DIMACS Technical Report 97-14
April 1997

Computing Integral Points in Convex Semi-algebraic Sets[1]

by

Leonid Khachiyan[2]
Department of Computer Science
Rutgers University
New Brunswick, New Jersey 08903
leonid@cs.rutgers.edu
and

Lorant Porkolab[3]
RUTCOR
Rutgers University
New Brunswick, New Jersey 08903-5062
porkolab@rutcor.rutgers.edu

[1]Research supported by NSF Grant CCR-9618796 and ONR Grant N00014-92-J-1375.
[2]Permanent Member
[3]Affiliated Graduate Student Member

DIMACS is a cooperative project of Rutgers University, Princeton University, AT&T Bell Laboratories and Bellcore.

DIMACS is an NSF Science and Technology Center, funded under contract STC–91–19999; and also receives support from the New Jersey Commission on Science and Technology.

ABSTRACT

Let Y be a convex set in $\mathbb{R}^k$ defined by polynomial inequalities and equations of degree $d \geq 2$ with integer coefficients of binary length l. We show that if $Y \cap \mathbb{Z}^k \neq \emptyset$, then Y contains an integral point of binary length $ld^{O(k^4)}$. For fixed k, our bound implies a polynomial-time algorithm for computing an integral point $y \in Y$. 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

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

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 $g_i(y, x^{[1]}, \ldots, x^{[\omega]}) \bigtriangleup_i 0$, $i = 1, \ldots, m$, in which $\bigtriangleup_i \in \{<, =\}$, and the g_i's are polynomials of degree at most $d \geq 2$ with integer coefficients of binary size at most l.

We call d and l the *degree* and *bitlength* of $F(y)$, respectively.

Let $Y = \{y \in \mathbb{R}^k \mid F(y) \text{ true}\}$ be the solution set of $F(y)$. Our aim in this paper is to prove the following two results.

Theorem 1.1 *If Y is convex and $Y \cap \mathbb{Z}^k \neq \emptyset$, then Y contains an integral point $y = (y_1, \ldots, y_k)$ such that*

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

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

Theorem 1.2 *There is an algorithm that, given a formula $F(y)$ whose solution set Y is convex, either finds an integral point $y \in Y$, or determines that no such point exists. For any fixed number $k + \Sigma_{i=1}^{\omega} n_i$ of free and quantified variables, the algorithm runs in $(lmd)^{O(1)}$ time and requires $(md)^{O(1)}$ evaluations of the Boolean function $P(\cdot)$.*

Theorem 1.2 is a generalization of the well-known theorem of Lenstra [12] on the polynomial-time solvability of linear integer programming in fixed dimension. This theorem also implies the polynomial-time solvability of systems of convex and quasi-convex polynomial inequalities with any fixed number of integer variables [10],[2]. Theorem 1.2, however, applies to a wider class of convex semi-algebraic sets than those defined by quasi-convex algebraic inequalities. As an example, consider the formula

$$\forall \lambda \in \mathbb{R} \ \{ \ [\ \wedge_{i=1}^{m} \ (A_i \cdot X \leq b_i) \ ] \ \wedge \ [\ (\det(X - \lambda I) \neq 0) \ \vee \ (\lambda \geq 0) \ ] \ \},$$

where $A_1, \ldots A_m$ are given integer symmetric matrices, I is the identity matrix, and $A \cdot X = \operatorname{tr}(AX)$ is the standard inner product on the space of symmetric matrices. The convex solution set of this formula consists of all positive semidefinite symmetric matrices X such that $A_i \cdot X \leq b_i, \ i = 1, \ldots, m$. 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 X satisfying a given system of linear inequalities $A_i \cdot X \leq b_i$, $i = 1, \ldots, m$, or decides that no such matrix exists.*

The above result also holds for systems of strict and/or nonstrict linear inequalities in positive definite and/or semidefinite matrices with integer and/or real variables, i.e., for mixed semidefinite programming.

Note that Barvinok [3] gave 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 2-dimensional convex region $\{ (y_1, y_2) \mid 1 \leq y_1 \leq a,\ 1 \leq y_2 \leq b,\ y_1 y_2 \geq b \}$ 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. The next section reviews some results related to decision methods for the first-order theory of the reals and Kronecker's theorem on simultaneous Diophantine approximation. Sections 3 and 4 prove Theorems 1.1 and 1.2.

2 Preliminaries

2.1 Notation

For a real vector $\xi = (\xi_1, \ldots, \xi_k)$, we denote by

$$|\xi| = \max\{|\xi_1|, \ldots, |\xi_k|\}, \qquad \|\xi\|_2 = (\sum_{i=1}^{k} \xi_i^2)^{1/2}, \qquad \|\xi\| = \min\{\ |\xi - x|\ :\ x \in \mathbb{Z}^k\ \}$$

the l_∞ and l_2-norms of ξ, and the l_∞-distance from ξ to the integral lattice $\mathbb{Z}^k$, respectively. In particular, if ξ is a real number, then $\|\xi\| = \min\{\ |\xi - x|\ :\ x = 0, \pm 1, \pm 2, \ldots\}$ is the distance from ξ to the nearest integer. If $h(y_1, \ldots, y_k) = \sum a_{i_1 \ldots i_k} y_1^{i_1} \cdots y_k^{i_k} \in \mathbb{Z}[y_1, \ldots, y_k]$ is a polynomial with integral coefficients, then $|h| = \max |a_{i_1 \ldots i_k}|$ 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) is equivalent to a quantifier-free formula

$$\vee_{i=1}^{I} \wedge_{j=1}^{J_i} (h_{ij}(y)\ \triangle_{ij}\ 0), \qquad (QF)$$

where $h_{ij}(y) \in \mathbb{Z}[y_1, \ldots, y_k]$ are polynomials with integer coefficients and $\triangle_{ij} \in \{<, =\}$. The best currently known bounds on the degrees and binary length of the polynomials $h_{ij}(y)$ are due to Basu, Pollack, and Roy [4].

Proposition 2.1 (cf. Theorem 1 of [4]) *Each formula (F) can be transformed into an equivalent quantifier-free formula (QF) such that* $I \leq m^{(k+1)\Pi_{i=1}^{\omega}(n_i+1)} d^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}$, $J_i \leq$

$m^{\Pi_{i=1}^{\omega}(n_i+1)}d^{\Pi_{i=1}^{\omega}O(n_i)}$, $\deg\ h_{ij}(y) \le d^{\Pi_{i=1}^{\omega}O(n_i)}$, *and* $\log|h_{ij}| \le l d^{(k+1)\Pi_{i=1}^{\omega}O(n_i)}$. *The transformation (F) $\to$ (QF) can be carried out over* $l d^{(k+1)\Pi_{i=1}^{\omega}O(n_i)}$*-bit numbers and 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* $P(\cdot)$.

The following proposition is implicit in [4], Section 3.1.3.

Proposition 2.2 *Let Y be the solution set of a system of J polynomial equations and inequalities $\wedge_{j=1}^{J}(h_j(y)\ \triangle_j\ 0)$, where $h_j(y) \in \mathbb{Z}[y_1,\dots,y_k]$ are polynomials of degree $D \ge 2$ with coefficients of binary length L. In $J^{k+1}D^{O(k)}$ arithmetic operations over $LD^{O(k)}$-bit numbers one can determine whether $Y \ne \emptyset$, and if so, find a nontrivial polynomial $G(t) \in \mathbb{Z}[t]$, a vector $\sigma \in \{0,\pm1\}^{\deg(G)-1}$, and $k+1$ polynomials $Q(t), P_1(t),\dots,P_k(t) \in \mathbb{Z}[t]$ such that $\deg(G), \deg(Q), \deg(P_1),\dots,\deg(P_k) \le O(D)^k$, $\log\max\{(|G|,|Q|,|P_1|,\dots,|P_k|\} \le LD^{O(k)}$, and*

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

where

$$G(\theta)=0, \quad (\mathrm{sign}(G'(\theta)),\dots,\mathrm{sign}(G^{(\deg(G)-1)}(\theta)) = \sigma. \tag{2}$$

Note that the conditions (2), known as Thom's encoding of θ, uniquely define the algebraic number θ even if the polynomial $G(t)$ is reducible. On the other hand, since $G(t)$ can be factored in polynomial time (Lenstra, Lenstra, Lovász [11]), 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 $\log|g| \le \log|G| + O(\deg(G))$ (see e.g. Mignotte [13]). 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 sub-resultants by $O(\deg(gQ)\log(|g||Q|\deg(gQ)))$ bits (see e.g. [7], [5]), Propositions 2.1 and 2.2 readily imply the following result.

Corollary 2.3 *There is an algorithm that, given a 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 $q \ne 0$, and k polynomials $p_1(t),\dots,p_k(t) \in \mathbb{Z}[t]$ such that*

$$y = \frac{1}{q}(p_1(\theta),\dots,p_k(\theta)) \in Y, \quad g(\theta)=0, \tag{3}$$

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

If the number $k+\Sigma_{i=1}^{\omega}n_i$ of free and quantified variables is fixed , the algorithms runs in $(lmd)^{O(1)}$ time and requires $(md)^{O(1)}$ calls to $P(\cdot)$.

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 Semi-algebraic Set

Proposition 2.5 below is a restatement of Theorems 5 and 6 of [4].

Proposition 2.5 *Let $Y \neq \emptyset$ be the solution set of a system of strict polynomial inequalities $\wedge_{j=1}^{J}(h_j(y) < 0)$, where $h_j(y) \in \mathbb{Z}[y_1, \ldots, y_k]$ are polynomials of degree $D \geq 2$ with coefficients of binary length 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 Propositions 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 a given set of s 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 $\epsilon > 0$ there is an $x = (x_1, \ldots, x_s) \in \mathbb{Z}^s$ such that $\|\alpha + \sum_{i=1}^{s} x_i\beta_i\| \leq \epsilon$;*

(ii) *For every $u = (u_1, \ldots, u_k)^T \in \mathbb{Z}^k$, if $\|\beta_1 u\| = \ldots = \|\beta_s u\| = 0$ then $\|\alpha u\| = 0$.*

(See e.g. Cassels [6].) 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 ([6], 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*

$$\|\alpha + \sum_{i=1}^{s} x_i\beta_i\| \leq \epsilon, \quad |x| \leq X \tag{4}$$

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

$$\|\alpha u\| \leq \gamma \max\{\ \epsilon|u|,\ X\|\beta_1 u\|, \ldots, X\|\beta_s u\|\ \} \tag{5}$$

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

Since $\|\alpha u\| \leq 1/2$, from Proposition 2.7 it follows that (4) can be satisfied for *any* α provided that the right-hand side of (5) is at least 1/2. Since this is so for $|u| \geq 1/(\gamma\epsilon)$, we conclude that for every $\alpha \in \mathbb{R}^k$ there is an $x \in \mathbb{Z}^s$ that satisfies (4) with

$$X = 1/\min\{\max_{j=1,\ldots,s} \|\beta_j u\| \;:\; u \in B'_{1/\gamma\epsilon}\},$$

where $B'_{1/\gamma\epsilon} = \{u \in \mathbb{Z}^k \mid 0 < |u| \leq 1/(\gamma\epsilon)\ \}$ (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

$$\|\alpha + \sum_{i=1}^{s} x_i\beta_i\| \leq \epsilon, \quad 0 \leq x_i \leq X = \frac{2}{\min\{\max_j \|\beta_j u\| : u \in B'_{1/\gamma\epsilon}\}}, \; i = 1,\ldots,s, \qquad (6)$$

can always be satisfied by some integral x provided that the expression for X on the right-hand side of (6) is finite.

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

$$\|\alpha + \sum_{i=1}^{s} \lambda_i\beta_i\| \leq \epsilon, \quad 0 \leq \lambda_i \leq \Lambda = \frac{2}{\min\{\max_j |\beta_j u| \;:\; u \in B'_{1/\gamma\epsilon}\}}, \; i = 1,\ldots,s. \qquad (7)$$

Proof. First, the Λ is finite because the set $B'_{1/\gamma\epsilon}$ contains finitely many integral vectors $u \neq 0$ for each of which $(\beta_1 u, \ldots, \beta_s u) \in \mathbb{R}^s \setminus \{0\}$. Next, let $\lambda = \tau x$, where $x \in \mathbb{Z}^s$ and $\tau > 0$ is a fixed positive parameter. Then finding a solution to $\|\alpha + \sum_{i=1}^{s}\lambda_i\beta_i\| \leq \epsilon$ is equivalent to solving $\|\alpha + \tau\sum_{i=1}^{s} x_i\beta_i\| \leq \epsilon$ in integral x. For τ sufficiently small, we have $\|\tau\beta_i u\| = \tau|\beta_i u|$ for all $i = 1,\ldots,s$ and $u \in B'_{1/\gamma\epsilon}$. Hence $\|\alpha + \tau\sum_{i=1}^{s} x_i\beta_i\| \leq \epsilon$ can be solved by an integral x such that $0 \leq x_i \leq \Lambda/\tau$ (cf. (6) and (7)). This implies $0 \leq \lambda_i = \tau x_i \leq \Lambda$ for all $i = 1,\ldots,s$. □

In the sequel, 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 (3):*

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_s \end{pmatrix} = \sum_{j=0}^{D-1} \theta^j B_j, \quad g(\theta) = 0, \qquad (8)$$

where $g(t) = t^D + g_1 t^{D-1} + \ldots + g_D \in \mathbb{Z}[t]$ 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:

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

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 $B_0[i]u = \ldots = B_{D-1}[i]u = 0,\ u \in \mathbb{Z}^k$, where $B_j[i]$ is the i-th 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 $s \le k$, and therefore $\log(1/\gamma) = \log\left([(k+s)!]^2/2^{k-1}\right) = O(k \log k)$. Let $\nu = \min\{\max_i |\beta_i u| \ :\ u \in B'_{1/\gamma\epsilon}\}$, then $\nu = |\beta_{i^*} u^*|$ for some $i^* \in \{1, \ldots, s\}$ and $u^* \in B'_{1/\gamma\epsilon}$. By (8), $\nu = v(\theta)$, where $v(t) \in \mathbb{Z}[t]$ is a polynomial of height $|v| \le k2^L/(\gamma\epsilon)$. 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

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

Since $\theta_1, \ldots, \theta_D$ are the roots of the polynomial $g(t)$, by Landau's inequality [13]

$$\prod_{i=1}^{D} \max\{1, |\theta_i|\} \le (1 + |g_1|^2 + \ldots + |g_D|^2)^{1/2} \le (D+1)^{1/2}|g|.$$

Hence $|U| \le (|g||v|D)^{O(D)}$. But $\nu = v(\theta)$ is a positive root of $U(t) \in \mathbb{Z}[t]$, which implies that $\nu \ge 1/(1+|U|)$ (see e.g. [13]). Consequently, $\log \Lambda = \log(2/\nu) = O(D[L + \log D + \log(k/(\gamma\epsilon))])$. $\square$

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 $d \ge 2$ with integral coefficients of bitlength l. Suppose that the solution set $Y \subseteq \mathbb{R}^k$ of $\Phi(y)$ is convex and full-dimensional.

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

$$\log |\bar{y}| = ld^{\,ck^3(n+k)}, \tag{9}$$

where $c > 0$ is an absolute constant;

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

$$Y \subseteq \{\ y \in \mathbb{R}^k \ |\ b_1 \le ya \le b_2\}, \tag{10}$$

$$\log \max\{|a|, |b_1|, |b_2|\} = ld^{\,ck^2(n+k)}. \tag{11}$$

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

The 1-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 y^*. From Proposition 2.1 it follows that y^* satisfies a nontrivial polynomial equation $h(y) = 0$ with integral coefficients of bitlength $ld^{O(n)}$. Since the absolute value of any root of $h(y) = 0$ does not exceed $1 + |h|$, we have $\log |y^*| = ld^{O(n)}$. If $\text{int}\ Y \cap \mathbb{Z} \neq \emptyset$, then $|\bar{y} - y^*| \leq 1$ for some $\bar{y} \in \text{int}\ Y \cap \mathbb{Z}$, which gives (9). Otherwise the length of Y is at most 1, which implies (10) and (11).

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

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

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

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 bitlength $ld^{O(k+n)}$. Hence

$$\log |y| = ld^{O(k+n)} \quad \text{for all} \quad y \in Y, \tag{12}$$

which implies the theorem.

Constructing a spanning set for the recessive cone of Y. We assume henceforth that $\dim\ Y = k \geq 2$, and that the convex set Y is unbounded. Consider the recessive cone of Y, i.e., the set $C = \{y \in \mathbb{R}^k \mid \alpha + \lambda y \in Y \quad \text{for all} \quad \lambda > 0\}$, where α is an arbitrary interior point of Y. (It is well known that this definition is invariant with respect to $\alpha \in \text{int}\ Y$.) Let $\mathcal{L} = \mathit{lin.hull}\ C$ 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 $\mathit{lin.hull}\{\beta_1, \ldots, \beta_s\} = \mathcal{L}$.

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

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_s \end{pmatrix} = \sum_{j=0}^{D-1} \theta^j B_j, \quad g(\theta) = 0, \tag{13}$$

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

$$D = d^{\ O(sk(n+\log s))}, \tag{14}$$

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

$$\log \max\{|g|, |B_0|, \ldots, |B_{D-1}|\} = ld^{\ O(sk(n+\log s))}. \tag{15}$$

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 bitlength $ld^{O(kn)}$. The recessive cone C is the solution set of the formula

$$\forall\ \lambda \in \mathbb{R}\ \{\ (\ \lambda < 0\ )\ \vee\ \Phi(p/q + \lambda y)\ \}. \tag{16}$$

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 bitlength $ld^{O(kn)}$. In particular, (16) can be written as

$$(\forall\ \lambda \in \mathbb{R})\ (\exists\ x \in \mathbb{R}^n)\ \{\ (\ \lambda < 0\ )\ \vee\ P_*(\lambda, y, x)\ \}, \tag{17}$$

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, (17) can be transformed into an equivalent quantifier-free formula $C(y)$ of degree $d^{O(n)}$ and bitlength $ld^{O(kn)}$.

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 recessive cone C if and only if $C(\beta_1) \wedge \ldots \wedge C(\beta_s) \wedge (\ \det\ G(\beta_1, \ldots, \beta_s) \neq 0\ )$. 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 bitlength $ld^{O(kn)}$. 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. $\square$

We continue with the proof of Theorem 3.1.

Let $\mathcal{M} = \mathcal{L}^\perp = \{\ u \in \mathbb{R}^k \mid \beta_1 u = \ldots = \beta_s u = 0\ \}$ 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,

$$\mathcal{M}_I = \{\ u \in \mathbb{Z}^k \mid \beta_1 u = \ldots = \beta_s u = 0\} = \{\ u \in \mathbb{Z}^k \mid Mu = 0\}, \tag{18}$$

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

$$\log |M| = ld^{\ O(sk(n + \log s))}. \tag{19}$$

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

The Kronecker case. Suppose that $p = 0$. Then the only integral solution of $\beta_1 u = \ldots = \beta_s u = 0$ is $u = 0$. Hence the recessive 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 $\mathcal{B} \subseteq \text{int}\ Y$, 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 $\epsilon = (2R)^{-1}$ we conclude that there are nonnegative scalars $\lambda_1^*, \ldots, \lambda_s^*$ for which the conditions

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

can be satisfied with a Λ such that

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

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 (13) has integral coefficients of bitlength $ld^{\ O(sk(n+\log s))}$, we have $\log|\theta| = ld^{\ O(sk(n+\log s))}$. The latter bound along with (14) and (15) 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 (9).

Induction. Let $p = \dim \mathcal{M}_I \geq 1$. Then $p \in \{1, \ldots, k-s\}$, where $s = \dim\ C \geq 1$. By (18), $\mathcal{M}_I = \{\ u \in \mathbb{Z}^k \mid Mu = 0\ \}$ for some integral $(k-p) \times k$-matrix M of full row rank. The lattice $\mathcal{M}_I$ is invariant under all transformation $M \rightarrow VM$, where V is a nondegenerate rational matrix of order $k-p$. Next, for any unimodular matrix U of order k, the change of variables

$$y = y'U \tag{20}$$

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, (20) 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 recessive 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 U can be bounded by $O(k \log(k|M|))$ bits (see e.g. [15], Ch. 5), from (19) it follows that we may assume without loss of generality that

$$\log|U| = ld^{\ O(sk(n+\log s))}. \tag{21}$$

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

$$M = \begin{pmatrix} 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & 1 & \ldots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \tag{22}$$

for the *original* formula $\Phi(y)$, and that the bitlength of $\Phi(y)$ has been increased to $ld^{\ O(sk(n+\log s))}$. By (22), $\mathcal{M}_I = (\mathbb{Z}^p, 0)$ and hence

$$\beta_i = (0, \bar{\beta}_i), \ \ i = 1, \ldots, s, \tag{23}$$

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

$$\{\ u \in \mathbb{Z}^{k-p} \mid \bar{\beta}_1 u = \ldots = \bar{\beta}_s u = 0\} = \{0\}. \tag{24}$$

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

Proof of Lemma 3.3. The fact that $(\bar{y}^{[1]}, \bar{y}^{[2]}) \in \mathbb{Z}^k \cap \text{int } Y$ implies $\bar{y}^{[1]} \in \mathbb{Z}^p \cap \text{int } Y^{[1]}$ follows directly from the definition of $Y^{[1]}$. Suppose that $\bar{y}^{[1]} \in \mathbb{Z}^p \cap \text{int } Y^{[1]}$. Since $\bar{y}^{[1]}$ is an interior point of $Y^{[1]}$, and $Y^{[1]}$ is a projection of the convex full-dimensional set Y, there exists a real vector $\xi \in \mathbb{R}^{k-p}$ such that $(\bar{y}^{[1]}, \xi) \in \text{int } Y$. Hence there is a positive ϵ such that the open box $\mathcal{B} = \{\ (y^{[1]}, y^{[2]})\ :\ \mid y^{[1]} - \bar{y}^{[1]} \mid < \epsilon,\ \ \mid y^{[2]} - \xi \mid < \epsilon\ \}$ belongs to Y. In view of (24), Kronecker's theorem guarantees the existence of nonnegative scalars $\lambda_1, \ldots, \lambda_s$ such that $\|\xi + \sum_{i=1}^{s} \lambda_i \bar{\beta}_i\ \| < \epsilon$. Since the vectors $\beta_1, \ldots, \beta_s$ in (23) are recessive 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 $\mathbb{Z}^k \cap \text{int } Y \neq \emptyset$. Then $\Phi^{[1]}(y^{[1]})$ has an interior integral solution $\bar{y}^{[1]}$. The binary length of $\bar{y}^{[1]}$ can be bounded by applying the induction hypothesis (9) 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 $\bar{y}^{[1]} \in \text{int } Y^{[1]}$, it follows that $Y^{[2]}$ is convex and full-dimensional. By Lemma 3.3, $\mathbb{Z}^{k-p} \cap \text{int } Y^{[2]} \neq \emptyset$. Hence we can use the induction hypothesis (9) in $k - p$ dimensions to bound the bitlength of an interior integral solution $\bar{y}^{[2]}$ of $\Phi^{[2]}(y^{[2]})$. This yields the following bound

$$\log |(\bar{y}^{[1]}, \bar{y}^{[2]})| = ld^{\ cp^3(n+k)+c(k-p)^3(n+k-p)+O(sk(n+\log s))},$$

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 (20).) It is easy to see that the inclusions

$\bar{y}^{[i]} \in \text{int } Y^{[i]}$, $i = 1, 2$, guarantee that $(\bar{y}^{[1]}, \bar{y}^{[2]}) \in \text{int } Y$. To obtain the required bound (9) in k dimensions it remains to show that if $k \geq 2$, then

$$cp^3(n+k) + c(k-p)^3(n+k-p) + sk(n + \log s) \leq ck^3(n+k) \tag{25}$$

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

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

Hence (25) holds for $c \geq 2/3$.

(ii) Suppose that $\mathbb{Z}^k \cap \text{int } Y = \emptyset$. By Lemma 3.3, $\mathbb{Z}^p \cap \text{int } Y^{[1]} = \emptyset$. 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 (10) with

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

By (21),

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

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 (11) and completes the proof of Theorem 3.1. □

Corollary 3.4 *Let $P(y)$ be a quantifier-free formula composed of polynomial predicates $g_i(y) \bigtriangleup_i 0$, where $g_i(y) \in \mathbb{Z}[y_1, \ldots, y_k]$ are polynomials of degree $d \geq 2$ with coefficients of bitlength 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*

$$Y \cap \mathbb{Z}^k \subseteq \{ y \in \mathbb{Z}^k \mid b_1 \leq ya \leq b_2 \}, \tag{26}$$

$$\log \max\{|a|, |b_1|, |b_2|\} = ld^{\,O(k^3)}. \tag{27}$$

Proof of Corollary 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, Corollary 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 $u \in \mathbb{R}^k$ 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

$$\begin{pmatrix} u^* \\ v^* \end{pmatrix} = \sum_{j=0}^{D-1} \theta^j \begin{pmatrix} u_j^* \\ v_j^* \end{pmatrix}, \quad \begin{pmatrix} u_j^* \\ v_j^* \end{pmatrix} \in \mathbb{Z}^{k+1}, \ \ j = 0, \ldots, D-1,$$

where θ is an algebraic integer of degree $D = d^{\,O(k^2)}$, 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 (26) and (27) with $a = u_j^*$ and $b_1 = b_2 = v_j^*$. $\square$

Corollary 3.5 *Let $P(y)$ satisfy the assumptions of Corollary 3.4, and let Y be the solution set for $P(y)$. If $Y \cap \mathbb{Z}^k \neq \emptyset$, then Y contains an integral point y such that*

$$\log|y| = ld^{\,ck^4}, \tag{28}$$

where $c > 0$ is an absolute constant.

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

$$Y \cap \{\ y \in \mathbb{Z}^k \mid ya = b\} \neq \emptyset, \tag{29}$$

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 over $\mathbb{Z}^{k-1}$ and T and t are integral $(k-1) \times k$ matrix and k-vector such that

$$\log\max\{|T|, |t|\} = ld^{\,O(k^3)}. \tag{30}$$

(See e.g. [15], Ch. 5.) Substituting $t + y'T$ for y into the original formula $P(y)$, we obtain a new quantifier-free formula formula $P'(y') = P(t + Ty')$ whose set of solutions is still convex. It is easy to see that the degree d', bitlength 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 (29), $P'(y')$

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. But then $\bar{y} = t + \bar{y}'T$ is an integral solution for $P(y)$ for which (30) yields

$$\log|\bar{y}| = ld^{c(k-1)^4+O(k^3)}.$$

This inductively proves (28). □

Proof of Theorem 1.1. By Proposition 2.1, any input formula (F) with $\omega \geq 1$ quantifiers can be transformed into an equivalent quantifier-free formula (QF) of degree $d_{QF} = d^{\Pi_{i=1}^{\omega} O(n_i)}$ and bitlength $l_{QF} = ld^{\ (k+1)\Pi_{i=1}^{\omega} O(n_i)}$. Substituting d_{QF} and l_{QF} for d and l in (28) results in the required bound (1) for (F). □

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 the theorem for quantifier-free formulae $P(y)$. Next, the theorem trivially holds for $k = 1$ (even without the convexity assumption). Finally, we can assume without loss of generality that the convex solution set of $P(y)$ is full-dimensional, for otherwise we can reduce the number of variables by using the arguments presented in the proof of Corollary 3.4.

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.

Let $\mathcal{QF}(m, d, l)$ be the class of bounded convex k-dimensional sets $Y \subset \mathbb{R}^k$ defined by quantifier-free formulae $P(y)$ with m polynomial relations of degree d and bitlength l.

Lemma 4.1 *Given a set $Y \in \mathcal{QF}(m, d, l)$, one can compute in $l^{O(1)}(md)^{O(k^3)}$-time a rational affine transformation that $(k+1)$-rounds Y. 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 [9]. Suppose that Y is defined by a quantifier-free formula $P(y)$. Then the non-empty set of all k-rounding affine transformations for Y can be defined 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 $\|(a', A') - (a, A)\|_2 \leq \epsilon$ for some exact solution (a, A) of

$R(a, A)$. Since the Hausdorff distance

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

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 $U_{1-\epsilon(r^*+1)} \subseteq a' + YA' \subseteq \bar{U}_{k+\epsilon(r^*+1)}$. By (12), $\log r^* = ld^{O(k)}$. Hence Y can be $(k+1)$-rounded by computing an ϵ-approximate solution for $R(a, A)$ with $-\log\epsilon = ld^{O(k)}$. 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 that an ϵ-approximate solution for an arbitrary formula (F) can be computed in $l^{O(1)}(md)^{O(k)\Pi_i O(n_i)} \log\log(3 + r/\epsilon)$-time, where r is an upper bound on the Euclidean norm of an exact solution (Renegar [14], Theorem 1.2). Applying this result to $R(a, A)$, the lemma follows. □

Remark 4.2 *In fact, any set $Y \in \mathcal{QF}(m, d, l)$ can be $(k+1)$-rounded in $l^{O(1)}(md)^{O(k)}$ time by the shallow-cut ellipsoid method [8], [15].*

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

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

Suppose that for each set $Y \in \mathcal{K}$ we can compute in polynomial time a rational affine transformation that ρ-rounds Y. Then Lenstra's polynomial-time algorithm can either solve problem P_k, or find a rational vector $a = (a_1, \ldots, a_k)^T \neq 0$ and an interval $[b, c]$ of length $\rho 2^{O(k)}$ such that

$$Y \cap \mathbb{Z}^k \subseteq Y_b \cup Y_{b+1} \cup \ldots \cup Y_c,$$

where $Y_i = Y \cap \{y \in \mathbb{R}^k \mid ya = i\}$. By Lemma 4.1, for $\mathcal{K} = \mathcal{QF}(m, d, l)$ this reduces problem P_k to $2^{O(k)}$ similarly structured $(k-1)$-dimensional problems each of which replaces the input set Y by the intersection of Y with a rational hyperplane ([1]; also see [12], [8], [15]). The recursive application of the algorithm leads to the following result:

Corollary 4.3 *In fixed dimension, the integer programming problem P_k can be solved in $(lmd)^{O(1)}$ time for any set $Y \in \mathcal{QF}(m, d, l)$.*

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 the formula $P_r(y) \doteq P(y) \wedge (|y| \leq r)$, where r is a constant such that $\log r = ld^{O(k^4)}$. This means that Theorem 1.2 follows from Corollary 4.3. □

References

[1] L. BABAI, *On Lovász' Lattice Reduction and the Nearest Lattice Point Problem*, Combinatorica 6(1986), pp. 1-13.

[2] B. BANK, T. KRICK, R. MANDEL and P. SOLERNO, *A Geometrical Bound for Integer Programming with Polynomial Constraints* (extended abstract), Fundamentals of Computation Theory (ed. by L. Budach), Lecture Notes in Comp. Sci., 529, Springer, Berlin, 1991, pp. 121-125.

[3] A.I. BARVINOK, *A Polynomial Time Algorithm for Counting Integral Points in Polyhedra when the Dimension Is Fixed*, Math. Oper. Res., 19(1994), pp. 769-779.

[4] S. BASU, R. POLLACK, and M.-R. ROY, *On the Combinatorial and Algebraic Complexity of Quantifier Elimination*, J. ACM, 43(1996), pp. 1002-1045.

[5] W.S. BROWN and J.F. TRAUB, *On Euclid's Algorithm and the Theory of Subresultants*, J. ACM, 18(1971), pp. 505-514.

[6] J.W.S. CASSELS, *An Introduction to Diophantine Approximation*, University Press, Cambridge, 1957.

[7] G.E. COLLINS, *Polynomial Reminder Sequences and Determinants*, Am. Math. Monthly, 73(1966), pp. 708-712.

[8] M. GRÖTSCHEL, L. LOVÁSZ, and A. SCHRIJVER, *Geometric Algorithms and Combinatorial Optimization*, Springer, 1988.

[9] F. JOHN, *Extremum Problems with Inequalities as Subsidiary Conditions*, in: Studies and Essays, presented to R. Courant on his 60th Birthday January 8th, 1948, Wiley Interscience, New York, pp. 187-204.

[10] L. KHACHIYAN, *Convexity and Complexity in Polynomial Programming*, Proceedings of the International Congress of Mathematicians, August 16-24, 1983, Warsaw, pp. 1569-1577.

[11] A.K. LENSTRA, H.W. LENSTRA, JR., and L. LOVÁSZ, *Factoring Polynomials with Rational Coefficients*, Math. Ann., 261(1982), pp. 515-534.

[12] H.W. LENSTRA, JR., *Integer Programming with a Fixed Number of Variables*, Math. Oper. Res., 8(1983), pp. 538-548.

[13] M. MIGNOTTE, *Some Useful Bounds*, Computer Algebra, Symbolic and Algebraic Computation (Second Edition, ed. by B. Buchberger, G.E. Collins, and R. Loos, in cooperation with R. Albrecht), Springer, Wien, 1982.

[14] J. RENEGAR, *On the Computational Complexity of Approximating Solutions for Real Algebraic Formulae*, SIAM J. on Computing, 21(1992), pp. 1008-1025.

[15] A. SCHRIJVER, *Theory of Linear and Integer Programming*, Wiley, 1986.