Discrete Comput Geom 23:207–224 (2000)
DOI: 10.1007/s004549910014

Discrete & Computational
Geometry

Integer Optimization on Convex Semialgebraic Sets*

L. Khachiyan[1] and L. Porkolab[2]

[1]Department of Computer Science, Rutgers University,
New Brunswick, NJ 08903, USA
leonid@cs.rutgers.edu

[2]Max Planck Institut für Informatik,
Im Stadtwald, 66123 Saarbrücken, Germany
porkolab@data.mpi-sb.mpg.de

Abstract. Let Y be a convex set in $\mathbb{R}^k$ defined by polynomial inequalities and equations of degree at most $d \geq 2$ with integer coefficients of binary length at most l. We show that if the set of optimal solutions of the integer programming problem $\min\{y_k \mid y = (y_1, \ldots, y_k) \in Y \cap \mathbb{Z}^k\}$ is not empty, then the problem has an optimal solution $y^* \in Y \cap \mathbb{Z}^k$ of binary length $ld^{O(k^4)}$. For fixed k, our bound implies a polynomial-time algorithm for computing an optimal integral solution y^*. In particular, we extend Lenstra's theorem on the polynomial-time solvability of linear integer programming in fixed dimension to semidefinite integer programming.

1. Introduction

Let $F(y)$ be a first-order formula over the reals, i.e., an expression of the form

$$(Q_1 x^{[1]} \in \mathbb{R}^{n_1}) \ldots (Q_\omega x^{[\omega]} \in \mathbb{R}^{n_\omega}) \;\; P(y, x^{[1]}, \ldots, x^{[\omega]}), \tag{1}$$

where:

- $y = (y_1, \ldots, y_k) \in \mathbb{R}^k$ is the vector of free variables;
- each Q_i, $i = 1, \ldots, \omega$, is one of the quantifiers $\exists$ or $\forall$;
- $P(y, x^{[1]}, \ldots, x^{[\omega]})$ is a Boolean function of m atomic predicates $g_i(y, x^{[1]}, \ldots, x^{[\omega]}) \triangle_i 0$, $i = 1, \ldots, m$, in which $\triangle_i \in \{>, <, =\}$, and the g_i's are polynomials of degree at most $d \geq 2$ with integer coefficients of binary size at most l.

* The first author was supported in part by NSF Grant CCR-9618796 and ONR Grant N00014-J-1375, and the second author was supported in part by NSF Grant CCR-9618796, EU ESPRIT LTR Project 20244 (ALCOM-IT), and a DIMACS Graduate Student Fellowship.

We call d and l the *degree* and *bit length* of $F(y)$.

Let $Y = \{y \in \mathbb{R}^k \mid F(y) \text{ true}\}$ be the solution set of (1). Consider the integer programming problem

$$y_k^* = \min\{y_k \mid y = (y_1, \ldots, y_k) \in Y \cap \mathbb{Z}^k\}. \tag{2}$$

Note that for the formula $(y_{k+1} = 0) \wedge F(y_1, \ldots, y_k)$, the $(k+1)$-dimensional problem (2) is equivalent to computing an integral point $y = (y_1, \ldots, y_k) \in Y$.

Our aim in this paper is to prove the following two results.

Theorem 1.1. *Suppose that Y is convex. If the set of optimal solutions of* (2) *is not empty, then problem* (2) *has an optimal solution $y^* = (y_1^*, \ldots, y_k^*) \in Y \cap \mathbb{Z}^k$ such that*

$$\log \max\{|y_1^*|, \ldots, |y_k^*|\} = ld^{O(k^4)\Pi_{i=1}^{\omega} O(n_i)}. \tag{3}$$

(*We assume that $n_1, \ldots, n_\omega \geq 1$, $\Pi_{i=1}^{0} = 1$, and* $\log 0 = -\infty$.)

Theorem 1.2. *For any input formula $F(y)$ whose solution set is convex, the integer optimization problem* (2) *can be solved in $l^{O(1)}(md)^{O(k^4)\Pi_{i=1}^{\omega} O(n_i)}$ time with $(md)^{O(k)\Pi_{i=1}^{\omega} O(n_i)}$ evaluations of the Boolean function P: $\{\text{true, false}\}^m \to \{\text{true, false}\}$. In particular, if the number $k + \sum_{i=1}^{\omega} n_i$ of free and quantified variables is fixed, problem* (2) *can be solved in* $\text{poly}_1(l, m, d)$ *time with* $\text{poly}_2(m, d)$ *evaluations of P, where* poly_1 *and* poly_2 *are some polynomials.*

Theorem 1.2 is a generalization of the well-known result of Lenstra [14] on the polynomial-time solvability of linear integer programming in fixed dimension. We mention three other special cases of Theorem 1.2.

Computing Integral Points in Algebraic Polyhedra. Lenstra's theorem states that, for each fixed k, there exists a polynomial-time algorithm that, given a rational polyhedron

$$Y = \left\{ y \in \mathbb{R}^k \mid \sum_{j=1}^{k} a_{ij} y_j \leq a_{i0},\ i = 1, \ldots, m \right\}, \tag{4}$$

either finds an integral point $y \in Y$, or determines that no such point exists. Theorem 1.2 can be used to extend Lenstra's result to algebraic polyhedra. Specifically, suppose that each of the input coefficients $a_{ij},\ i = 1, \ldots, m;\ j = 0, \ldots, k$, is a real algebraic number defined by some quantifier-free univariate formula $G_{ij}(t)$:

$$a_{ij} = \{t \in \mathbb{R} \mid G_{ij}(t) \text{ true}\}.$$

For instance, if a_{ij} is a root of a given univariate polynomial $g_{ij}(t) \in \mathbb{Z}[t]$, and a_{ij} is separated from all other real roots of $g_{ij}(t)$ by a given rational interval $(\alpha_{ij}, \beta_{ij})$, we have

$$G_{ij}(t) \doteq (g_{ij}(t) = 0) \wedge (\alpha_{ij} < t < \beta_{ij}).$$

Another way to characterize a_{ij} is to use the Thom encoding

$$G_{ij}(t) \doteq (g_{ij}(t) = 0) \bigwedge_{s=1}^{\deg(g_{ij})-1} (g_{ij}^{(s)}(t) \triangle_s 0), \qquad \triangle_s \in \{>, <, =\},$$

which defines a_{ij} by specifying the signs of all derivatives of $g_{ij}(t)$ at a_{ij} (see Section 2.2).

Consider the formula

$$\forall x \in \mathbb{R}^{k+1} \left\{ \bigwedge_{i=1}^{m} \left(\left[\bigwedge_{j=0}^{k} G_{ij}(x_j) \right] \Rightarrow \sum_{j=1}^{k} x_j y_j \leq x_0 \right) \right\}.$$

This formula contains $2k + 1$ free and quantified variables, and its solution set is the polyhedron (4). Hence we conclude that Lenstra's theorem holds for arbitrary algebraic polyhedra in bounded dimension.

Convex and Quasi-Convex Polynomial Programming [12], [3], [2]. Let $g_i(y_1, \ldots, y_k) \in \mathbb{Z}[y_1, \ldots, y_k]$, $i = 0, \ldots, m$, be given convex quadratic, convex polynomial, or quasi-convex polynomial functions. Theorem 1.2 implies that, for each fixed k, the integer programming problem

$$\min\{g_0(y_1, \ldots, y_k) \mid g_i(y_1, \ldots, y_k) \leq 0,\ i = 1, \ldots, m,\ \ (y_1, \ldots, y_k) \in \mathbb{Z}^k\}$$

can be solved in polynomial time.

Semidefinite Integer Programming. Theorem 1.2 applies to a wider class of semialgebraic sets than those defined by systems of quasi-convex polynomial inequalities. As an illustration, consider the formula

$$\forall x \in \mathbb{R} \left\{ \left[\bigwedge_{i=1}^{m} (a_i \cdot y \leq b_i) \right] \wedge [(\det(y - xI) \neq 0) \vee (x \geq 0)] \right\},$$

where $y \in \mathbb{R}^{k(k+1)/2}$ is a real symmetric $k \times k$ matrix, $a_1, \ldots, a_m$ are given integer symmetric matrices, $b_1, \ldots, b_m$ are given integers, I is the identity matrix, and $a \cdot y = \operatorname{trace}(ay)$ is the Frobenius inner product on the space of symmetric matrices. The convex solution set of this formula consists of all symmetric positive semidefinite matrices y such that $a_i \cdot y \leq b_i$, $i = 1, \ldots, m$. Hence the following generalization of Lenstra's theorem to integer semidefinite programming:

Corollary 1.3. *For each fixed k, there exists a polynomial-time algorithm which finds an integer symmetric positive semidefinite $k \times k$ matrix y satisfying a given system of linear inequalities $a_i \cdot y \leq b_i$, $i = 1, \ldots, m$, or decides that no such matrix exists. Given a symmetric matrix $a_0 \in \mathbb{Z}^{k(k+1)/2}$, this polynomial-time algorithm can also solve the integer semidefinite programming problem*

$$\min\{a_0 \cdot y \mid a_i \cdot y \leq b_i,\ i = 1, \ldots, m,\ y \in \mathbb{Z}^{k(k+1)/2} \textit{ positive semidefinite}\}.$$

Note that Corollary 1.3 also holds for systems of strict and/or nonstrict linear inequalities with algebraic coefficients and for positive definite and/or semidefinite matrices y.

Finally, we mention that Barvinok [4] gives a polynomial-time algorithm for counting integral points in a polytope of fixed dimension. This result should be contrasted with the observation that computing the number $N(a, b)$ of integral points in the two-dimensional convex region $\{(y_1, y_2) \mid 1 \le y_1 \le a,\ 1 \le y_2 \le b,\ y_1 y_2 \ge b\}$ is at least as hard as factoring (because $N(a, b) - N(a, b+1) + a =$ the number of integer divisors of b in the interval $[1, a]$).

The paper is organized as follows. Section 2 reviews some results related to decision methods for the first-order theory of the reals and Kronecker's theorem on simultaneous Diophantine approximation. Section 3 contains the proof of Theorem 1.1. First, in Theorem 3.1, we consider an arbitrary formula with one existential quantifier and convex full-dimensional solution set $Y \subseteq \mathbb{R}^k$. We show by induction on k that either Y contains a small integral interior point, or Y can be "sandwiched" between two parallel hyperplanes defined by linear equations with small integral coefficients. If Y is bounded, the statement follows from the bound on real solutions of first-order formulae due to Basu et al. [6]. Assuming that Y is unbounded, we construct algebraic vectors $\beta_1, \ldots, \beta_s \in \mathbb{R}^k$ of low degree and small height such that $\beta_1, \ldots, \beta_s$ belong to the recession cone C of Y and generate the linear subspace spanned by C. Then we apply Kronecker's theorem to $\{\beta_1, \ldots, \beta_s\}$. In particular, if the only integral point in $\text{lin.hull}\{\beta_1, \ldots, \beta_s\}^\perp$ is $u = 0$, the size of an interior integral point in Y can be bounded by a quantitative version of Kronecker's theorem developed in Section 2. Otherwise, we use a unimodular transformation and projection of Y to finish the proof of Theorem 3.1 by induction on the dimension of the lattice $\mathbb{Z}^k \cap \text{lin.hull}\{\beta_1, \ldots, \beta_s\}^\perp$. Next, we generalize Theorem 3.1 to formulae whose convex solution set Y is not necessarily full-dimensional and argue that either Y has a small integral solution, or $\mathbb{Z}^k \cap Y$ is contained between two parallel hyperplanes defined by small integral coefficients. This easily implies Theorem 1.1. Finally, in Section 4 we derive the complexity bounds of Theorem 1.2 by using the bound of Theorem 1.1 along with a straightforward adaptation of Lenstra's integer programming algorithm for convex semialgebaic sets.

2. Preliminaries

2.1. *Notation*

Throughout the paper all vectors are row vectors, unless specified otherwise. For a real vector $\xi = (\xi_1, \ldots, \xi_k)$, we denote by

$$|\xi| = \max\{|\xi_1|, \ldots, |\xi_k|\}, \qquad \|\xi\|_2 = \left(\sum_{i=1}^{k} \xi_i^2\right)^{1/2}$$

the l_∞ and l_2-norms of ξ, respectively. The l_∞-distance from ξ to the lattice $\mathbb{Z}^k$ is denoted by

$$\|\xi\| = \min\{|\xi - x|\colon\ x \in \mathbb{Z}^k\}.$$

In particular, if ξ is a real number, then $\|\xi\| = \min\{|\xi - x|\colon\ x = 0, \pm 1, \pm 2, \ldots\}$ is the distance from ξ to the nearest integer. If $h(y_1, \ldots, y_k) = \sum a_{i_1 \cdots i_k} y_1^{i_1} \cdots y_k^{i_k} \in \mathbb{Z}[y_1, \ldots, y_k]$ is a polynomial with integral coefficients, then $|h| = \max |a_{i_1 \cdots i_k}|$ denotes the height of h.

2.2. *Computing Algebraic Solutions for First-Order Formulae*

It is well known that over the reals, any first-order formula $F(y)$ is equivalent to a quantifier-free formula

$$\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} (h_{ij}(y) \ \triangle_{ij}\ 0), \tag{QF}$$

where $h_{ij}(y) \in \mathbb{Z}[y_1, \ldots, y_k]$ are polynomials with integer coefficients and $\triangle_{ij} \in \{<, =\}$. The following bounds on the degrees and binary lengths of the polynomials $h_{ij}(y)$ are due to Basu et al. [6].

Proposition 2.1 (see Theorem 1 of [6]). *Each formula* (1) *can be transformed into an equivalent quantifier-free formula* (QF) *such that*

$$I \le m^{(k+1)\Pi_{i=1}^{\omega}(n_i+1)} d^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}, \qquad J_i \le m^{\Pi_{i=1}^{\omega}(n_i+1)} d^{\Pi_{i=1}^{\omega} O(n_i)},$$

$$\deg\ h_{ij}(y) \le d^{\Pi_{i=1}^{\omega} O(n_i)}, \qquad \log|h_{ij}| \le l d^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}.$$

The above transformation requires $m^{(k+1)\Pi_{i=1}^{\omega}(n_i+1)} d^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}$ *arithmetic operations and evaluations of the Boolean function* P *and it can be carried out over* $l d^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}$*-bit numbers.*

Proposition 2.2 below is implicit in [6].

Proposition 2.2. *Let* Y *be the solution set of a system* $\bigwedge_{j=1}^{J} (h_j(y) \ \triangle_j\ 0)$ *of* J *polynomial equations and inequalities, where* $h_j(y) \in \mathbb{Z}[y_1, \ldots, y_k]$, $j = 1, \ldots, J$, *are polynomials of degree at most* $D \ge 2$ *with coefficients of binary length at most* L. *In* $J^{k+1} D^{O(k)}$ *arithmetic operations over* $L D^{O(k)}$*-bit numbers one can determine whether* $Y \ne \emptyset$, *and, if so, find a nontrivial polynomial* $G(t) \in \mathbb{Z}[t]$, *a vector* $\sigma \in \{0, \pm 1\}^{\deg(G)-1}$, *and* $k+1$ *polynomials* $Q(t), P_1(t), \ldots, P_k(t) \in \mathbb{Z}[t]$ *such that*

$$\max\{\deg(G), \deg(Q), \deg(P_1), \ldots, \deg(P_k)\} = O(D)^k,$$

$$\log \max\{(|G|, |Q|, |P_1|, \ldots, |P_k|\} = L D^{O(k)},$$

and

$$y = \left(\frac{P_1(\theta)}{Q(\theta)}, \ldots, \frac{P_k(\theta)}{Q(\theta)} \right) \in Y,$$

where θ *is a real algebraic number satisfying the conditions*

$$G(\theta) = 0, \qquad (\operatorname{sign}(G'(\theta)), \ldots, \operatorname{sign}(G^{(\deg(G)-1)}(\theta)) = \sigma. \tag{5}$$

Note that conditions (5) characterize θ. These conditions, known as Thom's encoding of θ, define θ even if $G(t)$ is a reducible polynomial. On the other hand, since $G(t)$ can be factored in polynomial time [13], and the sign of any of its factors at θ can also be determined in polynomial time, the minimal polynomial $g(t) \in \mathbb{Z}[t]$ for θ can be computed in time polynomial in $\deg(G)$ and $\log|G|$. Furthermore, it is well known that $\log|g| \leq \log|G| + O(\deg(G))$ (see, e.g., [15]). Since the polynomial $Q^{-1}(t) \bmod g(t)$ can be computed in polynomial time, and the binary length of its rational coefficients can be bounded via subresultants by $O(\deg(gQ)\log(|g||Q|\deg(gQ)))$ bits (see, e.g., [9] and [7]), Propositions 2.1 and 2.2 readily imply the following result.

Corollary 2.3. *There is an algorithm that, given a first-order formula $F(y)$, either determines that $F(y)$ has no real solution, or finds an irreducible polynomial $g(t) \in \mathbb{Z}[t]$, an integer $q \neq 0$, and k polynomials $p_1(t), \ldots, p_k(t) \in \mathbb{Z}[t]$ such that*

$$y = \frac{1}{q}(p_1(\theta), \ldots, p_k(\theta)) \in Y, \qquad g(\theta) = 0, \tag{6}$$

$$\deg(p_1), \ldots, \deg(p_k) < \deg(g) = d^{O(k)\Pi_{i=1}^{\omega} O(n_i)},$$

$$\log \max\{|g|, |q|, |p_1|, \ldots, |p_k|\} = ld^{O(k)\Pi_{i=1}^{\omega} O(n_i)},$$

where Y is the solution set of $F(y)$. The algorithm runs in $l^{O(1)}(md)^{O(k)\Pi_{i=1}^{\omega} O(n_i)}$ time and requires $(md)^{O(k)\Pi_{i=1}^{\omega} O(n_i)}$ evaluations of P.

Remark 2.4. Suppose that the solution set of $F(y)$ is homogeneous, i.e., $\lambda y \in Y$ for all $y \in Y$ and $\lambda > 0$. Then in Corollary 2.3 we can choose $q = 1$, and assume without loss of generality that θ is an algebraic integer: lead.coeff $g(t) = 1$.

2.3. *Inscribing a Box into a Full-Dimensional Semialgebraic Set*

Proposition 2.5 below is a restatement of Theorems 5 and 6 of [6].

Proposition 2.5. *Let $Y \neq \emptyset$ be the solution set of a system of strict polynomial inequalities $\bigwedge_{j=1}^{J} (h_j(y) < 0)$, where $h_j(y) \in \mathbb{Z}[y_1, \ldots, y_k]$, $j = 1, \ldots, J$, are polynomials of degree at most $D \geq 2$ with coefficients of binary length at most L. Then Y contains a box $\{y \in \mathbb{R}^k : |y - \alpha| < 1/R\}$ such that $|\alpha| \leq R$ and $\log R = LD^{O(k)}$.*

This result along with Proposition 2.1 leads to the following bound.

Corollary 2.6. *If the solution set Y of a formula $F(y)$ is full-dimensional, then there is a box $\mathcal{B} = \{y \in \mathbb{R}^k : |y - \alpha| < 1/R\} \subseteq Y$ such that $|\alpha| \leq R$ and $\log R = ld^{O(k)\Pi_{i=1}^{\omega} O(n_i)}$.*

2.4. *Kronecker's Theorem on Simultaneous Diophantine Approximations*

Let $\beta_1, \ldots, \beta_s$ be given vectors in $\mathbb{R}^k$. The classical Kronecker theorem on simultaneous Diophantine approximations asserts that *for every real vector $\alpha \in \mathbb{R}^k$ the following two*

statements are equivalent:

(i) *For any* $\varepsilon > 0$ *there is an* $x = (x_1, \ldots, x_s) \in \mathbb{Z}^s$ *such that* $\|\alpha + \sum_{i=1}^s x_i\beta_i\| \le \varepsilon$.
(ii) *For every* $u = (u_1, \ldots, u_k)^T \in \mathbb{Z}^k$, *if* $\|\beta_1 u\| = \cdots = \|\beta_s u\| = 0$ *then* $\|\alpha u\| = 0$.

(See, e.g., [8].) The fact that (i) implies (ii) is trivial. Proposition 2.7 below can be regarded as a quantitative version of the reverse implication.

Proposition 2.7 [8, Chapter V, Theorem XVII, Part B]. *Let* $\alpha \in \mathbb{R}^k$ *be a given vector, and let* X *and* ε *be given positive numbers. A sufficient condition that*

$$\left\| \alpha + \sum_{i=1}^{s} x_i\beta_i \right\| \le \varepsilon, \qquad |x| \le X, \tag{7}$$

holds for some $x \in \mathbb{Z}^s$ *is that*

$$\|\alpha u\| \le \gamma \max\{\varepsilon|u|, X\|\beta_1 u\|, \ldots, X\|\beta_s u\|\} \tag{8}$$

for all $u \in \mathbb{Z}^k$ *with* $\gamma = 2^{k-1}/[(k+s)!]^2$.

Since $\|\alpha u\| \le \frac{1}{2}$ for all α and u, from Proposition 2.7 it follows that (7) can be satisfied for any α provided that the right-hand side of (8) is at least $\frac{1}{2}$. Since this is so for $|u| \ge 1/(\gamma\varepsilon)$, we conclude that for every $\alpha \in \mathbb{R}^k$ there is an $x \in \mathbb{Z}^s$ that satisfies (7) with

$$X = \frac{1}{\min\left\{\max_{j=1,\ldots,s} \|\beta_j u\| : u \in B'_{1/\gamma\varepsilon}\right\}},$$

where $B'_{1/\gamma\varepsilon} = \{u \in \mathbb{Z}^k \mid 0 < |u| \le 1/(\gamma\varepsilon)\}$ (assuming the finiteness of X). On replacing X and α by $2X$ and $\alpha + X\sum_{i=1}^s \beta_i$, respectively, it follows that the conditions

$$\left\| \alpha + \sum_{i=1}^{s} x_i\beta_i \right\| \le \varepsilon, \qquad 0 \le x_i \le X, \quad i = 1, \ldots, s,$$

$$X = \frac{2}{\min\{\max_j \|\beta_j u\| : u \in B'_{1/\gamma\varepsilon}\}} \tag{9}$$

can be satisfied by some integral x provided that the expression for X in (9) is finite.

Corollary 2.8. *Suppose that the only integral solution of the homogeneous system of linear equations* $\beta_1 u = \cdots = \beta_s u = 0$ *is* $u = 0$. *Then for any* $\alpha \in \mathbb{R}^k$ *and any* $\varepsilon > 0$ *there is a real vector* $\lambda = (\lambda_1, \ldots, \lambda_s)$ *such that*

$$\left\| \alpha + \sum_{i=1}^{s} \lambda_i\beta_i \right\| \le \varepsilon, \qquad 0 \le \lambda_i \le \Lambda, \quad i = 1, \ldots, s,$$

where

$$\Lambda = \frac{2}{\min\{\max_j |\beta_j u| : u \in B'_{1/\gamma\varepsilon}\}}. \tag{10}$$

Proof. First, Λ is finite because the set $B'_{1/\gamma\varepsilon}$ contains finitely many integral vectors $u \neq 0$ for each of which $(\beta_1 u, \ldots, \beta_s u) \in \mathbb{R}^s \backslash \{0\}$. Next, let $\lambda = \tau x$, where $x \in \mathbb{Z}^s$ and $\tau > 0$ is a fixed positive parameter. Then finding a solution to $\|\alpha + \sum_{i=1}^s \lambda_i \beta_i\| \leq \varepsilon$ is equivalent to solving $\|\alpha + \tau \sum_{i=1}^s x_i \beta_i\| \leq \varepsilon$ for integral x. For τ sufficiently small, $\|\tau \beta_i u\| = \tau |\beta_i u|$ for all $i = 1, \ldots, s$ and $u \in B'_{1/\gamma\varepsilon}$. Hence $\|\alpha + \tau \sum_{i=1}^s x_i \beta_i\| \leq \varepsilon$ can be solved by an integral x such that $0 \leq x_i \leq \Lambda/\tau$ (see (9) and (10)). This implies $0 \leq \lambda_i = \tau x_i \leq \Lambda$ for all $i = 1, \ldots, s$. □

In what follows we will be dealing with algebraic vectors $\beta_1, \ldots, \beta_s$.

Corollary 2.9. *Let $\beta_1, \ldots, \beta_s \in \mathbb{R}^k$ satisfy the assumption of Corollary* 2.8. *Suppose that the components of $\beta_1, \ldots, \beta_s$ are algebraic integers represented in the form* (6):

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_s \end{pmatrix} = \sum_{j=0}^{D-1} \theta^j B_j, \qquad g(\theta) = 0, \tag{11}$$

where $g(t) = t^D + g_1 t^{D-1} + \cdots + g_D \in \mathbb{Z}[t]$ is an irreducible polynomial of degree D, and $B_0, \ldots, B_{D-1}$ are integral $s \times k$ matrices such that $\log \max\{|g|, |B_0|, \ldots, |B_{D-1}|\} \leq L$. *Then the parameter Λ in Corollary* 2.8 *can be bounded as follows*:

$$\log \Lambda = O\left(D[L + \log(D/\varepsilon) + k \log k]\right).$$

Proof. Since the powers $1, \theta, \ldots, \theta^{D-1}$ are linearly independent over the rationals, and the matrices B_j are integral, each linear equation $\beta_i u = 0,\ u \in \mathbb{Z}^k$, is equivalent to the system of D Diophantine equations $B_0[i]u = \cdots = B_{D-1}[i]u = 0,\ u \in \mathbb{Z}^k$, where $B_j[i]$ is the ith row of the matrix B_j. This means that the assumption of Corollary 2.8 holds for a subsystem of $\beta_1, \ldots, \beta_s$ consisting of at most k vectors. We can thus assume that $s \leq k$, and therefore $\log(1/\gamma) = \log([(k+s)!]^2/2^{k-1}) = O(k \log k)$. Let $\nu = \min\{\max_i |\beta_i u| : u \in B'_{1/\gamma\varepsilon}\}$; then $\nu = |\beta_{i^*} u^*|$ for some $i^* \in \{1, \ldots, s\}$ and $u^* \in B'_{1/\gamma\varepsilon}$. By (11), $\nu = v(\theta)$, where $v(t) \in \mathbb{Z}[t]$ is a polynomial of height $|v| \leq k 2^L/(\gamma\varepsilon)$. Consider the univariate polynomial $U(t) = \prod_{j=1}^D (t - v(\theta_j))$, where $\theta_1 = \theta, \theta_2, \ldots, \theta_D$ are the conjugates of θ. It is easy to see that the coefficients of $U(t)$ are integral, and that

$$|U| \leq 2^D \prod_{i=1}^D \max\{1, |v(\theta_i)|\} \leq (2D|v|)^D \left(\prod_{i=1}^D \max\{1, |\theta_i|\} \right)^{D-1}.$$

Since $\theta_1, \ldots, \theta_D$ are the roots of the polynomial $g(t)$, by Landau's inequality [15] we have $\prod_{i=1}^D \max\{1, |\theta_i|\} \leq (1 + |g_1|^2 + \cdots + |g_D|^2)^{1/2} \leq (D+1)^{1/2}|g|$. Hence $|U| \leq (|g||v|D)^{O(D)}$. However, $\nu = v(\theta)$ is a positive root of $U(t) \in \mathbb{Z}[t]$, which implies that $\nu \geq 1/(1+|U|)$ (see, e.g., [15]). Consequently, $\log \Lambda = \log(2/\nu) = O(D[L + \log D + \log(k/(\gamma\varepsilon))])$. □

3. Proof of Theorem 1.1

We start with the following result.

Theorem 3.1. *Let $\Phi(y) \doteq \exists x \in \mathbb{R}^n P(y, x)$ be a formula with one existential quantifier, where $P(y, x)$ is a Boolean function of m polynomial predicates $g_i(y, x) \triangle_i 0$ of degree $d \geq 2$ with integral coefficients of binary length l. Suppose that the solution set $Y \subseteq \mathbb{R}^k$ of $\Phi(y)$ is convex and full-dimensional.*

(i) *If $\mathbb{Z}^k \cap \operatorname{int} Y \neq \emptyset$, then Y contains an interior integral point $\bar{y}$ such that*

$$\log|\bar{y}| \leq ld^{ck^3(n+k)}, \tag{12}$$

where $c > 0$ is an absolute constant.

(ii) *If $\mathbb{Z}^k \cap \operatorname{int} Y = \emptyset$, then there is an integral vector $a = (a_1, \ldots, a_k)^T \neq 0$ and integers b_1, b_2 such that*

$$Y \subseteq \{y \in \mathbb{R}^k \mid b_1 \leq ya \leq b_2\}, \tag{13}$$

$$\log \max\{|a|, |b_1|, |b_2|\} \leq ld^{ck^2(n+k)}. \tag{14}$$

Proof of Theorem 3.1. We prove the theorem by induction on $k = \dim Y$.

The One-Dimensional Case. For $k = 1$ the set Y is an interval. If $Y = \mathbb{R}$, we have nothing to prove. Otherwise Y has a finite endpoint α. From Proposition 2.1 it follows that α satisfies a nontrivial polynomial equation $h(y) = 0$ with integral coefficients of binary length $ld^{O(n)}$. Since the absolute value of any root of $h(y) = 0$ does not exceed $1 + |h|$, we have $\log|\alpha| = ld^{O(n)}$. If $\operatorname{int} Y \cap \mathbb{Z} \neq \emptyset$, then $|\bar{y} - \alpha| \leq 1$ for some $\bar{y} \in \operatorname{int} Y \cap \mathbb{Z}$, which gives (12). Otherwise the length of Y is at most 1, which implies (13) and (14).

For convenience, we separately consider another special case of Theorem 3.1.

The Bounded Case. Suppose that Y is bounded, and consider the formula

$$\forall(y, x) \in \mathbb{R}^{k+n} \left\{ \neg P(x, y) \vee \bigwedge_{j=1}^{k} (\pm y_j \leq r) \right\}.$$

The solution set of this formula is the interval $[r^*, +\infty)$, where $r^* = \sup\{|y| : y \in Y\} < +\infty$. By Proposition 2.1, r^* satisfies a univariate polynomial equation with integral coefficients of binary length $ld^{O(k+n)}$. Hence

$$\log|y| = ld^{O(k+n)} \qquad \text{for all} \quad y \in Y, \tag{15}$$

which implies the theorem.

We assume henceforth that $\dim Y = k \geq 2$, and that the convex full-dimensional set Y is unbounded.

Constructing a Spanning Set for the Recession Cone of Y. Consider the recession cone of Y, i.e., the set $C = \{y \in \mathbb{R}^k \mid \alpha + \lambda y \in Y \text{ for all } \lambda > 0\}$, where α is an arbitrary interior

point of Y. (It is well known that this definition is invariant with respect to $\alpha \in \operatorname{int} Y$.) Let $\mathcal{L} = \text{lin.hull } C$ and $s = \dim \mathcal{L}$. Since Y is unbounded, $s \in \{1, \ldots, k\}$. A set of s vectors $\beta_1, \ldots, \beta_s \in C$ is called a *spanning set for* C if $\text{lin.hull}\{\beta_1, \ldots, \beta_s\} = \mathcal{L}$.

Lemma 3.2. *The recession cone C has an algebraic integer spanning set $\beta_1, \ldots, \beta_s$ of the form*

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_s \end{pmatrix} = \sum_{j=0}^{D-1} \theta^j B_j, \qquad g(\theta) = 0, \tag{16}$$

where $g(t) = t^D + g_1 t^{D-1} + \cdots + g_D \in \mathbb{Z}[t]$ is an irreducible polynomial of degree

$$D = d^{O(sk(n+\log s))}, \tag{17}$$

and $B_0, \ldots, B_{D-1}$ are integral $s \times k$ matrices such that

$$\log \max\{|g|, |B_0|, \ldots, |B_{D-1}|\} = ld^{O(sk(n+\log s))}. \tag{18}$$

Proof of Lemma 3.2. By Corollary 2.6, the full-dimensional set Y contains a rational interior point $p/q = (p_1/q, \ldots, p_k/q)$ such that $p_1, \ldots, p_k$ and $q \geq 1$ are integers of binary length $ld^{O(kn)}$. The recession cone C is the solution set of the formula

$$\forall\, \lambda \in \mathbb{R}\{(\lambda < 0) \vee \Phi(p/q + \lambda y)\}. \tag{19}$$

The change of variables $y \to p/q + \lambda y$ transforms each of the m atomic polynomial predicates $g_i(y, x) \triangle_i 0$ into the polynomial relation $G_i(\lambda, y, x) \triangle_i 0$, where $G_i(\lambda, y, x) \doteq q^d g_i(p/q + \lambda y, x) \in \mathbb{Z}[\lambda, y, x]$ is a polynomial with integral coefficients of binary length $ld^{O(kn)}$. In particular, (19) can be written as

$$(\forall\, \lambda \in \mathbb{R})\ (\exists x \in \mathbb{R}^n)\{(\lambda < 0) \vee P_*(\lambda, y, x)\}, \tag{20}$$

where $P_*(\lambda, y, x)$ is obtained from $P(y, x)$ by the substitution $g_i(y, x) \to G_i(\lambda, y, x)$. By Proposition 2.1, (20) can be transformed into an equivalent quantifier-free formula $C(y)$ of degree $d^{O(n)}$ and bit length $ld^{O(kn)}$.

Given s vectors $\beta_1, \ldots, \beta_s \in \mathbb{R}^k$, denote by $G(\beta_1, \ldots, \beta_s)$ their Gram matrix $G_{ij} = \beta_i \beta_j^T$. By definition, $\{\beta_1, \ldots, \beta_s\}$ is a spanning set for the recession cone C if and only if $C(\beta_1) \wedge \cdots \wedge C(\beta_s) \wedge (\det G(\beta_1, \ldots, \beta_s) \neq 0)$. This quantifier-free formula has sk variables and consists of polynomial relations of degree $\max\{d^{O(n)}, 2s\} = d^{O(n+\log s)}$ with integral coefficients of binary length $ld^{O(kn)}$. Since the set of all spanning vectors $\{\beta_1, \ldots, \beta_s\}$ is homogeneous, the lemma follows from Corollary 2.3 and Remark 2.4. □

We continue with the proof of Theorem 3.1.

Let $\mathcal{M} = \mathcal{L}^\perp = \{u \in \mathbb{R}^k \mid \beta_1 u = \cdots = \beta_s u = 0\}$ be the orthogonal complement of $\mathcal{L}$, i.e., the set of all linear forms u that vanish on C. Denote by $\mathcal{M}_I = \mathbb{Z}^k \cap \mathcal{M}$ the set of all integral points in $\mathcal{M}$. By Lemma 3.2, $\mathcal{M}_I = \{u \in \mathbb{Z}^k \mid \beta_1 u = \cdots = \beta_s u = 0\}$ is a lattice of the form

$$\mathcal{M}_I = \{u \in \mathbb{Z}^k \mid Mu = 0\}, \tag{21}$$

where M is an integral $(k-p)\times k$ matrix of full row rank such that

$$\log|M| = ld^{O(sk(n+\log s))}. \tag{22}$$

Note that p, the dimension of $\mathcal{M}_I$, is bounded by $\dim \mathcal{M} = k-s$. Hence $p \in \{0,1,\ldots,k-1\}$. We now split the proof into two cases: $p=0$ and $p \geq 1$.

The Kronecker Case. Suppose that $p=0$. Then the only integral solution of $\beta_1 u = \cdots = \beta_s u = 0$ is $u=0$. Hence the recession directions $\beta_1,\ldots,\beta_s$ satisfy the assumption of Corollary 2.9 with $D = d^{O(sk(n+\log s))}$ and $L = ld^{O(sk(n+\log s))}$. By Corollary 2.6, Y contains an open box $\mathcal{B} = \{y \in \mathbb{R}^k : |y-\alpha| < 1/R\}$ such that $|\alpha| \leq R$ and $\log R = ld^{O(kn)}$. Since $\mathcal{B} \subseteq \operatorname{int} Y$, and $\beta_1,\ldots,\beta_s \in C$, we have $\mathcal{B} + \sum_{i=1}^s \lambda_i \beta_i \subseteq Y$ for all nonnegative $\lambda_1,\ldots,\lambda_s$. Applying Corollary 2.9 with $\varepsilon = (2R)^{-1}$ we conclude that there are nonnegative scalars $\lambda_1^*,\ldots,\lambda_s^*$ for which the conditions

$$\mathbb{Z}^k \cap \left(\mathcal{B} + \sum_{i=1}^s \lambda_i^* \beta_i\right) \neq \emptyset, \qquad 0 \leq \lambda_i^* \leq \Lambda, \quad i = 1,\ldots,s,$$

can be satisfied with a Λ such that

$$\log \Lambda = O\left(D[L + \log(D/\varepsilon) + k\log k]\right) = ld^{O(sk(n+\log s))}.$$

Let $\bar{y}$ be an (interior) integral point in $\mathcal{B} + \sum_{i=1}^s \lambda_i^* \beta_i$. Since the polynomial $g(t)$ in (16) has integral coefficients of binary length $ld^{O(sk(n+\log s))}$, we have $\log|\theta| = ld^{O(sk(n+\log s))}$. The latter bound along with (17) and (18) shows that $\log \max\{|\beta_1|,\ldots,|\beta_s|\} = ld^{O(sk(n+\log s))}$. Consequently, $\log|\bar{y}| = ld^{O(sk(n+\log s))}$. Since $s < k$, it follows that $\log|\bar{y}| = ld^{O(k^2(n+\log k))}$. This means that, for $p=0$, $\Phi(y)$ has an interior integral solution that satisfies (12).

Induction. Let $p = \dim \mathcal{M}_I \geq 1$. Then $p \in \{1,\ldots,k-s\}$, where $s = \dim C \geq 1$. By (21), $\mathcal{M}_I = \{u \in \mathbb{Z}^k \mid Mu = 0\}$ for some integral $(k-p)\times k$ matrix M of full row rank. The lattice $\mathcal{M}_I$ is invariant under all transformations $M \to VM$, where V is a nondegenerate rational matrix of order $k-p$. Next, for any unimodular matrix U of order k, the change of variables

$$y = y'U \tag{23}$$

transforms $\Phi(y)$ into the formula $\Phi'(y') = \exists x \in \mathbb{R}^n P(y'U, x)$ with the solution set $Y' = YU^{-1}$. By unimodularity, $Y' \cap \mathbb{Z}^k = (Y \cap \mathbb{Z}^k)U^{-1}$, that is, (23) gives a one-to-one correspondence between the sets of integral solutions of $\Phi(y)$ and $\Phi'(y')$. Note that $C' = CU^{-1}$ and $\mathcal{M}_I' = \{u \in \mathbb{Z}^k \mid VMU^{-1}u = 0\}$, where C' is the recession cone of Y' and $\mathcal{M}_I'$ is the lattice of integral forms vanishing on C'. By reducing the matrix M to the Smith normal form, we can compute a nondegenerate rational matrix V and a unimodular matrix U such that $M' = VMU^{-1} = (0, I)$, where I is the identity matrix of order $k-p$. Moreover, since the binary length of each element of U can be bounded by $O(k\log(k|M|))$ bits (see, e.g., Chapter 5 of [17]), from (22) it follows that we may assume without loss of generality that

$$\log|U| = ld^{O(sk(n+\log s))}. \tag{24}$$

Consequently, $\Phi'(y')$ has bit length $ld^{O(sk(n+\log s))}$. For simplicity of notation, we assume henceforth that

$$M = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \tag{25}$$

for the *original* formula $\Phi(y)$, and that the bit length of $\Phi(y)$ has been increased to $ld^{O(sk(n+\log s))}$. By (25), $\mathcal{M}_I = (\mathbb{Z}^p, 0)$ and hence

$$\beta_i = (0, \bar{\beta}_i), \qquad i = 1, \ldots, s, \tag{26}$$

where the vectors $\bar{\beta}_i \in \mathbb{R}^{k-p}$ satisfy the assumption of Corollary 2.9:

$$\{u \in \mathbb{Z}^{k-p} \mid \bar{\beta}_1 u = \cdots = \bar{\beta}_s u = 0\} = \{0\}. \tag{27}$$

Consider the partition $y = (y^{[1]}, y^{[2]})$, where $y^{[1]} = (y_1, \ldots, y_p)$ and $y^{[2]} = (y_{p+1}, \ldots, y_k)$. Let

$$\Phi^{[1]}(y^{[1]}) \doteq \exists (y^{[2]}, x) \in \mathbb{R}^{n+k-p} P(y, x),$$

and let $Y^{[1]}$ be the solution set of $\Phi^{[1]}(y^{[1]})$. Since $Y^{[1]}$ is a projection of Y, the set $Y^{[1]} \subseteq \mathbb{R}^p$ is convex and full-dimensional.

Lemma 3.3. *A point $\bar{y}^{[1]}$ belongs to $\mathbb{Z}^p \cap \operatorname{int} Y^{[1]}$ if and only if there is a point $\bar{y}^{[2]} \in \mathbb{Z}^{k-p}$ such that $(\bar{y}^{[1]}, \bar{y}^{[2]}) \in \mathbb{Z}^k \cap \operatorname{int} Y$.*

Proof of Lemma 3.3. The fact that $(\bar{y}^{[1]}, \bar{y}^{[2]}) \in \mathbb{Z}^k \cap \operatorname{int} Y$ implies $\bar{y}^{[1]} \in \mathbb{Z}^p \cap \operatorname{int} Y^{[1]}$ follows directly from the definition of $Y^{[1]}$. Suppose that $\bar{y}^{[1]} \in \mathbb{Z}^p \cap \operatorname{int} Y^{[1]}$. Since $\bar{y}^{[1]}$ is an interior point of $Y^{[1]}$, the set $Y^{[1]}$ is a projection of Y, and Y is convex and full-dimensional, there exists a real vector $\xi \in \mathbb{R}^{k-p}$ such that $(\bar{y}^{[1]}, \xi) \in \operatorname{int} Y$. Hence there is a positive ε such that the open box $\mathcal{B} = \{(y^{[1]}, y^{[2]}) : |y^{[1]} - \bar{y}^{[1]}| < \varepsilon, |y^{[2]} - \xi| < \varepsilon\}$ belongs to Y. In view of (27), Kronecker's theorem guarantees the existence of nonnegative scalars $\lambda_1, \ldots, \lambda_s$ such that $\|\xi + \sum_{i=1}^s \lambda_i \bar{\beta}_i\| < \varepsilon$. Since the vectors $\beta_1, \ldots, \beta_s$ in (26) are recession directions of Y, it follows that the set $\mathcal{B} + \sum_{i=1}^s \lambda_i \beta_i$ belongs to Y and contains an interior integer point. □

Now we are ready to prove parts (i) and (ii) of Theorem 3.1 by induction.

(i) Suppose that $\mathbb{Z}^k \cap \operatorname{int} Y \neq \emptyset$. Then $\Phi^{[1]}(y^{[1]})$ has an interior integral solution $\bar{y}^{[1]}$ whose binary length can be bounded by applying the induction hypothesis (12) in p dimensions:

$$\log|\bar{y}^{[1]}| = ld^{cp^3(n+k)+O(sk(n+\log s))},$$

where the multiplicative constant hidden in the term $O(sk(n + \log s))$ does not depend on c. Substitute $\bar{y}^{[1]}$ into $\Phi(y)$ and consider the resulting formula

$$\Phi^{[2]}(y^{[2]}) \doteq \Phi(\bar{y}^{[1]}, y^{[2]}).$$

The solution set $Y^{[2]} \subseteq \mathbb{R}^{k-p}$ of $\Phi(y^{[2]})$ is the intersection of Y with the subspace $\{y \in \mathbb{R}^k \mid y^{[1]} = \bar{y}^{[1]}\}$. Since $\bar{y}^{[1]} \in \operatorname{int} Y^{[1]}$, it follows that $Y^{[2]}$ is convex and full-dimensional. By Lemma 3.3, $\mathbb{Z}^{k-p} \cap \operatorname{int} Y^{[2]} \neq \emptyset$. Hence we can use the induction hypothesis (12) in $k-p$ dimensions to bound the binary length of an interior integral solution $\bar{y}^{[2]}$ of $\Phi^{[2]}(y^{[2]})$. We can thus assume that $\log|(\bar{y}^{[1]}, \bar{y}^{[2]})|$ is bounded by

$$ld^{cp^3(n+k)+c(k-p)^3(n+k-p)+O(sk(n+\log s))},$$

where, as before, the constant in the term $O(sk(n+\log s))$ does not depend on c. (Note that this bound remains true after the transformation (23).) It is easy to see that the inclusions $\bar{y}^{[i]} \in \operatorname{int} Y^{[i]}$, $i = 1, 2$, guarantee that $(\bar{y}^{[1]}, \bar{y}^{[2]}) \in \operatorname{int} Y$. To obtain the required bound (12) in k dimensions it remains to show that if $k \geq 2$, then

$$cp^3(n+k) + c(k-p)^3(n+k-p) + sk(n+\log s) \leq ck^3(n+k)$$

for c sufficiently large. (We have scaled the multiplicative constant in the term $O(sk(n+\log s))$ to 1.) Since $1 \leq p \leq k-1$ and $s \leq k$, we have

$$\begin{aligned} cp^3(n+k) + c(k-p)^3(n+k-p) + sk(n+\log s) &\leq c[p^3 + (k-p)^3](n+k) + k^2(n+\log k) \\ &\leq [c(k-1)^3 + c + k^2](n+k). \end{aligned}$$

Hence the required inequality holds for $c \geq \frac{2}{3}$.

(ii) Suppose that $\mathbb{Z}^k \cap \operatorname{int} Y = \emptyset$. By Lemma 3.3, $\mathbb{Z}^p \cap \operatorname{int} Y^{[1]} = \emptyset$. Inductively applying part (ii) of the theorem to $\Phi^{[1]}(y^{[1]})$ we conclude that $Y^{[1]} \subseteq \{y^{[1]} \in \mathbb{R}^p \mid b_1 \leq y^{[1]}a^{[1]} \leq b_2\}$, where $a^{[1]} \in \mathbb{Z}^p \setminus \{0\}$, and $\log\max\{|a^{[1]}|, |b_1|, |b_2|\} = ld^{cp^2(n+k)+O(sk(n+\log s))}$. Hence we obtain (13) with

$$a = U^{-1}\begin{pmatrix} a^{[1]} \\ 0 \end{pmatrix}.$$

By (24),

$$\log\max\{|a|, |b_1|, |b_2|\} = ld^{cp^2(n+k)+O(sk(n+\log s))}.$$

Scaling the constant in the term $O(sk(n+\log s))$ to 1, letting $c = 1$, and taking into account the inequality $s \leq k-p$, we can bound the exponent of d as follows:

$$\begin{aligned} p^2(n+k) + sk(n+\log s)) &\leq pk(n+k) + (k-p)k(n+\log(k-p)) \\ &\leq k[p(n+k) + (k-p)(n+k-p)] \leq k^2(n+k). \end{aligned}$$

This shows (14) and completes the proof of Theorem 3.1. □

Theorem 3.4. *Let $P(y)$ be a quantifier-free formula composed of polynomial predicates $g_i(y) \triangle_i 0$, where $g_i(y) \in \mathbb{Z}[y_1, \ldots, y_k]$ are polynomials of degree $d \geq 2$ with coefficients of binary length l. Suppose that the set $Y = \{y \in \mathbb{R}^k \mid P(y)\,\text{true}\}$ is convex.*

Then Y satisfies at least one of the following two conditions:

(i) *Y contains an integral point y such that* $\log|y| = ld^{O(k^4)}$.
(ii) *There is an integral vector $a \neq 0$ and integers b_1, b_2 such that*

$$Y \cap \mathbb{Z}^k \subseteq \{y \in \mathbb{Z}^k \mid b_1 \leq ya \leq b_2\}, \tag{28}$$

$$\log \max\{|a|, |b_1|, |b_2|\} = ld^{O(k^3)}. \tag{29}$$

Proof of Theorem 3.4. Any quantifier-free formula $P(y)$ can be written as $\exists x \in \mathbb{R}^1 P(y)$, where x is a dummy variable. If Y is full-dimensional, Theorem 3.4 is thus a special case of Theorem 3.1 for $n = 1$. Suppose that Y is not full-dimensional. Since $Y \subset \mathbb{R}^k$ is convex, there exist a vector $u = (u_1, \ldots, u_k)^T \in \mathbb{R}^k$ and a scalar $v \in \mathbb{R}$ such that $u \neq 0$ and $yu = v$ for all $y \in Y$. The set of all vectors $(u, v) \in \mathbb{R}^{k+1}$ that satisfy these two conditions is the solution set of the formula

$$H(u, v) \doteq \forall y \in \mathbb{R}^k \{[u^T u > 0] \wedge [\neg P(y) \vee (yu = v)]\}.$$

Since the solution set of $H(u, v)$ is homogeneous, from Corollary 2.3 and Remark 2.4 it follows that $H(u, v)$ has a solution of the form

$$\begin{pmatrix} u^* \\ v^* \end{pmatrix} = \sum_{j=0}^{D-1} \theta^j \begin{pmatrix} u_j^* \\ v_j^* \end{pmatrix},$$

where θ is an algebraic integer of degree $D = d^{O(k^2)}$,

$$\begin{pmatrix} u_j^* \\ v_j^* \end{pmatrix} \in \mathbb{Z}^{k+1}, \qquad j = 0, \ldots, D-1, \qquad \text{and}$$

$$\log \max\{|u_j^*|, |v_j^*| : j = 0, \ldots, D-1\} = ld^{O(k^2)}.$$

For integral y, the linear equation $yu^* = v^*$ is equivalent to the system of D Diophantine linear equations $yu_0^* = v_0^*, \ldots, yu_{D-1}^* = v_{D-1}^*$. Since $u^* = \sum_{j=0}^{D-1} \theta^j u_j^* \neq 0$, we have $u_j^* \neq 0$ for at least one of the D integral vectors $u_0^*, \ldots, u_{D-1}^*$. Hence we obtain (28) and (29) with $a = u_j^*$ and $b_1 = b_2 = v_j^*$. □

Corollary 3.5. *Let $P(y)$ satisfy the assumptions of Theorem* 3.4, *and let Y be the solution set of $P(y)$.*

(i) *If $Y \cap \mathbb{Z}^k \neq \emptyset$, then Y contains an integral point y such that* $\log|y| \leq ld^{ck^4}$, *where $c > 0$ is a constant.*
(ii) *If $y_k^* = \min\{y_k \mid y = (y_1, \ldots, y_k) \in Y \cap \mathbb{Z}^k\}$ is finite, then* $\log|y_k^*| \leq ld^{ck^4}$.

Proof of Corollary 3.5. (i) We prove the statement by induction on k, the number of free variables. The case $k = 1$ is trivial. Suppose that $k \geq 2$. By Theorem 3.4 we can assume without loss of generality that there exists an integral vector $a \neq 0$ and an integer b such that

$$Y \cap \{y \in \mathbb{Z}^k \mid ya = b\} \neq \emptyset, \tag{30}$$

and $\log \max\{|a|, |b|\} = ld^{O(k^3)}$. The general integral solution of the equation $ya = b$ has the form $y = t + y'T$, where y' runs through $\mathbb{Z}^{k-1}$, and T and t are an integral $(k-1) \times k$ matrix and k-vector such that

$$\log \max\{|T|, |t|\} = ld^{O(k^3)}. \tag{31}$$

(See, e.g., Chapter 5 of [17].) Substituting $t + y'T$ for y into the original formula $P(y)$, we obtain a new quantifier-free formula $P'(y') \doteq P(t + Ty')$ whose set of solutions is still convex. It is easy to see that the degree d', bit length l', and the number k' of free variables for $P'(y')$ can be bounded as follows: $d' \leq d$, $l' = ld^{O(k^3)}$, $k' \leq k-1$. Moreover, by (30), $P'(y')$ has an integer solution $\bar{y}'$. By the induction hypothesis, $\log|\bar{y}'|$ can be bounded by $l'(d')^{ck'^4}$. Hence $\log|\bar{y}'| = ld^{c(k-1)^4+O(k^3)}$, where the constant in the term $O(k^3)$ does not depend on c. However, then $\bar{y} = t + \bar{y}'T$ is an integral solution for $P(y)$ for which (31) yields $\log|\bar{y}| = ld^{c(k-1)^4+O(k^3)}$. This inductively proves (i).

(ii) We again use induction on k with the trivial base $k = 1$. If $y_k^* \geq 0$, then (ii) follows from part (i) above. Assume that $y_k^* < 0$ and let $\xi_k^* = \inf\{\xi_k \mid \xi = (\xi_1, \ldots, \xi_k) \in Y\}$. If $\xi_k^* > -\infty$, then $\log|\xi_1^*| = ld^{O(k)}$ by Proposition 2.1 and we are done. Suppose that $\xi_k^* = -\infty$. Then $\mathbb{Z}^k \cap \operatorname{int} Y = \emptyset$, for otherwise from Minkowski's theorem it would follow that Y contains a sequence of points $y = (y_1, \ldots, y_k) \in \mathbb{Z}^k \cap \operatorname{int} Y$ with $y_k \to -\infty$, which would contradict our assumption that y_k^* is finite. If Y is full-dimensional, Theorem 3.1 guarantees that the integer programming problem $\min\{y_k \mid y \in Y \cap \mathbb{Z}^k\}$ has an optimal solution y^* satisfying a linear equation $ya = b$ with integral coefficients $a = (a_1, \ldots, a_k)^T \neq 0$ and b of binary length $ld^{O(k^3)}$. If Y is not full-dimensional then such an equation can be found for the entire set Y (see the proof of Theorem 3.4). As before, the general integral solution of $ya = b$ can be written in the form $y = t + y'T$, where $y' \in \mathbb{Z}^{k-1}$ and $T \in \mathbb{Z}^{(k-1)\times k}$, $t \in \mathbb{Z}^k$ satisfy (31). After an appropriate unimodular transformation $y' \to y'U$, we can assume without loss of generality that $T_{1,k} = T_{2,k} = \cdots = T_{k-2,k} = 0$ and $T_{k-1,k} \geq 0$. If $T_{k-1,k} = 0$, then $y_k^* = t_k$ and (ii) follows from (31). Otherwise $y_k = t_k + y'_{k-1}T_{k-1,k}$ with $T_{k-1,k} > 0$. This reduces the original integer programming problem to $y'^*_{k-1} = \min\{y'_{k-1} \mid y' = (y'_1, \ldots, y'_{k-1}) \in Y' \cap \mathbb{Z}^{k-1}\}$, where $Y' \subset \mathbb{R}^{k-1}$ is the solution set of $P'(y') \doteq P(t + y'T)$, and completes the inductive proof. □

Corollary 3.6. *Let $P(y)$ be a quantifier-free formula whose solution set Y is convex. If the set of optimal solutions of the integer optimization problem $y_k^* = \min\{y_k \mid y = (y_1, \ldots, y_k) \in Y \cap \mathbb{Z}^k\}$ is nonempty, then the problem has an optimal solution y^* such that*

$$\log|y^*| = ld^{O(k^4)}, \tag{32}$$

where $d \geq 2$ and l are the degree and bit length of $P(y)$, respectively.

Proof of Corollary 3.6. Any integral solution of the formula $P^*(y) \doteq (y_k \leq y_k^*) \wedge P(y)$ solves the optimization problem. By part (ii) of Corollary 3.5, the bit length of $P^*(y)$ is $ld^{O(k^4)}$. Hence by part (i) of the same corollary, $P^*(y)$ has an integral solution y^* in the box (32). □

Proof of Theorem 1.1. By Proposition 2.1, any input formula $F(y)$ with $\omega \geq 1$ quantifiers can be transformed into an equivalent quantifier-free formula (QF) of degree $d_{\mathrm{QF}} = d^{\prod_{i=1}^{\omega} O(n_i)}$ and bit length $l_{\mathrm{QF}} = ld^{(k+1)\prod_{i=1}^{\omega} O(n_i)}$. Substituting d_{QF} and l_{QF} for d and l in (32) results in the required bound (3) for $F(y)$. □

4. Proof of Theorem 1.2

Before proceeding to the proof of Theorem 1.2 we pause to make a few observations. First, due to Proposition 2.1, it suffices to prove that the integer optimization problem (2) can be solved in $l^{O(1)}m^{O(k^3)}d^{O(k^4)}$ time for any convex set Y defined by a quantifier-free formula $P(y)$ of form (QF) with m polynomial predicates of degree d and integral coefficients of binary length l. Secondly, we can use binary search along with the bound of Theorem 1.1 to reduce the integer optimization problem (2) to $ld^{O(k^4)}$ feasibility subproblems of the following form: Given a fixed parameter $t \in \mathbb{Z}$, find an integral solution $y = (y_1, \ldots, y_k)$ for $(y_k \leq t) \wedge P(y)$, or prove that no such solution exists. Since $(y_k \leq t) \wedge P(y)$ is also a formula of the form (QF), to prove Theorem 1.2 we only need to show the following result:

> There is an algorithm of running time $l^{O(1)}m^{O(k^3)}d^{O(k^4)}$ that, given a quantifier-free formula $P(y)$ of form (QF) with convex solution set $Y \subseteq \mathbb{R}^k$ and m polynomial predicates of degree d and bit length l, either determines that $Y \cap \mathbb{Z}^k = \emptyset$ or finds a point $y \in Y \cap \mathbb{Z}^k$. (33)

Observe that (33) trivially holds for $k = 1$ (even without the convexity assumption). Finally, we can assume without loss of generality that Y is full-dimensional, for otherwise by using the argument presented in the proof of Theorem 3.4 the number of variables in $P(y)$ can be reduced in $l^{O(1)}(md)^{O(k^2)}$ time.

Let Y be a bounded convex full-dimensional set in $\mathbb{R}^k$. An affine transformation

$$y \to a + yA$$

ρ-rounds Y if $U_1 \subseteq a + YA \subseteq \bar{U}_\rho$, where $U_1 = \{y \in \mathbb{R}^k : \|y\|_2 < 1\}$ and $\bar{U}_\rho = \{y \in \mathbb{R}^k : \|y\|_2 \leq \rho\}$ are the open and closed Euclidean balls of radii 1 and ρ, respectively, centered at the origin. Denote by $\mathcal{QF}(k, m, d, l)$ the class of bounded convex k-dimensional sets $Y \subset \mathbb{R}^k$ defined by quantifier-free formulae (QF) composed of m polynomial relations of degree d and bit length l.

Lemma 4.1. *Given a set $Y \in \mathcal{QF}(k, m, d, l)$, a rational $(k+1)$-rounding affine transformation for Y can be computed in $l^{O(1)}(md)^{O(k^3)}$ time. In particular, for fixed k, such a transformation can be found in time polynomial in l, m, and d.*

Proof. It is well known that any bounded convex full-dimensional set in $\mathbb{R}^k$ can be k-rounded [11]. Suppose that Y is defined by a quantifier-free formula $P(y)$. Then the nonempty set of all k-rounding affine transformations for Y can be characterized by the the formula

$$R(a, A) \doteq (\forall y \in \mathbb{R}^k)\,\{[(\|a + yA\|_2 \geq 1) \vee P(y)] \wedge [(\|a + yA\|_2 \leq k) \vee \neg P(y)]\}.$$

Let ε be a positive number, and consider an *ε-approximate* solution of $R(a, A)$, i.e., a rational matrix (a', A') such that $\|(a', A') - (a, A)\|_2 \leq \varepsilon$ for some exact solution (a, A) of $R(a, A)$. Since the Hausdorff distance

$$\inf\{\delta \mid a + YA \subseteq \text{Euclidean } \delta\text{-neighborhood of } a' + YA', \\ \text{and } a' + YA' \subseteq \text{Euclidean } \delta\text{-neighborhood of } a + AY\}$$

between the sets $a' + YA'$ and $a + YA$ is at most $\|a' - a\|_2 + r^*\|A' - A\|_2$, where $r^* = \sup\{\|y\|_2 : y \in Y\}$, it follows that $U_{1-\varepsilon(r^*+1)} \subseteq a' + YA' \subseteq \bar{U}_{k+\varepsilon(r^*+1)}$. By (15), $\log r^* = ld^{O(k)}$. Hence Y can be $(k+1)$-rounded by computing an ε-approximate solution for $R(a, A)$ with $-\log \varepsilon = ld^{O(k)}$. Note that by Corollary 2.6, Y contains a Euclidean ball $\{y \in \mathbb{R}^k : \|y - \alpha\|_2 \leq 1/R\}$ such that $\|\alpha\|_2 \leq R$ and $\log R = ld^{O(k)}$. This implies that $\log\|(a, A)\|_2 = ld^{O(k)}$ for any solution (a, A) of $R(a, A)$.

It is known [16, Theorem 1.2] that an ε-approximate solution for an arbitrary formula $F(y)$ can be computed in $l^{O(1)}(md)^{O(k)\Pi_i O(n_i)} \log\log(3+r/\varepsilon)$-time, where r is an upper bound on the Euclidean norm of an exact solution. Applying this result to $R(a, A)$, the lemma follows. □

Let $\mathcal{K}$ be a class of bounded convex full-dimensional sets in $\mathbb{R}^k$. Consider the problem:

P_k: Given a set $Y \in \mathcal{K}$, determine whether $Y \cap \mathbb{Z}^k \neq \emptyset$, and, if so, find a point $y \in Y \cap \mathbb{Z}^k$.

Suppose that each set $Y \in \mathcal{K}$ can be ρ-rounded by an appropriate rational affine transformation. Then for a ρ-rounded set Y Lenstra's algorithm can either solve problem P_k in polynomial time, or reduce it to $\rho 2^{O(k)}$ subproblems P_{k-1}, each of which calls for computing an integral vector y in the intersection of Y with a given rational hyperplane $\{y \in \mathbb{R}^k \mid a_1y_1 + \cdots + a_ky_k = b\}$ ([1]; see also [14], [10], and [17]). By Lemma 4.1, this implies that for any set in $\mathcal{QF}(k, m, d, l)$ problem P_k can be solved in $l^{O(1)}(md)^{O(k^3)}$ time, or reduced to $2^{O(k)}$ similarly structured $(k-1)$-dimensional problems. Hence one can conclude by induction on k that problem P_k can be solved in $l^{O(1)}(md)^{O(k^3)}$ time for any input set $Y \in \mathcal{Q}(k, m, d, l)$. This proves (33) for *bounded* sets Y. Finally, suppose that the solution set Y of a quantifier-free formula $P(y)$ is convex but not necessarily bounded. By Theorem 1.1, computing an integral solution for $P(y)$ is equivalent to computing an integral solution for $(|y| \leq r) \wedge P(y)$, where r is a positive integer of binary size $ld^{O(k^4)}$. This proves (33) and hence Theorem 1.2 for an arbitrary convex semialgebraic set Y. □

We mention in closing that applying the shallow-cut ellipsoid method [10], [17] for rounding semialgebraic sets in $\mathcal{Q}(k, m, d, l)$, along with Theorem 1 of [5], the running time of the integer programming algorithm in Theorem 1.2 can be improved to $l^{O(1)}d^{O(k^4)\Pi_{i=1}^{\omega}O(n_i)}m^{O(k^2)\Pi_{i=1}^{\omega}O(n_i)}$. Most likely, the bound of Theorem 1.1 can also be improved in terms of its dependence on k. We also expect that Corollary 1.3 can be strengthened by developing an algorithm for semidefinite integer optimization in fixed dimension whose running time is linear m.

References

1. L. Babai, On Lovász' Lattice Reduction and the Nearest Lattice Point Problem, *Combinatorica* 6:1–13, 1986.
2. B. Bank, J. Heintz, T. Krick, R. Mandel, and P. Solernó, Une Borne Optimale pour la Programmation Entière Quasi-convexe, *Bull. Soc. Math. France*, 121:299–314, 1993.
3. B. Bank, T. Krick, R. Mandel, and P. Solernó, A Geometrical Bound for Integer Programming with Polynomial Constraints (extended abstract), in: *Fundamentals of Computation Theory* (ed. by L. Budach), Lecture Notes in Computer Science, vol. 529, pp. 121–125, Springer-Verlag, Berlin, 1991.
4. A.I. Barvinok, A Polynomial Time Algorithm for Counting Integral Points in Polyhedra when the Dimension Is Fixed, *Math. Oper. Res.*, 19:769–779, 1994.
5. S. Basu, An Improved Algorithm for Quantifier Elimination over Real Closed Fields, *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, pp. 56–65, 1997.
6. S. Basu, R. Pollack, and M.-R. Roy, On the Combinatorial and Algebraic Complexity of Quantifier Elimination, *J. Assoc. Comput. Mach.*, 43:1002–1045, 1996.
7. W.S. Brown and J.F. Traub, On Euclid's Algorithm and the Theory of Subresultants, *J. Assoc. Comput. Mach.*, 18:505–514, 1971.
8. J.W.S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge University Press, Cambridge, 1957.
9. G.E. Collins, Polynomial Reminder Sequences and Determinants, *Amer. Math. Monthly*, 73:708–712, 1966.
10. M. Grötschell, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, Berlin, 1988.
11. F. John, Extremum Problems with Inequalities as Subsidiary Conditions, in: *Studies and Essays*, presented to R. Courant on his 60th Birthday, January 8th, Wiley Interscience, New York, pp. 187–204, 1948.
12. L. Khachiyan, Convexity and Complexity in Polynomial Programming, *Proceedings of the International Congress of Mathematicians*, Warsaw, pp. 1569–1577, 1983.
13. A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász, Factoring Polynomials with Rational Coefficients, *Math. Ann.*, 261:515–534, 1982.
14. H.W. Lenstra, Jr., Integer Programming with a Fixed Number of Variables, *Math. Oper. Res.*, 8:538–548, 1983.
15. M. Mignotte, Some Useful Bounds, in: *Computer Algebra, Symbolic and Algebraic Computation* (second edition, ed. by B. Buchberger, G.E. Collins, and R. Loos, in cooperation with R. Albrecht), Springer-Verlag, Wien, pp. 259–263, 1982.
16. J. Renegar, On the Computational Complexity of Approximating Solutions for Real Algebraic Formulae, *SIAM J. Comput.*, 21:1008–1025, 1992.
17. A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, New York, 1986.

Received August 3, 1998, *and in revised form March* 22, 1999.