ISSN 1990-4789, Journal of Applied and Industrial Mathematics, 2020, Vol. 14, No. 1, pp. 56–72. © Pleiades Publishing, Ltd., 2020.
Russian Text © The Author(s), 2020, published in Diskretnyi Analiz i Issledovanie Operatsii, 2020, Vol. 27, No. 1, pp. 17–42.

Minimization of Even Conic Functions on the Two-Dimensional Integral Lattice

D. V. Gribanov[1]* **and D. S. Malyshev**[1]**

[1] *National Research University Higher School of Economics,
Bolshaya Pechyorskaya ul. 25/12, Nizhny Novgorod, 603155 Russia*

Received April 2, 2019; in final form, August 15, 2019; accepted August 28, 2019

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.

DOI: 10.1134/S199047892001007X

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

INTRODUCTION

The integer minimization problem of a (quasi)convex function under (quasi)convex constraints is a familiar and intensively studied generalization of the integer linear programming problem [1–13].

The target function and constraints can be given explicitly or by oracles. In [4, 13], some algorithms are given for solving the problem of checking the nonemptiness of the set $K \cap \mathbb{Z}^n$, where K is a convex set defined by a strong separation oracle included in a ball of radius R. The number of calls to the separation oracle produced by the given algorithms depends polynomially on $\log R$. Modification of this result and a good survey are given in [3], where some algorithm is proposed with complexity of $O(n)^n \operatorname{poly}(\log R)$ calls to the separation oracle. Furthermore, a randomized algorithm is given in [3] with expected complexity of $O(n)^n \operatorname{poly}(\log R)$ calls to the oracle for the minimization of a convex function f defined by a subgradient oracle on $K \cap \mathbb{Z}^n$, where the convex domain K is defined by the strong separation oracle. Some new approach, based on a generalization of the notion of the barycenter is proposed in [12, 14] to the integer-valued case.

The main defect of the oracles mentioned above is the complexity of their realization. Some more convenient way consists in using a comparison oracle and a 0th-order oracle computing the values of the function at points. However, it is shown in [15] that the problem of minimization of a quasiconvex function f on $K = R \cdot B_2^n \cap \mathbb{Z}^n$, where $R \cdot B_2^n$ stands for the n-dimensional ball of radius R in the Euclidean norm, cannot be solved by an algorithm with the number of calls to the comparison oracle polynomial in $\log R$.

The integer minimization problem for convex functions (and for functions close to convex) defined by a comparison oracle or a 0th-order oracle was considered in [1, 15, 16]. In [1], some new integer minimization algorithm was developed for the discrete strictly quasiconvex functions defined by a comparison oracle on $\mathbb{Z}^2$. The oracle complexity of the algorithm in [1] is at most $2\log_2^2 R + O(\log_2 R)$. In [16], the

*E-mail: dimitry.gribanov@gmail.com
**E-mail: dsmalyshev@rambler.ru

symmetric version of this problem was considered, in case the function f is additionally assumed even. The algorithm obtained in [16] has complexity of $4\log_2 R + O(1)$ calls to a 0th-order oracle.

In [15], the question was considered of constructing a restriction of the class of quasiconvex functions equipped by the comparison oracle for which the integer minimization problem in fixed dimension admits solving by an algorithm whose oracle complexity depends polynomially on $\log R$. In more detail, in [15], the classes of conic and discrete-conic functions were introduced. The class of conic functions contains convex functions, strictly quasiconvex functions, and quasiconvex polynomials as proper subclasses. For the problem of minimization of a conic function f equipped by the comparison oracle on $R \cdot B_2^n \cap \mathbb{Z}^n$, some algorithm was obtained in [15] with oracle complexity $O(n)^{2n} \log R$. Moreover, in [15], the lower bound $3^{n-1} \log_2(2R-1)$ was obtained for the necessary number of calls to the oracle. Under the assumption that the function f under minimization is additionally assumed even, the lower bound $(2^n - 1)\log_2(R-1)$ of oracle complexity was given.

The important problem that can be reduced to the integer nonlinear optimization problem is construction of the vectors constituting successive minima of a lattice with respect to some vector norm. The results of [17, 18] show that, for the Euclidean norm, this problem can be solved by an algorithm with overall complexity $4^n \operatorname{poly}(\operatorname{size}(R))$, where $\operatorname{size}(R)$ is the length of the bit encoding of R. In [19, 20], an approach was developed which, together with results from [17], makes it possible to solve the problem under consideration by a randomized algorithm with complexity $2^{n+o(n)} \operatorname{poly}(\operatorname{size}(R))$. Note that the results of the above works can be extended to wider classes of norms.

In this article, we study the generalized problem of constructing the vectors that constitute successive minima of a lattice with respect to the order defined by an arbitrary conic function f. For the problem of an arbitrary dimension n, we obtain an algorithm with complexity of $O(n)^{2n} \log R$ calls to the comparison oracle of the function f, where R is the radius of the ball containing the vectors of successive minima. In more detail, we consider the case $n = 2$ under the additional assumption that f is even. For this case, we propose an algorithm with oracle complexity $3.32 \log_2 R + O(1)$, whereas the lower complexity bound given in [15] is $3 \log_2 R + O(1)$.

1. DEFINITIONS AND NOTATIONS. SOME AUXILIARY RESULTS

Denote by B_p^n the n-dimensional unit ball of the l_p-norm:

$$B_p^n = \{x \in \mathbb{R}^n \mid \|x\|_p \le 1\}.$$

We use the special notations and names for the following sets of matrices generated by the columns of a matrix $B \in \mathbb{R}^{m\times n}$:

- $\operatorname{cone}(B) = \{Bt \mid t \in \mathbb{R}_+^n\}$ is the *cone,*
- $\operatorname{conv.hull}(B) = \Big\{Bt \mid t \in \mathbb{R}_+^n,\ \sum\limits_{i=1}^n t_i = 1\Big\}$ is the *convex hull,*
- $\operatorname{affine}(B) = \Big\{Bt \mid t \in \mathbb{R}^n,\ \sum\limits_{i=1}^n t_i = 1\Big\}$ is the *affine envelope,*
- $\operatorname{span}(B) = \{Bt \mid t \in \mathbb{R}^n\}$ is the *linear span,*
- $\mathrm{N}(B) = \{Bt \mid t \in \mathbb{Z}^n\}$ is the *lattice.*

Given $D \subseteq \mathbb{R}^n$, denote by $\operatorname{int}(D)$ and $\operatorname{br}(D)$ the subsets of its *interior* and *boundary* points respectively. The subsets of *interior* and *boundary points* of $D \subseteq \mathbb{R}^n$ relative to the affine envelope $\operatorname{affine}(D)$ will be denoted by $\operatorname{rel.int}(D)$ and $\operatorname{rel.br}(D)$ respectively.

Denote by $i : j = \{i, i+1, \dots, j\}$ the set of integers ranging from i to j. Denote by x_i the ith coordinate of $x \in \mathbb{R}^n$. The interval between $y, z \in \mathbb{R}^n$ will be denoted by

$$[y, z] = \{x = ty + (1-t)z \mid 0 \le t \le 1\}.$$

The symbol (y, z) stands for an open interval. A set D is called *convex* if $[x, y] \subseteq D$ for all $x, y \in D$. Denote the domain of a function f by $\operatorname{dom}(f)$. Given $y \in \operatorname{dom}(f)$, designate as $H_f^{\le}(y)$ the level set of f:

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

The sets $H_f^{<}(y)$ and $H_f^{=}(y)$ are defined similarly.

For denoting the indicators of the fulfillment of logical conditions, we will use the Iverson notation (see, for instance, [21, p. 11, 37]). Given a logical condition A, we put $[A] = 1$ if A is true and $[A] = 0$ if A is false.

Consider the set of functions $f\colon \operatorname{dom}(f) \to \mathbb{R}$ such that $\operatorname{dom}(f) \subseteq \mathbb{R}^n$ is a convex set. A function f is called *quasiconvex* if

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

A function f is called *strictly quasiconvex* if

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

A function f is called *convex* if

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

We denote these classes of functions by QConv_n (quasiconvex), SQConv_n (strictly quasiconvex), and Conv_n (convex) respectively. Designate as QCPoly_n the class of quasiconvex polynomials of nonzero degree with real coefficients.

Call a function $f\colon \operatorname{dom}(f) \to \mathbb{R}$ *bounded* if $\{x \in \operatorname{dom}(f) \mid f(x) \le \alpha\}$ is bounded for every $\alpha \in \mathbb{R}$.

Given $x^{(1)}, x^{(2)}, \dots, x^{(k)} \in \mathbb{R}^n$, denote by $\operatorname{cone}(x^{(1)}, \dots, x^{(k-1)} \mid x^{(k)})$ the set

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

which is the cone constituted by the vectors $-x^{(1)}, \dots, -x^{(k-1)}$ shifted by $x^{(k)}$.

Definition 1. Suppose that a set D is equipped by the linear order $\preceq$. Let $f\colon \operatorname{dom}(f) \to D$, where $\operatorname{dom}(f)$ is convex.

The function f is *conic* if, for all $y, z \in \operatorname{dom}(f)$ and $t \ge 0$ such that $f(y) \preceq f(z)$ and $z + t(z - y) \in \operatorname{dom}(f)$, the following is true:

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

The class of conic functions will be denoted by Conic_n.

Remark 1. Henceforth, we assume almost everywhere that $D = \mathbb{R}$ with the standard order. However, in the proof of Theorem 5, we need to use $D = \mathbb{R}^2$ with the lexicographic order. Note that all results of the article are also valid in the most general case.

Remark 2. It is not hard to see that the class Conic_n of conic functions is a subclass in the class of quasiconvex functions; i.e.,

$$\mathrm{Conic}_n \subset \mathrm{QConv}_n.$$

The inclusion is strict: a counterexample is given by the quasiconvex function $\operatorname{sgn}(x_1)$ which is not conic.

Denote by $\mathrm{MIN}_f(1)$ the set of minimum points of a function f:

$$\mathrm{MIN}_f(1) = \arg \min_{x \in \operatorname{dom}(f)} f(x).$$

If the set $\mathrm{MIN}_f(1)$ is undefined then we put $\mathrm{MIN}_f(1) = \varnothing$. Analogously, for $k \ge 2$, define the set $\mathrm{MIN}_f(k)$ of the points of the kth minimum of f:

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

If $\mathrm{MIN}_f(k)$ is undefined then we put $\mathrm{MIN}_f(k) = \varnothing$.

The following theorem [15] gives several equivalent ways of defining Conic_n:

Theorem 1. *Let $f\colon \operatorname{dom}(f) \to D$, where $\operatorname{dom}(f) \subseteq \mathbb{R}^n$ is convex and D is equipped by the linear order relation $\preceq$. The following are equivalent:*

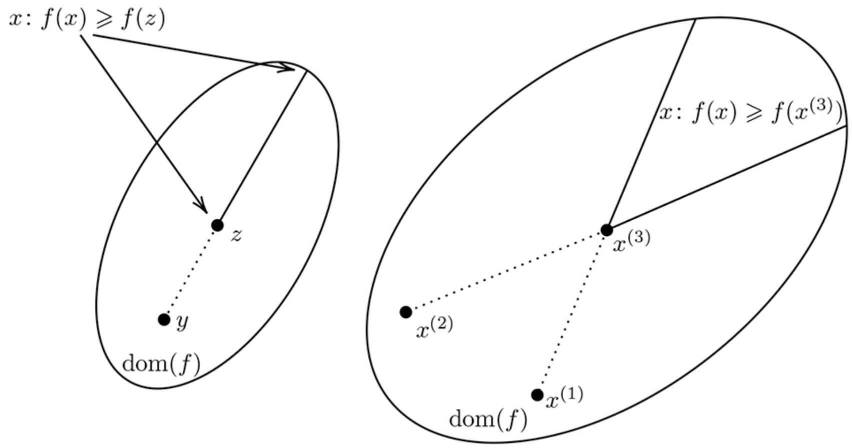

Fig. 1. Illustration to Theorem 1: definition (1) on the left and definition (2) on the right.

(1) *$f(z+t(z-y)) \succeq f(z)$ for every pair of points $y, z \in \mathrm{dom}(f)$ and all $t \geq 0$ such that*

$$f(y) \preceq f(z), \qquad z+t(z-y) \in \mathrm{dom}(f).$$

(2) *$f(y) \geq f(x^{(k)})$ for all $x^{(1)}, x^{(2)}, \dots, x^{(k)}, y \in \mathrm{dom}(f)$ such that*

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

Moreover, we may additionally require that $x^{(1)}, x^{(2)}, \dots, x^{(k)}$ be in general position (each collection of $i \leq k$ points is affinely independent).

(3) *If $x \in \mathrm{dom}(f)$, then $H_f^{\leq}(x)$ is convex (which is equivalent to the quasiconvexity of f) and*

$$\forall x \in \mathrm{dom}(f) \setminus \mathrm{MIN}_f(1) \qquad H_f^{=}(x) \subseteq \mathrm{rel.br}\,(H_f^{\leq}(x)).$$

Fig. 1 illustrates the definitions in Theorem 1.

The following theorems [15] state that Conic_n contains important subclasses of functions and is closed under some natural operations:

Theorem 2. *The following hold:*

(1) $\mathrm{SQConv}_n \subset \mathrm{Conic}_n \subset \mathrm{QConv}_n$,

(2) $\mathrm{QCPoly}_n \subset \mathrm{Conic}_n$,

(3) $\mathrm{Conv}_n \subset \mathrm{Conic}_n$.

Theorem 3. (1) *Suppose that $f_i \in \mathrm{Conic}_n$ and $w_i \in \mathbb{R}_+$ for each $i \in 1:k$.*

$$g(x) = \max_{i \in 1:k} \{w_i f_i(x)\}$$

belongs to Conic_n, where

$$\mathrm{dom}(g) = \bigcap_{i \in 1:k} \mathrm{dom}(f_i).$$

(2) *Let* $f \in \mathrm{Conic}_n$ *and let* $h\colon \mathbb{R} \to \mathbb{R}$ *be a nondecreasing conic function. Then* $g = h \circ f$ *belongs to* Conic_n.

(3) *Suppose that* $f \in \mathrm{Conic}_m$, $A \in \mathbb{R}^{m\times n}$, *and* $b \in \mathbb{R}^m$. *Then* $g(x) = f(Ax+b)$, *which is an affine image of* $f(x)$, *belongs to* Conic_n.

(4) *Suppose that* $f_1, f_2 \in \mathrm{Conic}_n$ *and* $D = \mathrm{dom}(f_1) \cap \mathrm{dom}(f_2)$. *Then*

$$g(x) = \left(\begin{smallmatrix} f_1(x) \\ f_2(x) \end{smallmatrix}\right)\colon D \to \mathbb{R}^2$$

is conic with respect to the lexicographic order on $\mathbb{R}^2$.

A function f is called *even* if, for all $x \in \mathrm{dom}(f)$, $-x \in \mathrm{dom}(f)$ and $f(x) = f(-x)$. A set $D \subseteq \mathbb{R}^n$ is called *discrete* if, for every $x \in D$, there exists a ball $B = x + R\cdot B_2^n$ of radius $R > 0$ centered at x such that $D \cap B = \{x\}$. A set $D \subseteq \mathbb{R}^n$ is called *uniformly discrete* if there exists a ball $B = R \cdot B_2^n$ of radius $R > 0$ such that $D \cap (x+B) = \{x\}$ for all $x \in D$.

Definition 2. Let $f\colon\ \mathrm{dom}(f) \to D$, where $\mathrm{dom}(f) \subset \mathbb{R}^n$ is discrete and D is equipped by the linear order relation $\preceq$. A function f is called *discrete-conic* if, for all points $y, x^{(1)}, x^{(2)}, \dots, x^{(k)} \in \mathrm{dom}(f)$ such that

$$f(x^{(1)}) \le f(x^{(2)}) \le \dots \le f(x^{(k)}), \qquad y \in \mathrm{cone}(x^{(1)}, x^{(2)}, \dots, x^{(k-1)} \mid x^{(k)}),$$

we have $f(y) \ge f(x^{(k)})$. The class of all discrete-conic functions will be denoted by DConic_n.

Is it true that each function in DConic_n is naturally extendible to a function in Conic_n? Theorem 14, proved in [15], answers this question for bounded functions with uniformly discrete domain.

Definition 3. Let $f \in \mathrm{DConic}_n$. A function $g \in \mathrm{Conic}_n$ is called an *extension of a function* f if

$$\mathrm{dom}(g) = \mathrm{conv.hull}(\mathrm{dom}(f)) \quad \text{and} \quad g(x) = f(x) \text{ for } x \in \mathrm{dom}(f).$$

Consider a bounded function $f \in \mathrm{DConic}_n$ such that $\mathrm{dom}(f)$ is a uniformly discrete set. The boundedness of f and the uniform discreteness of $\mathrm{dom}(f)$ imply that the sets $\{x \in \mathbb{R}^n \mid f(x) \le \alpha\}$ are finite, and so the sets $\mathrm{MIN}_f(i)$ are defined uniquely for all $i \ge 1$. Moreover, $\mathrm{MIN}_f(i)$ are finite and form a unique partition of $\mathrm{dom}(f)$:

$$\mathrm{dom}(f) = \bigcup_{i \ge 1} \mathrm{MIN}_f(i).$$

Assume for simplicity that $\mathrm{MIN}_f(i) \ne \varnothing$ for $i \ge 1$. Then let $z^{(i)}$ be a representative of $\mathrm{MIN}_f(i)$.

Theorem 4. *A function* $f \in \mathrm{DConic}_n$ *has an extension in terms of Definition* 14 *if and only if the following hold for all* $i \ge 2$:

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

Since $P_i = \mathrm{conv.hull}(H_f^{\le}(z^{(i)}))$, the condition can be reformulated as follows:

$$H_f^{=}(z) \subseteq \mathrm{rel.br}\,(\mathrm{conv.hull}(H_f^{\le}(z)))$$

for all $z \in \mathrm{dom}(f) \setminus \mathrm{MIN}_f(1)$.

Corollary 1. *For every function* $f \in \mathrm{DConic}_n$, *there exists a function* $g \in \mathrm{Conic}_n$ *such that*

$$\mathrm{dom}(g) = \mathrm{conv.hull}(\mathrm{dom}(f)), \qquad \mathrm{MIN}_g(1) = \mathrm{MIN}_f(1),$$
$$\varnothing \ne \mathrm{MIN}_g(2) \subseteq \mathrm{MIN}_f(2).$$

2. STATEMENT OF THE PROBLEM

A function $f\colon \operatorname{dom}(f) \to \mathbb{R}$ is called *discrete-quasiconvex* if $\operatorname{dom}(f)$ is discrete and

$$\forall x, y \in \operatorname{dom}(f)\, \forall z \in (x, y) \cap \operatorname{dom}(f) \qquad f(z) \le \max\{f(x), f(y)\}.$$

Classical in the geometry of numbers are the notions of a shortest vector of a lattice and successive minima of a lattice (see, for example, [22, pp. 201–219; 3, pp. 35–38; 17–20] These notions can be generalized to discrete-quasiconvex functions defined at the points of the lattices.

Definition 4. Let $\Lambda \subseteq \mathbb{R}^n$ be an n-dimensional lattice and let $f\colon \Lambda \to \mathbb{R}$ be a discrete-quasiconvex bounded function. Denote by $\lambda_1(\Lambda, f)$ the minimal value f among nonzero vectors of Λ:

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

A nonzero vector v of Λ satisfying $f(v) = \lambda_1(\Lambda, f)$ is called a *minimal vector of* Λ *with respect to* f. Given $i \in 2 : n$, put

$$\lambda_i(\Lambda, f) = \min\{\alpha \in \mathbb{R} \mid \dim L(\alpha) \ge i\}, \ \text{ where } L(\alpha) = \operatorname{span}\{x \in \Lambda \mid f(x) \le \alpha\}.$$

The values $\lambda_i(\Lambda, f)$ for $i \in 1 : n$ are called *successive minima of* Λ *with respect to* f.

We say that the vectors $b_1, b_2, \dots, b_n \in \Lambda$ *constitute successive minima of* Λ *with respect to* f if they are linearly independent and $f(b_i) = \lambda_i(\Lambda, f)$ for $i \in 1 : n$.

Given a matrix $A \in \mathbb{Q}^{m \times n}$, denote by $\operatorname{size}(A)$ the length of the binary encoding of A. Consider the following

Problem 1. *Suppose that $B \in \mathbb{Q}^{m \times n}$, $\Lambda = \Lambda(B)$, and $f\colon \mathbb{R}^n \to \mathbb{R}$ is a conic function equipped by the comparison oracle. Assume also that some vector of Λ at which the value $\lambda_n(\Lambda, f)$ is attained lies in the ball $R \cdot B_2^n$ of radius $R \in \mathbb{Q}_+$.*

The problem consists in constructing an algorithm which, given a matrix B, a number R, and a comparison oracle of f, finds the vectors constituting successive minima of Λ with respect to f. The number of calls to the oracle must be bounded by $C_n \log R$, where C_n is some constant depending only on n. The overall complexity of the algorithm must be bounded by $C_n \operatorname{poly}(s)$, where $s = \operatorname{size}(B) + \operatorname{size}(R)$.

Remark 3. Observe the two important circumstances: Firstly, it was demonstrated in [15] that for Problem 1 there is no algorithm with number of calls to the oracle $C_n \log R$ if the function class Conic_n is replaced by the wider class of quasiconvex functions QConv_n. It is this negative result that motivated us to consider the class of conic functions Conic_n. The existence of an algorithm with the desired properties for Conic_n will be proved below.

Secondly, the statement of the problem still makes sense if we replace the class of conic functions Conic_n by the class of discrete conic functions DConic_n. Nevertheless, in this case, we lose the possibility of asking questions to the comparison oracle at any points of $\mathbb{Q}^n$. As far as the authors are aware, all available algorithms on the base of oracles solving the nonlinear integer optimization problem for an arbitrary dimension n use this possibility. The existence of algorithms with the indicated properties using questions to the oracle at the points of the lattice Λ is known only for the dimension $n \le 2$. In [1], the existence was shown of an algorithm for strictly discrete-quasiconvex functions for $n = 2$ with complexity of $2 \log_2^2 R + O(\log R)$ calls to the comparison oracle. In [16], the existence was proved of an algorithm for the same problem with complexity of $4 \log_2 R + O(1)$ calls to a 0th-order oracle under the additional condition that the function is even. In the present article, the last result is generalized to the case of even functions of class DConic_2; the complexity of the algorithm is $3.32 \log_2 R + O(1)$ calls to the oracle.

Remark 4. Since the classes Conic_n and DConic_n are invariant under affine mappings, the problem of constructing the vectors constituting successive minima of $\Lambda(B)$ with respect to f is equivalent to the analogous problem for $\mathbb{Z}^n$ with respect to $g(x) = f(Bx)$. For this reason, we will henceforth consider only the problem of constructing successive minima for $\mathbb{Z}^n$.

Using integer optimization algorithms (see, for example, [3, 15]) it is easy to obtain some satisfactory solution of Problem 1.

Theorem 5. *Let $f\colon \mathbb{Z}^n \to \mathbb{R}$ be a discrete-conic function $f \in \mathrm{DConic}_n$ equipped by the comparison oracle. Suppose also that we know $R \in \mathbb{Q}_+$ such that some vector of a lattice Λ at which the value $\lambda_n(\Lambda, f)$ is attained lies in the ball $R \cdot B_2^n$. Then the problem of constructing successive minima of $\mathbb{Z}^n$ with respect to f admits an algorithm with oracle complexity $O(n)^{2n} \log R$. The overall complexity of the algorithm equals $O(n)^{2n}\,\mathrm{poly}(\mathrm{size}(R))$.*

Proof. Let D be a set with a linear order. It was proved in [15] that an algorithm with oracle complexity $O(n)^{2n} \log R$ exists for the problem of finding a vector that is a solution to the problem

$$\min_{x \in \mathbb{Z}^n} g(x),$$

where $g\colon \mathbb{R}^n \to D$ is a conic function defined by a comparison oracle. Moreover, it is additionally assumed that some minimum point lies in the ball of radius R.

Show how to find some vectors $v_1, v_2, \dots, v_n$ that are a solution to the problem.

Fix $k \in 0 : (n-1)$, assume that $v_1, v_2, \dots, v_{k-1}$ are already found, and show how to find v_k. The lengths of the bit representations of the vectors $v_1, v_2, \dots, v_{k-1}$ are bounded by some polynomial of $\mathrm{size}(R)$. This means that, in polynomial time of $\mathrm{size}(R)$ and n, we can find a matrix $A \in \mathbb{Z}^{(n-k+1)\times n}$ of full rank and a vector $b \in \mathbb{Z}^{n-k+1}$ such that

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

For $k = 0$, put $A = E$ and $b = 0$, where E is the identity matrix. The matrix A and the vector b can be found, for example, by the Gauss method whose polynomiality was proved in [23] (see also [24, p. 37]).

It is not hard to see that v_k is a solution to one of the $2n$ problems of the form

$$f(x) \to \min, \qquad \begin{cases} \pm A_{i*} x \le \pm b_i - 1, \\ x \in \mathbb{Z}^n, \end{cases} \tag{2}$$

where $i \in 1 : n$ and A_{i*} stands for the ith row of A. The symbol ± means that we, separately for each $i \in 1 : n$, consider the variant of the problem with the $+$ sign and the variant of the problem with the $-$ sign. For example, for $i = 1$, we will consider the problems with the inequalities

$$A_{1*} x \le b_1 - 1, \qquad -A_{1*} x \le -b_1 - 1.$$

Show how to solve (2) for $i = 1$ with the inequality $A_{1*} x \le b_1 - 1$; the remaining inequalities are solved by analogy. To this end, introduce the auxiliary function $h(x) = (A_{1*} x - b_1 + 1)_+$, where $(x)_+ = x[x \ge 0]$ stands for the positive part of a number x. By Theorem 3, $h(x)$ is conic since $h(x)$ is the composition of a convex function and a nondecreasing function. Put

$$\hat f(x) = \begin{pmatrix} h(x) \\ f(x) \end{pmatrix} \;:\; \mathbb{R}^n \to \mathbb{R}^2$$

and endow $\mathbb{R}^2$ with the lexicographic order. By Theorem 3, the function $\hat f(x)$ is conic; thus, the problem under consideration is equivalent to the problem

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

Here the lexicographic comparison oracle is easily obtained from the comparison oracle of f and the calculation of the values of the function $h(x) = (A_{1*} x - b_1 + 1)_+$; the last is achieved in time polynomial in $\mathrm{size}(R)$.

Thus, the problem of finding the vector v_k is reduced to $2n$ problems of the form (2). By the remark at the beginning of the proof, v_k can be found by an algorithm with oracle complexity $O(n)^{2n} \log R$. The resulting complexity of finding all vectors $v_1, v_2, \dots, v_n$ is the same.

Theorem 5 is proved. □

Remark 5. The complexity of the algorithm can be decreased by strengthening the hypothesis of the theorem and require that the function f be convex and equipped by the subgradient oracle.

It was proved in [3, pp. 245–255] that there exists a randomized algorithm for solving the problem

$$\min_{K\cap\mathbb{Z}^n} f(x),$$

where K is a convex set equipped by the separation oracle and f is a convex function equipped by the subgradient oracle. For this oracle, the expected number of calls to the oracle for this algorithm does not exceed $O(n)^n(\log R)^{O(1)}$. By analogy to the proof of Theorem 5, this algorithm can be applied for constructing successive minima for $\mathbb{Z}^n$ with respect to f. The expectation of the number of calls to the oracle for the resulting algorithm is $O(n)^n(\log R)^{O(1)}$.

For the most important case $f(x) = \|x\|_2$, there exist algorithms with complexity $2^{O(n)}\operatorname{poly}(\operatorname{size}(R))$ (see, for example, [17–20]).

3. A CRITERION FOR AN f-REDUCED BASIS FOR $\mathbb{Z}^2$

Consider the Successive Minima Problem for $\mathbb{Z}^2$ with respect to an even discrete-conic function $f\colon \mathbb{Z}^2 \to \mathbb{R}$ equipped by the comparison oracle. The substantial difference from Problem 14 is the fact that f is defined only at the points of $\mathbb{Z}^2$, which excludes questions to the oracle at arbitrary points of $\mathbb{Q}^2$.

By analogy with the definition of Minkowski reduced basis (see, for instance, [22, pp. 26–35]), introduce the definition of *f-reduced basis for $\mathbb{Z}^n$*. As we will show below, for $n = 2$, this definition is equivalent to the definition of successive minima for $\mathbb{Z}^2$.

Definition 5. Let $f\colon \mathbb{Z}^n \to \mathbb{R}$ be an even function of class DConic_n. A basis $b_1, b_2, \dots, b_n$ for $\mathbb{Z}^n$ is called *f-reduced* if $f(b_1) = \lambda_1(\mathbb{Z}^n, f)$ and for each $2 \le i \le n$ the vector b_i is a minimal vector with respect to f such that the system of vectors $b_1, b_2, \dots, b_i$ can be supplemented to a basis for $\mathbb{Z}^n$.

The following theorem and its corollary enable us to formulate some necessary and sufficient condition for the f-reducedness of a basis for $\mathbb{Z}^2$. Observe that, for every even discrete-quasiconvex function $f\colon \mathbb{Z}^2 \to \mathbb{R}$, the point 0 is a minumum point: $0 \in \mathrm{MIN}_f(1)$. In accordance with Remark 14, this property also holds for the class of discrete-conic functions DConic_n.

Theorem 6. *Let $f\colon \mathbb{Z}^2 \to \mathbb{R}$ be an even bounded function in* DConic_2. *Some $y \in \mathbb{Z}^2$ is the second minimum point of f ($y \in \mathrm{MIN}_f(2)$) if and only if there exists $z \in \mathbb{Z}^2$ satisfying the conditions:*

(1) *the vectors y and z constitute a basis for $\mathbb{Z}^2$;*

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

Proof. Sufficiency: Show that, $f(x) \ge f(y)$ for all $x \in \mathbb{Z}^2 \setminus \{0\}$. Theorem 3 about the properties of conic functions implies that the conditions of the theorem are invariant under unimodular transformations, and so we can assume that $y = \binom{1}{0}$ and $z = \binom{0}{1}$. Consider the cones

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

Fig. 2 shows that all points of $\mathbb{Z}^2 \setminus \{0\}$ are covered by these cones and their symmetric versions.

By the definition of functions of class DConic_2 and the inequalities of condition (2), we infer that $f(x) \ge f(y)$ for all integer points of the cones R_1, R_2, C, L, and their symmetric versions.

Necessity: Let $y \in \mathrm{MIN}_f(2)$. Show that there is $z \in \mathbb{Z}^2$ satisfying conditions (1) and (2) of the theorem. Let

$$M = \{x \in \mathbb{Z}^2 \mid y, x \text{ constitute a basis for } \mathbb{Z}^2\}.$$

Choose a point $z \in M$ so that $f(z) = \min\{f(x) \mid x \in M\}$; such z exists by boundedness. The inequality $f(y) \le f(z)$ of condition (2) obviously holds. The remaining inequalities are fulfilled since

$$\{z+y, z-y\} \subseteq M.$$

Theorem 6 is proved. □

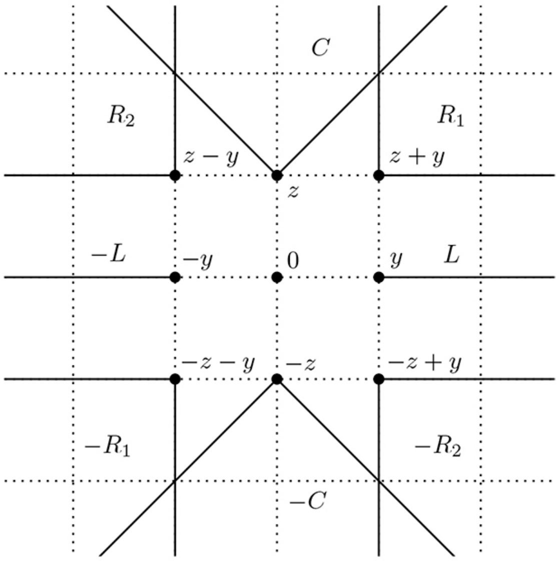

Fig. 2. The covering of $\mathbb{Z}^2 \setminus \{0\}$.

Remark 6. The requirement of the boundedness of f is needed only for proving necessity. It is also obvious that if we require that $f(y) = f(z)$ then all points of the integer lattice are covered by the cones $\mathrm{cone}(z, -z \mid y)$, $\mathrm{cone}(y, -y \mid z)$ and their symmetric versions. The inequalities $f(z) \le \min\{f(z+y), f(z-y)\}$ are unnecessary in this case.

Corollary 2. *Let $f\colon \mathbb{Z}^2 \to \mathbb{R}$ be an even function in* DConic_2 *and let $y, z \in \mathbb{Z}^2$. The following assertions are equivalent:*

(1) *y and z constitute an f-reduced basis for $\mathbb{Z}^2$;*

(2) *y and z constitute successive minima of $\mathbb{Z}^2$ with respect to f;*

(3) *y and z form a basis for $\mathbb{Z}^2$ such that*

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

4. AN ALGORITHM FOR CONSTRUCTING AN f-REDUCED BASIS FOR $\mathbb{Z}^2$

The goal of this section is to describe an algorithm for constructing an f reduced basis for $\mathbb{Z}^2$ given an even function $f\colon \mathbb{Z}^2 \to \mathbb{R}$ in DConic_2. Note that the results of [15] imply the lower complexity bound $3\log_2 R + O(1)$ for the minimal number of calls to the oracle necessary for searching the second minimum of f in a domain bounded by a ball of radius R.

We assume that the search for a minimum of $f(z+ty)$ for $t \in \mathbb{Z}$ is carried out by some separate procedure that will be considered later. Let by $y^{(k)}$ and $z^{(k)}$ denote the values of the variables y and z after the kth iteration of Algorithm 1. Denote also by t_k the value of the variable t in the search for a minimum of $f(y+tx)$ at iteration k. We assume that $t_k = 0$ for $k < 1$ and the iterations are enumerated from 1. Let $y^{(0)}$ and $z^{(0)}$ denote the values of the variables before the first iteration of the algorithm.

Algorithm 1

```
Input : The comparison oracle of $f$.
Output : A pair of vectors $(y, z)$ that is an $f$-reduced basis for $\mathbb{Z}^2$.
  1 : $y := e_1, z := e_2$
```

```
repeat
    if $f(y) > f(z)$ then
        $y \leftrightarrow z$
    end if
    $t := \arg\min_{t\in\mathbb{Z}} f(z+ty)$
    $z := z + ty$
until $t \neq 0$
return $(y, z)$
```

Theorem 7. *Let $f\colon \mathbb{Z}^2 \to \mathbb{R}$ be an even bounded function in* DConic_2. *Then, Algorithm* 1 *outputs some vectors (y, z) that are an f-reduced basis for $\mathbb{Z}^2$ after finitely many iterations.*

Proof. Note that if $k \geq 2$ and $f(y^{(k)}) \leq f(z^{(k)})$ then the algorithm interrupts at iteration $k+1$. Indeed, in this event, search for a minimum on a straight line, which has already been carried out, is implemented. Hence, $t_{k+1} = 0$.

If $f(y^{(k)}) > f(z^{(k)})$ then $f(y^{(k+1)}) < f(y^{(k)})$. Thus, the values $f(y^{(k)})$ are strictly monotone decreasing or the algorithm finishes. Since f is bounded, this proves the finiteness of the algorithm.

At each iteration, the property of the pair of vectors $(y^{(k)}z^{(k)})$ to form a basis for $\mathbb{Z}^2$ is preserved because, from iteration to iteration, the unimodular transformations of the following form are applied to them:

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

After the final iteration, we have

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

By Corollary 2, we conclude that the pair of vectors $(y^{(k)}z^{(k)})$ is an f-reduced basis for $\mathbb{Z}^2$.

Theorem 7 is proved. □

Remark 7. Some remark can help us to simplify the further analysis of Algorithm 1. If $f(e_1) \leq f(e_2)$ then there will no permutation of the variables (yz) at iteration 1 but this may fail to finish the algorithm at iteration 2, which would be the case at the iterations with numbers greater than 2. For reconstructing the homogeneity of the algorithm, in the case of $f(e_1) < f(e_2)$, interchange the vectors (e_1e_2). If $f(e_1) = f(e_2)$ then, by Remark 6, the points (e_1e_2) already constitute an f-reduced basis and the algorithm can be finished. Such a change has no influence on the complexity of the algorithm but substantially simplifies the formulas and the analysis.

If the kth iteration, $k \geq 1$, is final then

$$\text{either} \quad (z^{(k-1)}z^{(k)}) = (z^{(k-2)}z^{(k-1)}) \quad \text{or} \quad (z^{(k-1)}z^{(k)}) = (z^{(k-1)}z^{(k-2)}).$$

If the kth iteration is not final then

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

Put $z^{(-1)} = e_1$. Then for $k \geq 0$ we have $y^{(k)} = z^{(k-1)}$, whence we obtain

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

Put $a_k = z_2^{(k)}$ for $k \geq -1$ and $a_k = 0$ for $k < -1$. Then the sequence a_k satisfies

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

Examine the growth of $|a_k|$. The proofs of the following three lemmas for the case when f is a strictly discrete-quasiconvex function was done in [16]. Part of the proofs for functions of class DConic_n is carried over without substantial changes. However, we will give the proof to ensure the completeness and integrity of the exposition.

Lemma 1. *Suppose that the kth iteration, $k \geq 1$, is not final. Then*

$$f\big(z^{(k)}\big) \leq \min_{\tau \in \mathbb{Z}} f\big(\tau z^{(k-1)} \pm z^{(k)}\big).$$

Proof. Since the kth iteration, with $k \geq 1$, is not final,

$$z^{(k)} = \arg\min_{x \in L} f(x),$$

where $L = \{z^{(k-2)} + tz^{(k-1)} \mid t \in \mathbb{Z}\}$, and $z^{(k)} = z^{(k-2)} + t_k z^{(k-1)}$. Obviously, the points $\tau z^{(k-1)} \pm z^{(k)}$ lie on straight lines L and $-L$. Since f is even, we obtain the desired inequalities.

Lemma 1 is proved. □

Lemma 2. *Suppose that Algorithm* 1 *has produced $n \geq 2$ iterations. Then*

(1) $|t_1| \geq 1$, $|t_{n-1}| \geq 1$, *and* $t_n = 0$;

(2) $|t_k| \geq 2$ *for* $k \in 2 : (n-2)$;

(3) *if* $|t_k| = 2$ *then* $t_k t_{k+1} > 0$ *for* $k \in 2 : (n-3)$.

Proof. Item (1) stems from the fact that the first and $(n-1)$th iterations are not final. The equality $t_n = 0$ means that the nth iteration is final.

(2) Suppose on the contrary that $t_k = \pm 1$. Then

$$z^{(k)} = z^{(k-2)} \pm z^{(k-1)}$$

but, by Lemma 1, we have

$$f(z^{(k-1)}) \leq f(z^{(k-2)} \pm z^{(k-1)}) = f(z^{(k)}).$$

The last inequality means that the $(k+1)$th iteration is final, which is possible only for $k = n-1$.

(3) Consider the cones

$$R_1 = \mathrm{cone}\big(-z^{(k-1)}, z^{(k-1)} \mid z^{(k-1)} + z^{(k-2)}\big), \quad R_2 = \mathrm{cone}\big(-z^{(k-1)}, z^{(k-1)} \mid -z^{(k-1)} + z^{(k-2)}\big).$$

Since the $(k-1)$th iteration is not final, by Lemma 1, we have the inequalities

$$f\big(\pm z^{(k-1)} + z^{(k-2)}\big) \geq f\big(z^{(k-1)}\big).$$

Thus,

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

Suppose that $t_k = -2$ and $t_{k+1} = \tau \geq 1$. Then, by (3), we infer

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

whence $z^{(k+1)} \in R_2$. If $t_k = 2$ and $t_{k+1} = -\tau \leq 1$ then

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

whence $z^{(k+1)} \in -R_1$. In both cases,

$$f(z^{(k+1)}) \geq f(z^{(k-1)}) \geq f(z^{(k)}).$$

The last inequality means that the $(k+2)$th iteration is final, which is possible only for $k = n-2$.

Lemma 2 is proved. □

Consider only the sequence $\{b_k\}$ obtained from $\{a_k\}$ by putting $t_1 = -1$ and $t_k = 2$ for $k \geq 2$. It satisfies the equality

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

Lemma 3. *Suppose that Algorithm* 1 *has produced* $n \geq 2$ *iterations. Then*

(1) $|a_k| > |a_{k-1}|$ *for* $k \in 1 : (n-2)$;

(2) $\operatorname{sgn}(a_k) = \operatorname{sgn}(t_k a_{k-1})$ *for* $k \in 1 : (n-2)$;

(3) $|a_k| = |t_k||a_{k-1}| + \operatorname{sgn}(t_k t_{k-1})|a_{k-2}|$ *for* $k \in 2 : (n-2)$;

(4) $|a_k| \geq |b_k|$ *for* $k \in 0 : (n-2)$;

(5) $|a_k|/|a_{k-1}| \geq |b_k|/|b_{k-1}|$ *for* $k \in 1 : (n-2)$;

(6) $|a_{n-1}| \geq |a_{n-4}|$.

Proof. (1) Since the subsequence $\{a_k\}$ satisfies (4), we have $|a_1| > |a_0|$. By the triangle inequality and the induction assumption, we have

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

The desired inequality follows from the fact that $|t_k| \geq 2$ for $2 \leq k \leq n-2$.

Item (2) stems from item (1).

(3) Use the formula $|x + y| = |x| + \operatorname{sgn}(xy)|y|$, valid for $|x| \geq |y|$. Since

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

we obtain

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

(4) Let $t = \{t_k\} = \{t_1, t_2, \dots\}$ be some sequence. By analogy with (4), put

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

Consider the two sequences $t = \{t_k\}$ and $\hat{t} = \{\hat{t}_k\}$ with the properties mentioned in Lemma 2. Refer to a sequence $\hat{t}$ *dominating* if, for every other sequence t, we have $|a_k(t)| \geq |a_k(\hat{t})|$ for $0 \leq k \leq n-2$. The existence of a dominating sequence can be easily proved by induction by gluing dominating sequences of smaller lengths with varying initial conditions.

Suppose that $a_k = a_k(t)$ for some t. Then, for $k \geq 3$, we have

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

If $|t_{k-1}| \geq 3$ then the minimum of this expression is attained for $t_k = -\operatorname{sgn}(t_{k-1})2$. If $|t_{k-1}| = 2$ then, by property 3 of Lemma 2, we can choose t_k so that $t_k t_{k-1} > 0$. Then the minimum is attained at $t_k = \operatorname{sgn}(t_{k-1})2$.

Let $\hat{t}$ be a dominating sequence. It is easy to see that $\hat{t}_1 = \pm 1$ and $\hat{t}_2 = \mp 2$. For $k \geq 3$, the choice of t_k must agree with the greedy choice rule for t_k described in the previous paragraph. Using this rule, we obtain that a dominating sequence for $k \geq 3$ must satisfy $t_k = \mp 2$; which proves the assertion.

(5) In a similar fashion, use the notation $a_k(t) = a_{k-1}(t) t_k + a_{k-2}(t) + [t = 0]$ and introduce the definition of dominating sequence. Consider two arbitrary sequences $t = \{t_k\}$ and $\hat{t} = \{\hat{t}_k\}$ satisfying the properties of Lemma 2. Call a sequence $\hat{t}$ *dominating* if every other sequence t satisfies

$$\frac{|a_k(t)|}{|a_{k-1}(t)|} \geq \frac{|a_k(\hat{t})|}{|a_{k-1}(\hat{t})|}, \qquad 0 \leq k \leq n-2.$$

Let $a_k = a_k(t)$ for some t. Then for $k \geq 2$ we have

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

If $|t_{k-1}| \geq 3$ then the minimum of this expression is attained for $t_k = -\operatorname{sgn}(t_{k-1})2$. If $|t_{k-1}| = 2$ then, by property 3 of Lemma 2, we can choose t_k so that $t_k t_{k-1} > 0$. In this case, the minimum is attained for $t_k = \operatorname{sgn}(t_{k-1})2$.

Using analogous arguments, as at the end of item (4), we conclude that

$$\frac{|a_k|}{|a_{k-1}|} \geq \frac{|b_k|}{|b_{k-1}|}, \qquad k \geq 0.$$

(6) We cannot apply item (1) for $|a_{n-1}|$ since $|t_{n-1}| = 1$ is possible. However, we can show that $|a_{n-1}| \geq |a_{n-4}|$.

By definition,

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

If $|t_{n-1}| \geq 2$ or $\operatorname{sgn}(t_{n-1}t_{n-2}) = 1$ then, by Lemma 3(1), we have $|a_{n-1}| \geq |a_{n-2}| > |a_{n-4}|$. Otherwise,

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

If $|t_{n-2}| \geq 3$ or $\operatorname{sgn}(t_{n-2}t_{n-3}) = 1$ then $|a_{n-1}| \geq |a_{n-3}| > |a_{n-4}|$. Otherwise,

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

If $|t_{n-3}| \geq 3$ then $|a_{n-1}| \geq |a_{n-3}| > |a_{n-4}|$. Otherwise, $|t_{n-2}| = |t_{n-3}| = 2$ and $\operatorname{sgn}(t_{n-2}t_{n-3}) = -1$. By Lemma 2(3), this situation is impossible, and so either $|t_{n-2}| \geq 3$ or $|t_{n-3}| \geq 3$.

Lemma 3 is proved. □

Theorem 8. *For each $k \geq 0$, we have*

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

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

Proof. The sequence b_k is a shifted sequence of Pell numbers with changed initial conditions. Using the standard tools of the method of generating functions (see, for example, [21, pp. 337–350]), we can prove the first equality. Prove the second equality:

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

where $\alpha = (\sqrt{2} - 1)/(\sqrt{2} + 1)$. If k is even then $|b_k|/|b_{k+1}| \leq (\sqrt{2} + 1)^{-1}$. If k is odd then

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

Theorem 8 is proved. □

Theorem 9. *Suppose that Algorithm 1 has produced $n \geq 5$ iterations and $\mathrm{MIN}_f(2) \subseteq R \cdot B_2^2$. Then $n \leq \log_{(1+\sqrt{2})} R + O(1)$.*

Proof. Since the nth iteration is final, we have $|a_n| = |a_{n-1}|$ or $|a_n| = |a_{n-2}|$. We cannon apply Lemma 3(1) to $|a_{n-1}|$ but, by item(6), $|a_{n-1}| \geq |a_{n-4}|$.

Since the second minimum of f lies in $R \cdot B_2^2$, we have $|a_n| \leq R$. By Theorem 8 and Lemma 3(4), we obtain

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

for some constant C. Theorem 9 is proved. □

The following algorithms make it possible to carry out an effective search of a minimum point t^* of f on the straight line $L(t) = z + t(z - y)$ and are used at Step 5 in Algorithm 1:

Algorithm 2

Input : The comparison oracle of f; a parameter k such that $t^* \geq 2^k$.

Output : An interval $[t_{st}, t_{fn})$ containing t^*.

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

Algorithm 3

Input : The comparison oracle of f and an interval $[t_{st}, t_{fn})$ containing t^*.

Output : The point t^*.

```
while $t_{st} \neq t_{fn} - 1$ do
    $t_{\text{mid}} := \lfloor (t_{st} + t_{fn})/2 \rfloor$
    if $f(z + (t_{\text{mid}} - 1)y) \leq f(z + t_{\text{mid}}y)$ then
        $t_{fn} := t_{\text{mid}}$
    else
        $t_{st} := t_{\text{mid}}$
    end if
end while
return $t_{st}$
```

Lemma 4. *Suppose that a point*

$$t^* \in \arg\min_{t \in \mathbb{Z}} f(z + ty)$$

is defined for a function f in DConic_2 *and $k \in \mathbb{N}$. Then there exists an algorithm for the search for t^* making at most $2 + k$ comparisons for $|t^*| \in [0, 2^k)$ and at most $3 - k + 2\log_2 |t^*|$ comparisons for $|t^*| \in [2^k, +\infty)$.*

Proof. Let $g(t) = f(z + ty)$. For finding t^*, we must determine to which of the rays corresponding to $t \geq 0$ and $t \leq 0$ the point t^* belongs. This can be done by comparing $g(0)$ and $g(1)$. Suppose that $t^* \in [0, +\infty)$.

Compare the values $g(2^k - 1)$ and $g(2^k)$. If $g(2^k - 1) \leq g(2^k)$ then the minimum is in $[0, 2^k)$; apply Algorithm 3 for finding it. This case requires $2 + k$ calls to the oracle in total.

In the opposite case, we have $g(2^k - 1) > g(2^k)$ and $t^* \in [2^k, +\infty)$. For finding an interval of the form $[2^{k+p-1}, 2^{k+p})$ to which t^* belongs, use Algorithm 2 with parameter k. For this, the algorithm needs p calls to the oracle. After that apply Algorithm 3 to find t^* in this interval, for which we need $k + p - 1$ calls to the oracle. In total, the case under consideration requires $1 + k + 2p$ calls to the oracle. Since $p \leq \log_2 t^* - k + 1$, the total number of calls to the oracle is at most $3 - k + 2\log_2 t^*$.

Lemma 4 is proved. □

Theorem 10. *Suppose that Algorithm* 1 *has been launched for finding an f-reduced basis for $\mathbb{Z}^2$ with respect to an even function $f\colon \mathbb{Z}^2 \to \mathbb{R}$ in* DConic_2 *equipped by the comparison oracle. Suppose that the second minimum point of f lies in the ball of radius R and Algorithm* 1 *has produced $n \geq 3$ iterations for its search.*

Then the total number of calls to the oracle produced by Algorithm 1 *is at most*

$$3.32 \log_2 R + O(1).$$

The estimate is found provided that Lemma 4 *was used for finding a minimum on straight lines arising at Step* 5 *of Algorithm* 1.

Proof. Let s be the number of the iterations of the algorithm at which $|t_i| < 2^k$. Note that, at the last iteration, at most two calls to the oracle are made and $t_n = 0$. By Lemma 2, $|t_i| \geq 2$ for all $2 \leq i \leq n-2$. We will assume that $|t_{n-1}| \geq 2$ since otherwise the analysis is only simplified. By Lemma 4, the total number of calls to the oracle with account taken of an additional comparison made at the beginning of each iteration is equal to

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

Estimate the sum using the following

Lemma 5.

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

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

Proof. It is easy to verify that the following inequality holds for every integer $t \geq 2$ and $\epsilon \in (0,1)$:

$$\log_2 t \leq \log_2(t-\epsilon) + 1 - \log_2(2-\epsilon), \tag{6}$$

where equality is attained for $t = 2$. Prove that

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

By Lemma 3(1), reckoning with the fact that $|t_{n-1}| \geq 2$, for $1 \leq i \leq n-1$ we have

$$|a_i| \geq |t_i||a_{i-1}| - |a_{i-2}|,$$

whence

$$\frac{|a_i|}{|a_{i-1}|} \geq |t_i| - \frac{|a_{i-2}|}{|a_{i-1}|}.$$

By Lemma 3(5), for $1 \leq i \leq n-2$ the following

$$\frac{|a_i|}{|a_{i-1}|} \geq \frac{|b_i|}{|b_{i-1}|}$$

is true. By Theorem 8, we obtain

$$\frac{|b_i|}{|b_{i-1}|} \geq (1+\sqrt{2}) \frac{1}{1 + O(\alpha^{i-1})},$$

where $\alpha = (\sqrt{2}-1)/(\sqrt{2}+1)$. Since $|t_{n-1}| \geq 2$, we obtain $|a_{n-1}|/|a_{n-2}| \geq 1$. Since $a_{-1} = 0$, $a_0 = 1$, $a_1 = t_1$, and $|a_{n-1}| \leq R$, multiplying the inequalities for $|a_i|/|a_{i-1}|$ and taking the logarithm, we infer what was required.

Using (6) and (7), we obtain

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

$$\text{where } \epsilon_i = |a_i|/|a_{i+1}|. \qquad (8)$$

By Lemma 3(5) and Theorem 8, for $0 \leq i \leq n-3$ we have

$$\epsilon_i \leq \frac{1}{\sqrt{2}+1}(1 + O(\alpha^k)).$$

The obtained inequalities yield

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

The lemma follows from this inequality and (8). Lemma 5 is proved. □

Using (5) and Lemma 5, we conclude that the total number of calls to the oracle is as follows:

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

For $k \leq 3 < 3/2 + \sqrt{2} + \gamma$, we can neglect the third summand in the estimate. In this case, the minimum is attained for $k = 3$ and equals

$$(1 + 2\gamma)n + O(1) + 2\log_2 R.$$

Using Theorem 9, we infer that the number of calls to the oracle is equal to

$$\left(2 + \frac{1+2\gamma}{\log_2(1+\sqrt{2})}\right)\log_2 R + O(1) \leq 3.32\log_2 R + O(1).$$

Theorem 10 is proved. □

ACKNOWLEDGMENTS

The authors are especially grateful to S. I. Veselov, N. Yu. Zolotykh, and A. Yu. Chirkov for their invaluable help in the preparation of the manuscript.

FUNDING

The authors were supported by the Russian Foundation for Basic Research (project no. 18–31–2001–mol-a-ved).

REFERENCES

1. A. Yu. Chirkov, "Minimization of a Quasiconvex Function on 2-Dimensional Lattice," Vestnik of Lobachevsky State University of Nizhny Novgorod, Ser. Modeling and Optimal 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).
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 *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (Palm Springs, California, October 23–25, 2011)*, pp. 580–589.
5. L. Khachiyan and L. Porkolab, "Integer Optimization on Convex Semialgebraic Sets," Discrete and 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*, Thes. Doct. Phylosophy (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. Gribanov, 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. Gribanov, N. Yu. Zolotykh, and A. Yu. Chirkov, "Minimizing a Symmetric Quasiconvex Function on a Two-Dimensional Lattice," Discret. Anal. Issled. Oper. **25** (3), 23–35 (2018) [J. Appl. Indust. Math. **12** (3), 587–594 (2018)].
17. D. Micciancio, "Efficient Reductions Among Lattice Problems," in *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, California, January 20–22, 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 *STOC'15. Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing (Portland, Oregon, USA, June 14–17, 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 *IEEE 56th Annual Symposium on Foundations of Computer Science (Berkeley, California, October 18–20, 2015)*, pp. 563-582.
21. R. Graham, D. Knuth, and O. Patashnik, *Concrete Mathematics—A Foundation for Computer Science*, 2nd ed. (Addison-Wesley Prof., Reading, MA, USA, 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. National 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, 2nd corr. ed. (Springer, Berlin, 1993).