, по лемме 1 верны неравенства $f(\pm z^{(k-1)} + z^{(k-2)}) \geq f(z^{(k-1)})$. Таким образом,

$$\forall x \in R_1 \cup R_2 \cup -R_1 \cup -R_2 \quad f(x) \geq f(z^{(k-1)}).$$

Предположим, что $t_k = -2$ и $t_{k+1} = \tau \geq 1$. Тогда по формулам (3) имеем

$$\begin{aligned} z^{(k+1)} &= (1 - 2\tau)z^{(k-1)} + \tau z^{(k-2)} \\ &= (-z^{(k-1)} + z^{(k-2)}) + (\tau - 1)(-2z^{(k-1)} + z^{(k-2)}) \in R_2, \end{aligned}$$

откуда $z^{(k+1)} \in R_2$. Если $t_k = 2$ и $t_{k+1} = -\tau \leq 1$, то

$$\begin{aligned} -z^{(k+1)} &= (2\tau - 1)z^{(k-1)} + \tau z^{(k-2)} \\ &= (z^{(k-1)} + z^{(k-2)}) + (\tau - 1)(2z^{(k-1)} + z^{(k-2)}) \in R_1, \end{aligned}$$

откуда $z^{(k+1)} \in -R_1$. В обоих случаях $f(z^{(k+1)}) \geq f(z^{(k-1)}) \geq f(z^{(k)})$. Последнее неравенство означает, что итерация с номером $k+2$ будет завершающей, что возможно только при $k = n-2$. Лемма 2 доказана.

Определим также последовательность $\{b_k\}$, получающуюся из $\{a_k\}$, если положить $t_1 = -1$ и $t_k = 2$ для $k \geq 2$. Она удовлетворяет равенству

$$b_k = 2b_{k-1} + b_{k-2} - 3[k=1] + [k=0].$$

Лемма 3. Пусть алгоритм 1 произвёл $n \geq 2$ итераций. Тогда

- (1) $|a_k| > |a_{k-1}|$ для $k \in 1 : (n-2)$;
- (2) $\text{sgn}(a_k) = \text{sgn}(t_k a_{k-1})$ для $k \in 1 : (n-2)$;
- (3) $|a_k| = |t_k||a_{k-1}| + \text{sgn}(t_k t_{k-1})|a_{k-2}|$ для $k \in 2 : (n-2)$;
- (4) $|a_k| \geq |b_k|$ для $k \in 0 : (n-2)$;
- (5) $\frac{|a_k|}{|a_{k-1}|}$ для $k \in 1 : (n-2)$;
- (6) $|a_{n-1}| \geq |a_{n-4}|$.

ДОКАЗАТЕЛЬСТВО. (1) Поскольку последовательность $\{a_k\}$ удовлетворяет равенству (4), верно $|a_1| > |a_0|$. По неравенству треугольника и предположению индукции имеем

$$|a_k| \geq |t_k||a_{k-1}| - |a_{k-2}| > (|t_k| - 1)|a_{k-1}|.$$

Требуемое неравенство следует из того, что $|t_k| \geq 2$, для $2 \leq k \leq n-2$.

П. (2) следует из п. (1).

(3) Воспользуемся формулой $|x + y| = |x| + \operatorname{sgn}(xy)|y|$, справедливой при $|x| \geq |y|$. Так как

$$\begin{aligned} \operatorname{sgn}(t_k a_{k-1} a_{k-2}) &= \operatorname{sgn}(t_k a_{k-2}) \operatorname{sgn}(a_{k-1}) \\ &= \operatorname{sgn}(t_k a_{k-2}) \operatorname{sgn}(t_{k-1} a_{k-2}) = \operatorname{sgn}(t_k t_{k-1}), \end{aligned}$$

получаем

$$|a_k| = |t_k a_{k-1}| + \operatorname{sgn}(t_k a_{k-1} a_{k-2}) |a_{k-2}| = |t_k| |a_{k-1}| + \operatorname{sgn}(t_k t_{k-1}) |a_{k-2}|.$$

(4) Пусть $t = \{t_k\} = \{t_1, t_2, \dots\}$ есть некоторая последовательность. Аналогично формуле (4) положим $a_k(t) = a_{k-1}(t)t_k + a_{k-2}(t) + [k = 0]$. Рассмотрим две последовательности $t = \{t_k\}$ и $\hat{t} = \{\hat{t}_k\}$, удовлетворяющие свойствам, указанным в лемме 2. Последовательность \hat{t} назовём доминирующей, если для любой другой последовательности t справедливо $|a_k(t)| \geq |a_k(\hat{t})|$ для $0 \leq k \leq n - 2$. Существование доминирующей последовательности может быть легко доказано с помощью индукции путём склеивания доминирующих последовательностей меньшей длины с варьирующимися начальными условиями.

Пусть $a_k = a_k(t)$ для некоторого t . Тогда для $k \geq 3$ верно

$$|a_k| = (|t_k| |t_{k-1}| + \operatorname{sgn}(t_k t_{k-1})) |a_{k-2}| + |t_k| \operatorname{sgn}(t_{k-1} t_{k-2}) |a_{k-3}|.$$

Если $|t_{k-1}| \geq 3$, то минимум данного выражения достигается при $t_k = -\operatorname{sgn}(t_{k-1})2$. Если $|t_{k-1}| = 2$, то согласно свойству 3 леммы 2 имеем право выбрать t_k так, что $t_k t_{k-1} > 0$. Тогда минимум достигается в точке $t_k = \operatorname{sgn}(t_{k-1})2$.

Пусть \hat{t} есть доминирующая последовательность. Легко видеть, что $\hat{t}_1 = \pm 1$, $\hat{t}_2 = \mp 2$. Для $k \geq 3$ выбор t_k должен быть согласован с жадным правилом выбора t_k , описанным в предыдущем абзаце. Используя данное правило, получаем, что доминирующая последовательность для $k \geq 3$ должна удовлетворять формуле $t_k = \mp 2$, что доказывает утверждение.

(5) Аналогичным образом будем использовать обозначение $a_k(t) = a_{k-1}(t)t_k + a_{k-2}(t) + [t = 0]$ и введём определение доминирующей последовательности. Рассмотрим две последовательности $t = \{t_k\}$ и $\hat{t} = \{\hat{t}_k\}$, удовлетворяющие свойствам, указанным в лемме 2. Последовательность \hat{t} назовём доминирующей, если для любой другой последовательности t справедливо $\frac{|a_k(t)|}{|a_{k-1}(t)|} \geq \frac{|a_k(\hat{t})|}{|a_{k-1}(\hat{t})|}$ для $0 \leq k \leq n - 2$.

Пусть $a_k = a_k(t)$ для некоторого t . Тогда для $k \geq 2$ верно

$$\frac{|a_k|}{|a_{k-1}|} = |t_k| + \operatorname{sgn}(t_k t_{k-1}) \frac{|a_{k-2}|}{|a_{k-1}|}.$$

Если $|t_{k-1}| \geq 3$, то минимум данного выражения достигается при $t_k = -\operatorname{sgn}(t_{k-1})2$. Если $|t_{k-1}| = 2$, то согласно свойству 3 леммы 2 имеем право

выбирать t_k так, что $t_k t_{k-1} > 0$. В этом случае минимум достигается при $t_k = \operatorname{sgn}(t_{k-1})2$.

Используя аналогичные рассуждения, как и в конце п. (4), получаем, что $\frac{|a_k|}{|a_{k-1}|} \geq \frac{|b_k|}{|b_{k-1}|}$ для $k \geq 0$.

(6) Для элемента $|a_{n-1}|$ нельзя применить утверждение п. (1), так как возможна ситуация $|t_{n-1}| = 1$. Тем не менее можно показать, что $|a_{n-1}| \geq |a_{n-4}|$.

По определению $|a_{n-1}| = |t_{n-1}| |a_{n-2}| + \operatorname{sgn}(t_{n-1} t_{n-2}) |a_{n-3}|$. Если имеет место $|t_{n-1}| \geq 2$ или $\operatorname{sgn}(t_{n-1} t_{n-2}) = 1$, то в силу п. (1) леммы 3 верно $|a_{n-1}| \geq |a_{n-2}| > |a_{n-4}|$. В противном случае

$$|a_{n-1}| = |a_{n-2}| - |a_{n-3}| = (|t_{n-2}| - 1) |a_{n-3}| + \operatorname{sgn}(t_{n-2} t_{n-3}) |a_{n-4}|.$$

Если $|t_{n-2}| \geq 3$ или $\operatorname{sgn}(t_{n-2} t_{n-3}) = 1$, то $|a_{n-1}| \geq |a_{n-3}| > |a_{n-4}|$. В противном случае

$$|a_{n-1}| = |a_{n-3}| - |a_{n-4}| = (|t_{n-3}| - 1) |a_{n-4}| + \operatorname{sgn}(t_{n-3} t_{n-4}) |a_{n-5}|.$$

Если $|t_{n-3}| \geq 3$, то $|a_{n-1}| \geq |a_{n-3}| > |a_{n-4}|$. В противном случае имеем $|t_{n-2}| = |t_{n-3}| = 2$ и $\operatorname{sgn}(t_{n-2} t_{n-3}) = -1$. По п. (3) леммы 2 такая ситуация невозможна, а значит, либо $|t_{n-2}| \geq 3$, либо $|t_{n-3}| \geq 3$. Лемма 3 доказана.

Теорема 8. Для любого $k \geq 0$ верно

$$b_k = (-1)^k \frac{1}{2} (\sqrt{2} - 1)^{k-1} - \frac{1}{2} (\sqrt{2} + 1)^{k-1},$$

$$\frac{|b_k|}{|b_{k+1}|} \leq \frac{1}{\sqrt{2} + 1} (1 + O(\alpha^k)), \quad \text{где } \alpha = \frac{\sqrt{2} - 1}{\sqrt{2} + 1}.$$

ДОКАЗАТЕЛЬСТВО. Последовательность b_k представляет собой сдвинутую последовательность чисел Пелля с изменёнными начальными условиями. Стандартными средствами метода производящих функций (см., например, [21, с. 337–350]) можно показать справедливость первого равенства. Докажем второе равенство:

$$\frac{|b_k|}{|b_{k+1}|} = \frac{(\sqrt{2} + 1)^{k-1} + (-1)^{k-1} (\sqrt{2} - 1)^{k-1}}{(\sqrt{2} + 1)^k + (-1)^k (\sqrt{2} - 1)^k} = \frac{1}{\sqrt{2} + 1} \cdot \frac{1 + (-\alpha)^{k-1}}{1 + (-\alpha)^k},$$

где $\alpha = \frac{\sqrt{2}-1}{\sqrt{2}+1}$. Если k чётное, то $\frac{|b_k|}{|b_{k+1}|} \leq \frac{1}{\sqrt{2}+1}$. Если k нечётное, то

$$\frac{|b_k|}{|b_{k+1}|} \leq \frac{1}{\sqrt{2} + 1} \cdot \frac{1 + \alpha^{k-1}}{1 - \alpha^k} = \frac{1}{\sqrt{2} + 1} (1 + O(\alpha^k)).$$

Теорема 8 доказана.

Теорема 9. Пусть алгоритм 1 совершил $n \geq 5$ итераций и $\operatorname{MIN}_f(2) \subseteq R \cdot B_2^2$. Тогда $n \leq \log_{(1+\sqrt{2})} R + O(1)$.

ДОКАЗАТЕЛЬСТВО. Так как итерация с номером n завершающая, то $|a_n| = |a_{n-1}|$ или $|a_n| = |a_{n-2}|$. Для элемента $|a_{n-1}|$ нельзя применить п. (1) леммы 3, но по п. (6) $|a_{n-1}| \geq |a_{n-4}|$.

Так как второй минимум f находится в области $R \cdot B_2^2$, то $|a_n| \leq R$. Используя теорему 8 и п. (4) леммы 3, получаем, что

$$C(1 + \sqrt{2})^{n-5} = |b_{n-4}| \leq |a_{n-4}| \leq |a_n| \leq R$$

для некоторой константы C . Теорема 9 доказана.

Следующие алгоритмы позволяют производить эффективный поиск точки t^* минимума функции f на прямой $L(t) = z + t(z - y)$ и используются на шаге 5 алгоритма 1.

Алгоритм 2

Вход: Оракул сравнения функции f ; параметр k такой, что $t^* \geq 2^k$.

Выход: Интервал $[t_{st}, t_{fn})$, содержащий точку t^* .

```

1:  $t_{st} := 2^k, t_{fn} := 2^{k+1}$ 
2: while  $f(z + (t_{fn} - 1)y) > f(z + t_{fn}y)$  do
3:    $t_{st} := t_{fn}, t_{fn} := t_{fn} \cdot 2$ 
4: end while
5: return  $[t_{st}, t_{fn})$ 

```

Алгоритм 3

Вход: Оракул сравнения функции f и интервал $[t_{st}, t_{fn})$, содержащий точку t^* .

Выход: Точка t^* .

```

1: while  $t_{st} \neq t_{fn} - 1$  do
2:    $t_{mid} := \lfloor (t_{st} + t_{fn})/2 \rfloor$ 
3:   if  $f(z + (t_{mid} - 1)y) \leq f(z + t_{mid}y)$  then
4:      $t_{fn} := t_{mid}$ 
5:   else
6:      $t_{st} := t_{mid}$ 
7:   end if
8: end while
9: return  $t_{st}$ 

```

Лемма 4. Пусть определена точка $t^* \in \arg \min_{t \in \mathbb{Z}} f(z + ty)$ для функции f класса DConic_2 и $k \in \mathbb{N}$. Тогда существует алгоритм для поиска t^* , делающий не более $2 + k$ сравнений для случая $|t^*| \in [0, 2^k)$ и не более $3 - k + 2 \log_2 |t^*|$ сравнений для случая $|t^*| \in [2^k, +\infty)$.

ДОКАЗАТЕЛЬСТВО. Пусть $g(t) = f(z + ty)$. Для поиска t^* нужно определить, какому из лучей, соответствующих $t \geq 0$ и $t \leq 0$, принадлежит t^* . Это можно сделать, сравнив значения $g(0)$ и $g(1)$. Предположим, что $t^* \in [0, +\infty)$.

Сравним значения $g(2^k - 1)$ и $g(2^k)$. Если $g(2^k - 1) \leq g(2^k)$, то минимум находится в интервале $[0, 2^k)$, применим алгоритм 3 для его поиска. Суммарно в этом случае будет произведено $2 + k$ обращений к оракулу.

В противоположном случае имеем $g(2^k - 1) > g(2^k)$ и $t^* \in [2^k, +\infty)$. Для поиска интервала вида $[2^{k+p-1}, 2^{k+p})$, содержащего t^* , используем алгоритм 2 с параметром k . Для этого алгоритму потребуется p обращений к оракулу. После этого применим алгоритм 3 для поиска t^* в данном интервале, для чего потребуется $k + p - 1$ обращений к оракулу. Итого в рассматриваемом случае потребуется $1 + k + 2p$ обращений к оракулу. Так как $p \leq \log_2 t^* - k + 1$, общее число обращений к оракулу не превосходит $3 - k + 2 \log_2 t^*$. Лемма 4 доказана.

Теорема 10. Пусть алгоритм 1 был запущен для поиска f -приведённого базиса решётки \mathbb{Z}^2 относительно чётной функции $f: \mathbb{Z}^2 \rightarrow \mathbb{R}$ класса DConic_2 , оснащённой оракулом сравнения. Пусть также точка второго минимума функции f расположена в круге радиуса R и алгоритм 1 произвёл $n \geq 3$ итераций для её поиска.

Тогда общее число обращений к оракулу, производимое алгоритмом 1, не превосходит $3,32 \log_2 R + O(1)$. Оценка произведена при условии, что для поиска минимума на прямых, возникающих на шаге 5 алгоритма 1, использовалась лемма 4.

ДОКАЗАТЕЛЬСТВО. Пусть s означает количество итераций алгоритма, в которых $|t_i| < 2^k$. Отметим, что на последней итерации делается не более двух обращений к оракулу и $t_n = 0$. По лемме 2 для всех $2 \leq i \leq n - 2$ верно $|t_i| \geq 2$. Будем считать, что $|t_{n-1}| \geq 2$, так как в противном случае анализ только упрощается. По лемме 4 суммарное число обращений к оракулу с учётом дополнительного сравнения, производимого в начале каждой итерации, равно

$$n + O(1) + s(2 + k) + (n - s)(3 - k) + 2 \sum_{i=1}^{n-1} [|t_i| \geq 2^k] \log_2 |t_i|. \quad (5)$$

Оценим величину суммы с помощью следующей леммы.

Лемма 5.

$$\sum_{i=1}^{n-1} [|t_i| \geq 2^k] \log_2 |t_i| \leq \log_2 R - (1 + \sqrt{2})s + \gamma(n - s) + O(1),$$

где $\gamma = 1 - \log_2(2 - (\sqrt{2} + 1)^{-1})$.

ДОКАЗАТЕЛЬСТВО. Нетрудно проверить, что для любых целого $t \geq 2$ и $\epsilon \in (0, 1)$ справедливо неравенство

$$\log_2 t \leq \log_2(t - \epsilon) + 1 - \log_2(2 - \epsilon), \quad (6)$$

причём равенство достигается при $t = 2$. Докажем, что

$$\sum_{i=1}^{n-1} [|t_i| \geq 2^k] \log \left(|t_i| - \frac{|a_{i-2}|}{|a_{i-1}|} \right) \leq \log_2 R - (1 + \sqrt{2})s + O(1). \quad (7)$$

По п. (1) леммы 3 с учётом того, что $|t_{n-1}| \geq 2$, для $1 \leq i \leq n-1$ верно $|a_i| \geq |t_i||a_{i-1}| - |a_{i-2}|$, откуда $\frac{|a_i|}{|a_{i-1}|} \geq |t_i| - \frac{|a_{i-2}|}{|a_{i-1}|}$. Согласно п. (5) леммы 3 для $1 \leq i \leq n-2$ верно $\frac{|a_i|}{|a_{i-1}|} \geq \frac{|b_i|}{|b_{i-1}|}$. По теореме 8 имеем $\frac{|b_i|}{|b_{i-1}|} \geq (1 + \sqrt{2}) \frac{1}{1 + O(\alpha^{i-1})}$, где $\alpha = \frac{\sqrt{2}-1}{\sqrt{2}+1}$. В силу того, что $|t_{n-1}| \geq 2$, верно $\frac{|a_{n-1}|}{|a_{n-2}|} \geq 1$. Так как $a_{-1} = 0$, $a_0 = 1$, $a_1 = t_1$ и $|a_{n-1}| \leq R$, перемножая неравенства для $\frac{|a_i|}{|a_{i-1}|}$ и логарифмируя, получаем требуемое.

Используя неравенства (6) и (7), получаем

$$\begin{aligned} \sum_{i=1}^{n-1} [|t_i| \geq 2^k] \log_2 |t_i| &\leq \log_2 R - (1 + \sqrt{2})s + O(1) \\ &+ \sum_{i=1}^{n-1} [|t_i| \geq 2^k] (1 - \log_2(2 - \epsilon_{i-2})), \quad \text{где } \epsilon_i = \frac{|a_i|}{|a_{i+1}|}. \end{aligned} \quad (8)$$

По п. (5) леммы 3 и теореме 8 для $0 \leq i \leq n-3$ справедливо $\epsilon_i \leq \frac{1}{\sqrt{2}+1} (1 + O(\alpha^k))$. Из полученных неравенств следует, что

$$\begin{aligned} \log_2(2 - \epsilon_{k-2}) &\geq \log_2(2 - (\sqrt{2} + 1)^{-1} (1 + O(\alpha^k))) \\ &= \log_2(2 - (\sqrt{2} + 1)^{-1}) + O(\alpha^k). \end{aligned}$$

Утверждение леммы следует из данного неравенства и (8). Лемма 5 доказана.

Используя (5) и лемму 5, получаем, что общее число обращений к оракулу выражается следующей формулой:

$$(4 - k + 2\gamma)n + O(1) + (2k - 3 - 2(\sqrt{2} + \gamma))s + 2 \log_2 R.$$

Для $k \leq 3 < 3/2 + \sqrt{2} + \gamma$ третьим слагаемым в оценке можно пренебречь. Минимум в этом случае достигается при $k = 3$ и равен $(1 + 2\gamma)n + O(1) + 2 \log_2 R$. Используя теорему 9, получаем, что число обращений к оракулу равно

$$\left(2 + \frac{1 + 2\gamma}{\log_2(1 + \sqrt{2})} \right) \log_2 R + O(1) \leq 3,32 \log_2 R + O(1).$$

Теорема 10 доказана.

Авторы выражают особую благодарность С. И. Веселову, Н. Ю. Золотых и А. Ю. Чиркову за неоценимую помощь в подготовке статьи.

ЛИТЕРАТУРА

1. **Чирков А. Ю.** Минимизация квазивыпуклой функции на двумерной целочисленной решётке // Вестн. Нижегород. ун-та им. Н. И. Лобачевского. Сер. Мат. моделирование и оптим. управление. 2003. № 1. С. 227–238.
2. **Ahmadi A., Olshevsky A., Parrilo P., Tsitsiklis J.** NP-hardness of deciding convexity of quadratic polynomials and related problems // Math. Program. 2013. Vol. 137, No. 1–2. P. 453–476.
3. **Dadush D.** Integer programming, lattice algorithms, and deterministic volume estimation: Thes. ... doct. philosophy. Georgia Inst. Tech., 2012. 280 p.
4. **Dadush D., Peikert C., Vempala S.** Enumerative lattice algorithms in any norm via M-ellipsoid coverings // Proc. 52nd Annu. IEEE Symp. Foundations of Computer Science (Palm Springs, CA, USA, Oct. 23–25, 2011). Washington: IEEE Comput. Soc., 2011. P. 580–589.
5. **Khachiyan L., Porkolab L.** Integer optimization on convex semialgebraic sets // Discrete Comput. Geom. 2000. Vol. 23, No. 2. P. 207–224.
6. **Lenstra H.** Integer programming with a fixed number of variables // Math. Oper. Res. 1983. Vol. 8, No. 4. P. 538–548.
7. **De Loera J. A., Hemmecke R., Koppe M., Weismantel R.** Integer polynomial optimization in fixed dimension // Math. Oper. Res. 2006. Vol. 31, No. 1. P. 147–153.
8. **Heinz S.** Complexity of integer quasiconvex polynomial optimization // J. Complexity. 2005. Vol. 21, No. 4. P. 543–556.
9. **Heinz S.** Quasiconvex functions can be approximated by quasiconvex polynomials // ESAIM Control Optim. Calc. Var. 2008. Vol. 14, No. 4. P. 795–801.
10. **Hemmecke R., Onn S., Weismantel R.** A polynomial oracle-time algorithm for convex integer minimization // Math. Program. 2011. Vol. 126, No. 1. P. 97–117.
11. **Hildebrand R., Köppe M.** A new Lenstra-type algorithm for quasiconvex polynomial integer minimization with complexity $2^{O(n \log n)}$ // Discrete Optim. 2013. Vol. 10, No. 1. P. 69–84.
12. **Oertel T.** Integer convex minimization in low dimensions: Thes. ... doct. philosophy. Eidgenös. Techn. Hochschule, Zürich, 2014. 127 p.
13. **Oertel T., Wagner C., Weismantel R.** Integer convex minimization by mixed integer linear optimization // Oper. Res. Lett. 2014. Vol. 42, No. 6. P. 424–428.
14. **Basu A., Oertel T.** Centerpoints: A link between optimization and convex geometry // SIAM J. Optim. 2017. Vol. 27, No. 2. P. 866–889.
15. **Chirkov A. Yu, Griбанов D. V., Malyshev D. S., Pardalos P. M., Veselov S. I., Zolotykh A. Yu.** On the complexity of quasiconvex integer minimization problem // J. Global Optim. 2018. Vol. 73, No. 4. P. 761–788.

16. **Веселов С. И., Грибанов Д. В., Золотых Н. Ю., Чирков А. Ю.** Минимизация симметричной квазивыпуклой функции на двумерной решётке // Дискрет. анализ и исслед. операций. 2018. Т. 25, № 3. С. 23–35.
17. **Micciancio D.** Efficient reductions among lattice problems // Proc. 19th Annu. ACM-SIAM Symp. Discrete Algorithms (San Francisco, CA, Jan. 20–22, 2008). Philadelphia, PA: SIAM, 2008. P. 84–93.
18. **Micciancio D., Voulgaris P.** A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations // SIAM J. Comput. 2010. Vol. 42, No. 3. P. 1364–1391.
19. **Aggarwal D., Dadush D., Regev O., Stephens-Davidowitz N.** Solving the Shortest Vector Problem in 2^n time via discrete Gaussian sampling // Proc. 47th Annu. ACM Symp. Theory of Computing (Portland, OR, USA, June 14–17, 2015). New York: ACM, 2015. P. 733–742.
20. **Aggarwal D., Dadush D., Stephens-Davidowitz N.** Solving the Closest Vector Problem in 2^n time — the discrete Gaussian strikes again! // Proc. 56th Annu. IEEE Symp. Foundations of Computer Science (Berkeley, CA, USA, Oct. 18–20, 2015). Washington: IEEE Comput. Soc., 2015. P. 563–582.
21. **Graham R., Knuth D., Patashnik O.** Concrete mathematics – A foundation for computer science. Reading, MA: Addison-Wesley, 1994. 657 p.
22. **Cassels J.** An introduction to the geometry of numbers. Berlin; Heidelberg: Springer-Verl. 1997. 343 p.
23. **Edmonds J.** Systems of distinct representatives and linear algebra // J. Res. Nat. Bureau Stand. B. Math. Math. Phys. 1967. Vol. 71, No. 4. P. 241–245.
24. **Grötschel M., Lovász L., Schrijver A.** Geometric algorithms and combinatorial optimization. Algorithms and Combinatorics. Vol. 2. Berlin; Heidelberg: Springer-Verl. 1993. 363 p.

Грибанов Дмитрий Владимирович
Мальшев Дмитрий Сергеевич

Статья поступила
2 апреля 2019 г.
После доработки —
15 августа 2019 г.
Принята к публикации
28 августа 2019 г.

MINIMIZATION OF EVEN CONIC FUNCTIONS ON THE TWO-DIMENSIONAL INTEGRAL LATTICE

D. V. Griбанov^a and D. S. Malyshev^b

National Research University Higher School of Economics,
25/12 Bolshaya Pechyorskaya Street, 603155 Nizhny Novgorod, Russia
E-mail: ^adimitry.gribanov@gmail.com, ^bdsmalyshev@rambler.ru

Abstract. Under consideration is the Successive Minima Problem for the 2-dimensional lattice with respect to the order given by some conic function f . We propose an algorithm with complexity of $3.32 \log_2 R + O(1)$ calls to the comparison oracle of f , where R is the radius of the circular searching area, while the best known lower oracle complexity bound is $3 \log_2 R + O(1)$. We give an efficient criterion for checking that given vectors of a 2-dimensional lattice are successive minima and form a basis for the lattice. Moreover, we show that the similar Successive Minima Problem for dimension n can be solved by an algorithm with at most $O(n)^{2n} \log R$ calls to the comparison oracle. The results of the article can be applied to searching successive minima with respect to arbitrary convex functions defined by the comparison oracle. Illustr. 2, bibliogr. 24.

Keywords: quasiconvex function, convex function, conic function, quasiconvex polynomial, integral lattice, nonlinear integer programming, successive minima, reduced basis of a lattice.

REFERENCES

1. A. Yu. Chirkov, Minimization of a quasiconvex function on 2-dimensional lattice, *Vestn. Lobachevsky State Univ. Nizhny Novgorod, Ser. Model. Optim. Control* **1**, 227–238 (2003).
2. A. Ahmadi, A. Olshevsky, P. Parrilo, and J. Tsitsiklis, NP-hardness of deciding convexity of quadratic polynomials and related problems, *Math. Program.* **137** (1–2), 453–476 (2013).

This research is supported by Russian Foundation for Basic Research (Project 18–31–20001–mol-a-ved).

English version: Journal of Applied and Industrial Mathematics **14** (1), 56–72 (2020), DOI 10.1134/S199047892001007X.

3. **D. Dadush**, Integer programming, lattice algorithms, and deterministic volume estimation, *Ph. D. Thesis* (ProQuest LLC, Ann Arbor, MI; Georgia Institute of Technology, 2012).
4. **D. Dadush, C. Peikert**, and **S. Vempala**, Enumerative lattice algorithms in any norm via M-ellipsoid coverings, in *Proc. 52nd Annual IEEE Symp. Foundations of Computer Science, Palm Springs, CA, USA, Oct. 23–25, 2011* (IEEE Comput. Soc., Washington, 2011), pp. 580–589.
5. **L. Khachiyan** and **L. Porkolab**, Integer optimization on convex semialgebraic sets, *Discrete Comput. Geom.* **23** (2), 207–224 (2000).
6. **H. Lenstra**, Integer programming with a fixed number of variables, *Math. Oper. Res.* **8** (4), 538–548 (1983).
7. **J. A. de Loera, R. Hemmecke, M. Koppe**, and **R. Weismantel**, Integer polynomial optimization in fixed dimension, *Math. Oper. Res.* **31** (1), 147–153 (2006).
8. **S. Heinz**, Complexity of integer quasiconvex polynomial optimization, *J. Complexity* **21** (4), 543–556 (2005).
9. **S. Heinz**, Quasiconvex functions can be approximated by quasiconvex polynomials, *ESAIM Control Optim. Calc. Var.* **14** (4), 795–801 (2008).
10. **R. Hemmecke, S. Onn**, and **R. Weismantel**, A polynomial oracle-time algorithm for convex integer minimization, *Math. Program.* **126** (1), 97–117 (2011).
11. **R. Hildebrand** and **M. Köppe**, A new Lenstra-type algorithm for quasiconvex polynomial integer minimization with complexity $2^{O(n \log n)}$, *Discrete Optim.* **10** (1), 69–84 (2013).
12. **T. Oertel**, Integer convex minimization in low dimensions, *Ph. D. Thesis* (Eidgenössische Technische Hochschule, Zürich, 2014).
13. **T. Oertel, C. Wagner**, and **R. Weismantel**, Integer convex minimization by mixed integer linear optimization, *Oper. Res. Lett.* **42** (6), 424–428 (2014).
14. **A. Basu** and **T. Oertel**, Centerpoints: A link between optimization and convex geometry, *SIAM J. Optim.* **27** (2), 866–889 (2017).
15. **A. Yu. Chirkov, D. V. Griбанov, D. S. Malyshev, P. M. Pardalos, S. I. Veselov**, and **A. Yu. Zolotykh**, On the complexity of quasiconvex integer minimization problem, *J. Global Optim.* **73** (4), 761–788 (2018).
16. **S. I. Veselov, D. V. Griбанov, N. Yu. Zolotykh**, and **A. Yu. Chirkov**, Minimizing a symmetric quasiconvex function on a two-dimensional lattice, *Diskretn. Anal. Issled. Oper.* **25** (3), 23–35 (2018) [*J. Appl. Ind. Math.* **12** (3), 587–594 (2018)].
17. **D. Micciancio**, Efficient reductions among lattice problems, in *Proc. 19th Annual ACM-SIAM Symp. Discrete Algorithms, San Francisco, California, Jan. 20–22, 2008* (SIAM, Philadelphia, PA, 2008), pp. 84–93.
18. **D. Micciancio** and **P. Voulgaris**, A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations, *SIAM J. Comput.* **42** (3), 1364–1391 (2010).

19. **D. Aggarwal, D. Dadush, O. Regev, and N. Stephens-Davidowitz**, Solving the shortest vector problem in 2^n time via discrete Gaussian sampling, in *Proc. 47th Annual ACM Symp. Theory of Computing, Portland, OR, USA, June 14–17, 2015* (ACM, New York, 2015), pp. 733–742.
20. **D. Aggarwal, D. Dadush, and N. Stephens-Davidowitz**, Solving the closest vector problem in 2^n time – the discrete Gaussian strikes again! in *Proc. 56th Annual IEEE Symp. Foundations of Computer Science, Berkeley, CA, USA, Oct. 18–20, 2015*, (IEEE Comput. Soc., Washington, 2011), pp. 563–582.
21. **R. Graham, D. Knuth, and O. Patashnik**, *Concrete Mathematics – A Foundation for Computer Science*, (Addison-Wesley Prof., Reading, MA, 1994).
22. **J. Cassels**, *An Introduction to the Geometry of Numbers* (Springer, Berlin, 1997).
23. **J. Edmonds**, Systems of distinct representatives and linear algebra, *J. Res. Natl. Bureau of Stand. B: Math. Math. Phys.* **71 B** (4), 241–245 (1967).
24. **M. Grötschel, L. Lovász, and A. Schrijver**, Geometric Algorithms and Combinatorial Optimization, in *Algorithms and Combinatorics*, Vol. 2, (Springer, Berlin, 1993).

Dmitry V. Gribanov
Dmitry S. Malyshev

Received April 2, 2019
Revised August 15, 2019
Accepted August 28, 2019