ABSTRACT OF THE DISSERTATION

On the Complexity of Real and Integer Semidefinite Programming

by Lorant Porkolab

Dissertation Director: Professor Leonid Khachiyan

We consider the general feasibility problem for semidefinite programming: Determine whether a given system of linear inequalities has a solution in the cone of symmetric positive semidefinite matrices. We give upper bounds on the size of real feasible solutions and obtain a strongly polynomial-time algorithm for testing the feasibility of semidefinite programs in fixed dimension whose required number of arithmetic operations grows linearly in the number of constraints. We also consider semidefinite systems in integral matrices and extend Lenstra's theorem on the polynomial-time solvability of linear integer programming in fixed dimension to integer semidefinite programming. In fact, we address the more general problem of computing an integral point in an arbitrary convex semi-algebraic set, and show that in fixed dimension this problem can be solved in polynomial time.

Acknowledgements

I would like to express my gratitude to my advisor Professor Leonid Khachiyan for his invaluable help and guidance during the course of this work. I am also grateful to Professors Farid Alizadeh, Vašek Chvátal, Michael D. Grigoriadis, and James Renegar for serving on my dissertation committee.

This work was supported in part by NSF Grants CCR-9208371, CCR-9208539, CCR-9501941, CCR-9618796, ONR Grants N00014-92-J-1375, N00014-96-1-0704, and a DIMACS Graduate Student Fellowship. (DIMACS is a cooperative project of Rutgers University, Princeton University, AT&T Labs, Bellcore, and Bell Labs. 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.)

Table of Contents

Chapter 1

Introduction

Recently, there has been substantial interest in semidefinite programming (SDP). Semidefinite programming can be regarded as an extension of linear programming in which the positive orthant is replaced by the cone of symmetric positive semidefinite matrices. Many convex optimization problems, e.g., linear and convex quadratically constrained quadratic programs, maximum eigenvalue and matrix norm minimization, and also the computation of extremal ellipsoids for polyhedral sets, can be cast as SDP [26]. Applications of semidefinite programming include system and control theory [6], statistics [12], [13], [33], [35], and combinatorial optimization [16], [14], [19], [15].

It is well known that approximately solving semidefinite programs with explicitly given bounds on the size of an optimal solution can be accomplished in polynomial time by interior-point methods [1], [26]. However, the complexity of the general SDP problem, and in particular the complexity of testing the feasibility of a given semidefinite program, remains an open fundamental problem of mathematical programming.

The first part of the thesis studies the computational complexity of the general feasibility problem for SDP over the reals: Determine whether a given system of linear inequalities has a real solution in the cone of positive semidefinite matrices. Since any system of convex quadratic inequalities can be written as a semidefinite program, there are feasible systems of linear inequalities all of whose solutions in the cone of positive semidefinite matrices are doubly-exponentially large in the dimension of the problem. In addition, unlike systems of linear inequalities, some infeasible semidefinite programs can be made feasible by arbitrarily small perturbations of the input. For these reasons, in contrast

to linear programming, the polynomial-time solvability of semidefinite programming cannot be derived from the ellipsoid or interior point methods. In fact, it is not even known whether for the standard bit model of computation, the problem of testing the feasibility of a given semidefinite program belongs to the complexity class NP. (For the real number model of computation this problem is known to be in NP $\cap$ coNP [28], but the question of polynomial-time solvability remains open.) Since the complexity status of the general feasibility problem seems to be a very difficult question, it is natural to ask what other known complexity results for linear programming can be extended to semidefinite programming.

A classical complexity result in linear programming is the linear-time solvability of linear programs in fixed dimension (Megiddo [24]). The first part of the dissertation presents an extension of this result to semidefinite programming for the bit model of computation. Specifically, we first give an upper bound on the minimum binary size of a feasible solution to a given semidefinite program with integral coefficients (and show that our bound it is not very far from best possible). Then we use the above bound and the decision methods for the first-order theory of the reals due to Renegar [29] and Basu, Pollack and Roy [5], along with Chazelle and Matoušek's [9] derandomized variant of Clarkson's algorithm [10] to prove the following result:

> *In fixed dimension, the feasibility of a given semidefinite program can be tested in a number of arithmetic operations which grows linearly in the number of constraints and does not depend on the binary size of the input program.*

Note that Megiddo's theorem also holds for the real number model of computation, whereas the question of extending the above complexity result to semidefinite programs with real coefficients remains open.

The second part of the thesis studies the complexity of SDP over the integers. In fact, it considers the more general problem of computing an integral point in an arbitrary convex semi-algebraic set (i.e., the solution set of an arbitrary first-order algebraic formula with free and quantified variables). By applying a quantitative version of Kronecker's

theorem on simultaneous Diophantine approximation, and some recent bounds [5] on the combinatorial and algebraic complexity of quantifier elimination methods for the first order theory of the reals, we first obtain an upper bound on the minimum binary size of an integral point contained in a given convex semi-algebraic set. Next we show that this bound implies the following generalization of the celebrated result of Lenstra [23] on the polynomial-time solvability of linear integer programming in fixed dimension:

> *For each fixed n, there exists a polynomial-time algorithm that, given a convex semi-algebraic set defined by a first-order formula with n free and quantified variables, checks whether the input set contains an integral point, and if so, computes one.*

In addition to linear integer programming, this readily implies the polynomial-time solvability of systems of convex and quasi-convex polynomial inequalities with any fixed number of integer variables ([20], [3]). It should be mentioned, however, that the above complexity result is more robust – it only uses the convexity of the solution set and does not require that each algebraic constraint be quasi-convex. In particular, it leads to the following corollary for integer semidefinite programming:

> *For each fixed n, there is a polynomial-time algorithm which finds an integral symmetric positive semidefinite $n \times n$ matrix satisfying a given system of linear inequalities, or decides that no such matrix exists.*

This corollary 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 SDP.

The thesis is organized as follows. In Chapter 2, we discuss some known complexity results from semi-algebraic geometry and prove upper bounds on feasible solutions and discrepancies of semidefinite programs. Next we present our complexity results for testing the feasibility of semidefinite programs over the reals. We close Chapter 2

by stating similar bounds and complexity results for some other standard formats of semidefinite programs. In Chapter 3, we briefly review a quantitative version of the classical theorem of Kronecker on simultaneous Diophantine approximation and derive some of its implications. We then prove our bounds on the size of integral points contained in convex semi-algebraic sets, and show the polynomial-time complexity of the related computational problem.

Chapter 2

Testing the Feasibility of Real Semidefinite Programs

2.1 Results

This chapter is concerned with the general *semidefinite feasibility problem*:

> *Given integral $n \times n$ symmetric matrices $A_1, \ldots, A_m$ and integers $b_1, \ldots, b_m$, determine whether there exists a real $n \times n$ symmetric matrix $X = (X_{ij})$ such that*
>
> $$A_i \cdot X \leq b_i, \quad i = 1, \ldots, m, \quad X \succeq 0, \tag{2.1}$$
>
> *where $A \cdot X = \mathrm{tr}(AX)$ denotes the standard inner product on the space of real symmetric matrices and the notation $(\cdot) \succeq 0$ indicates that $(\cdot)$ is a symmetric positive semidefinite matrix.*

We assume without loss of generality that $n \geq 2$, and denote by l the maximum binary length of the input coefficients. The main results of this chapter are the following:

Theorem 2.1.1

(i) *Any feasible system* (2.1) *has a solution X such that $\|X\|_2 = (\sum_{i,j=1}^{n} X_{ij}^2)^{1/2} \leq R$, where $\log R = ln^{O(\min\{m,n^2\})}$.*

(ii) *If the feasible set of* (2.1) *is bounded, then the above bound holds for any solution of* (2.1).

Theorem 2.1.2 *The feasibility of* (2.1) *can be tested in $mn^{O(\min\{m,n^2\})}$ arithmetic operations over $ln^{O(\min\{m,n^2\})}$-bit numbers.*

This complexity result implies that problem (2.1) can be solved in strongly polynomial time for any fixed number of variables or constraints, and that for $n = const$, the required number of arithmetic operations grows only linearly with m. Therefore, in the bit model of computation, Theorem 2.1.2 can be regarded as an extension of Megiddo's result [24] on the linear time solvability of linear programs in fixed dimension. Note also that in the bit model of computation, each arithmetic operation with $ln^{O(\min\{m,n^2\})}$-bit numbers can be replaced by $n^{O(\min\{m,n^2\})}$ operations with l-bit numbers. For this reason, the above complexity bound on arithmetic operations also applies to l-bit numbers.

In Section 2.2 we review some bounds and algorithmic results from semi-algebraic geometry and state some useful inequalities related to univariate polynomials. We prove Theorems 2.1.1 and 2.1.2 in Sections 2.3 and 2.5, respectively. To show that the bounds of Theorem 2.1.1 are not very far from best possible, we give examples of feasible systems (2.1) all of whose solutions have Euclidean norm at least R, where $\log R = l2^{\min\{m,n\}/2}$. In addition, we present similar bounds on the discrepancy of infeasible semidefinite systems. We close the chapter by discussing analogous results for other formats of semidefinite programs.

2.2 Preliminaries: Algorithmic Semi-algebraic Geometry

In this section we introduce some notation and record a few auxiliary propositions, which are used in Chapters 2 and 3.

2.2.1 Notation

Let S_n denote the space of symmetric $n \times n$ real matrices. Any matrix in S_n can thus be regarded as a vector in $\mathbb{R}^{n(n+1)/2}$.

For a given matrix $X \in S_n$, $\|X\|_2 = (\sum_{i,j=1}^n X_{ij}^2)^{1/2}$ is the Frobenius norm of X, and $\lambda_1(X) \geq \ldots \geq \lambda_n(X)$ denote the (real) eigenvalues of X. We write $X \succ 0$ if $\lambda_n(X) > 0$, i.e., if X is positive definite.

Let $C = \{X \in S_n \mid X \succeq 0\}$ be the cone of symmetric positive semidefinite matrices. For a positive number R, we denote by C_R the compact set $C \cap \{X \in S_n \mid \mathrm{tr}(X) \leq R\}$.

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

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

the l_∞ and l_2-norms of ξ.

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 $|h| = \max |a_{i_1 \ldots i_k}|$ and $\deg(h) = \max\ (i_1 + \ldots + i_k)$ denote the height and degree of h.

In Chapter 3 we use the notation $\|\xi\| = \min\{\ |\xi - x| \ :\ x \in \mathbb{Z}^k\ \}$ for the l_∞-distance from ξ to the integral lattice $\mathbb{Z}^k$. Thus, 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.

2.2.2 Some Useful Inequalities and Identities

We shall need the following well-known inequalities.

Proposition 2.2.1 (see e.g. [25]) *Let $P(x) = a_0 x^p + a_1 x^{p-1} + \ldots + a_{p-1} x + a_p$ and $Q(x) = b_0 x^q + b_1 x^{q-1} + \ldots + a_{q-1} x + a_q$ be univariate polynomials with integer coefficients such that $a_0 \neq 0,\ b_0 \neq 0,\ p \geq 1$.*

Cauchy's inequality: *If α is a nonzero root of $P(x)$, then*

$$1/(1 + |P|) \ \leq\ |\alpha| \ \leq\ 1 + |P|. \tag{2.2}$$

Landau's inequality: *If $\alpha_1, \ldots, \alpha_p$ are the roots of $P(x)$, then*

$$|a_0| \prod_{j=1}^{p} \max\{1, |\alpha_j|\} \ \leq\ \|(a_0, \ldots, a_p)\|_2. \tag{2.3}$$

Mignotte's inequality: *If $Q(x)$ is a divisor of $P(x)$, then*

$$|b_0| + |b_1| + \ldots + |b_q| \ \leq\ \frac{|b_0|}{|a_0|}\ 2^q\ \|(a_0, \ldots, a_p)\|_2. \tag{2.4}$$

The following two identities hold for any $R \geq 0$:

$$\min\{A \cdot X \mid X \succeq 0,\ \mathrm{tr}(X) = R\} = R\lambda_n(A), \tag{2.5}$$

$$\min\{A \cdot X \mid X \succeq 0,\ \mathrm{tr}(X) \leq R\} = \min\{0, R\lambda_n(A)\}. \tag{2.6}$$

To show the first of these identities, note that

$$\begin{aligned} \min \quad & \{A \cdot X \mid X \succeq 0, \mathrm{tr}(X) = R\} \\ & = R\lambda_n(A) + \min\{(A - \lambda_n(A)I_n) \cdot X \mid X \succeq 0, \mathrm{tr}(X) = R\} \\ & = R\lambda_n(A), \end{aligned}$$

where the last equality follows from the fact that $A - \lambda_n(A)I_n$ is a symmetric positive semidefinite matrix whose minimum eigenvalue is zero. To prove the second identity, note that if $A \succeq 0$, then $\min\{A \cdot X \mid X \succeq 0, \mathrm{tr}(X) \leq R\} = 0$. Otherwise $\lambda_n(A) < 0$, which means that the minimum on the l.h.s. of (2.6) is negative and hence it is attained at a matrix X such that $\mathrm{tr}(X) = R$. Then (2.6) becomes a consequence of (2.5).

2.2.3 Decision Methods for the First-order Theory of the Reals

A *formula* $F(y)$ in the first-order theory of the reals is an expression of the form

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

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 polynomial predicates of the form

  $$g_i(y, x^{[1]}, \ldots, x^{[\omega]}) \triangle_i 0, \quad i = 1, \ldots, m,$$

  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.

We call d and l the *degree* and *bitlength* of (F). Note that the above formula is in prenex form: all quantifiers in (F) occur in front. Formulae without free variables are called *sentences*. We say that $y \in \mathbb{R}^k$ is a solution of (F) if the sentence obtained by substituting y into (F) is true.

The following complexity result, due to Renegar [29], deals with the decision problem for the first-order theory of the reals: Determine whether a sentence (F) is true or false.

Proposition 2.2.2 (cf. Theorem 1.1 of [29]) *There is an algorithm for the decision problem for the first-order theory of the reals that requires* $(md)^{\Pi_{i=1}^{\omega} O(n_i)}$ *arithmetic operations with* $l(md)^{\Pi_{i=1}^{\omega} O(n_i)}$*-bit numbers and* $(md)^{\Sigma_{i=1}^{\omega} O(n_i)}$ *evaluations of the Boolean function* $P(\cdot)$.

2.2.4 Computing Algebraic Solutions for First-Order Formulae

It is well known [34] that, over the reals, any first-order formula (F) is equivalent to a quantifier-free formula

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

where $h_{ij}(y) \in \mathbb{Z}[y_1, \ldots, y_k]$ are polynomials with integer coefficients and $\bigtriangleup_{ij} \in \{<, =\}$. The best currently known bounds on the degrees and binary length of the polynomials $h_{ij}(y)$ are due to Basu, Pollack, and Roy [5].

Proposition 2.2.3 (cf. Theorem 1 of [5]) *Each formula (F) can be transformed into an equivalent quantifier-free formula (QF) such that* $I \leq m^{(k+1)\Pi_{i=1}^{\omega}(n_i+1)} d^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}$, $J_i \leq m^{\Pi_{i=1}^{\omega}(n_i+1)} d^{\Pi_{i=1}^{\omega} O(n_i)}$, $\deg\ h_{ij}(y) \leq d^{\Pi_{i=1}^{\omega} O(n_i)}$, *and* $\log |h_{ij}| \leq l d^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}$. *The transformation (F)* $\longrightarrow$ *(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 [5] (see Section 3.1.3).

Proposition 2.2.4 *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 $h_j(y) \in \mathbb{Z}[y_1, \ldots, y_k]$ are polynomials of degree $D \geq 2$ with integer coefficients of binary length L. In $J^{k+1}D^{O(k)}$ arithmetic operations over $LD^{O(k)}$-bit numbers one can determine whether $Y \neq \emptyset$, 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 $\deg(G), \deg(Q), \deg(P_1), \ldots, \deg(P_k) \leq O(D)^k$, $\log\max\{(|G|, |Q|, |P_1|, \ldots, |P_k|\} \leq LD^{O(k)}$, and*

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

where

$$G(\theta) = 0, \quad (\text{sign}(G'(\theta)), \ldots, \text{sign}(G^{(\deg(G)-1)}(\theta)) = \sigma. \tag{2.7}$$

Note that conditions (2.7), known as Thom's encoding of θ, uniquely define an 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 [22]), 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, from Mignotte's inequality (2.4) it follows that $\log|g| \leq \log|G| + O(\deg(G))$. 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. [11], [7]), Propositions 2.2.3 and 2.2.4 readily imply the following result.

Corollary 2.2.5 *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 $q \neq 0$, and k polynomials $p_1(t), \ldots, p_k(t) \in \mathbb{Z}[t]$ such that*

$$y = \frac{1}{q}(p_1(\theta), \ldots, p_k(\theta)) \in Y, \quad g(\theta) = 0, \tag{2.8}$$

$$\deg(p_1), \ldots, \deg(p_k) < \deg(g) = d^{\,O(k)\Pi_{i=1}^{\omega} O(n_i)}, \tag{2.9}$$

$$\log\max\{|g|, |q|, |p_1|, \ldots, |p_k|\} = ld^{\,O(k)\Pi_{i=1}^{\omega} O(n_i)}. \tag{2.10}$$

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 2.2.6 *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 2.2.5 we can choose $q = 1$, and assume without loss of generality that θ is an algebraic integer:* lead.coeff $g(t) = 1$.

Corollary 2.2.5 along with Cauchy's inequality (2.2) implies the following bound.

Corollary 2.2.7 *If a formula $F(y)$ has a nonempty solution set, then it has a solution $y \in \mathbb{R}^k$ such that $\|y\|_2 \leq R$, where* $\log R = ld^{O(k)\Pi_{i=1}^{\omega} O(n_i)}$.

2.2.5 Inscribing a Box into a Full-dimensional Semi-algebraic Set

Proposition 2.2.8 below is a restatement of Theorems 5 and 6 of [5].

Proposition 2.2.8 *Let Y 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 integer coefficients of binary length L. If $Y \neq \emptyset$, 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 2.2.3 leads to the following corollary.

Corollary 2.2.9 *If the solution set Y of a formula $F(y)$ is full-dimensional, then there is a box $\mathcal{B} = \{z \in \mathbb{R}^k : |y - \alpha| < 1/R\} \subseteq Y$ such that $|\alpha| \leq R$ and* $\log R = ld^{\,O(k)\Pi_{i=1}^{\omega} O(n_i)}$.

2.3 Upper Bounds on Feasible Solutions of Semidefinite Programs

In this section we prove Theorem 2.1.1, and present some examples of feasible semidefinite programs all of whose solutions have doubly-exponentially large (Frobenius) norms.

Proof of Theorem 2.1.1. Suppose that system (2.1) is feasible, and let

$$\begin{aligned}\Omega_R &= \{X \in C \mid \mathrm{tr}(X) = R\},\\ \Delta_m &= \{y \in \mathbb{R}^m \mid y_i \geq 0,\ i = 1,\ldots,m,\ \ \textstyle\sum_{i=1}^m y_i = 1\},\\ \Theta(R) &= \min_{X\in\Omega_R} \max\{A_1 \cdot X - b_1, \ldots, A_m \cdot X - b_m\}.\end{aligned}$$

(Recall that C is the cone of symmetric positive semidefinite matrices of order n.) From von Neumann's saddlepoint theorem (see, e.g., [31]) and (2.5), it follows that for any $R \geq 0$,

$$\begin{aligned}\Theta(R) &= \min_{X\in\Omega_R} \max_{y\in\Delta_m} \ \ \textstyle\sum_{i=1}^m y_i(A_i \cdot X - b_i)\\ &= \max_{y\in\Delta_m} \min_{X\in\Omega_R} \ \ \{\ (\textstyle\sum_{i=1}^m y_i A_i) \cdot X - \sum_{i=1}^m y_i b_i\ \}\\ &= \max_{y\in\Delta_m} \{\ R\lambda_n(\textstyle\sum_{i=1}^m y_i A_i) - \sum_{i=1}^m y_i b_i\ \}.\end{aligned}$$

Consider the formula

$$\Phi(R) \doteq \forall y \in \Delta_m \ \ \{\ R\lambda_n(\sum_{i=1}^m y_i A_i) - \sum_{i=1}^m y_i b_i \ \leq\ 0 \ \wedge R \geq 0\},$$

which can be written in the standard form (F) as follows:

$$\begin{aligned}\forall y \in \mathbb{R}^m\ \exists \lambda \in \mathbb{R} \ \ \{\ \{\ [\ y_1 \geq 0, \ldots, y_m \geq 0,\ \ \textstyle\sum_{i=1}^m y_i = 1] \Longrightarrow\\ [\ (\ \det(\textstyle\sum_{i=1}^m y_i A_i - \lambda I_n) = 0\ )\ \wedge\\ (R\lambda - \textstyle\sum_{i=1}^m y_i b_i\ \leq 0\ )\ ]\ \}\ \wedge\ (R \geq 0)\}.\end{aligned}$$

It is easy to see that for any $R \in \mathbb{R}$, the following statements are equivalent:

- (2.1) has a feasible solution in Ω_R;
- $\Theta(R) \leq 0$;
- R satisfies $\Phi(R)$.

Since (2.1) is feasible, there is a nonnegative R that satisfies $\Phi(R)$. Note that $\Phi(R)$ is a standard formula (F) of degree at most n with $k = 1$ free and $n_1 = m$, $n_2 = 1$ quantified variables, respectively. Since $\det(\sum_{i=1}^m y_i A_i - \lambda I_n)$ contains $n!$ products of linear forms in $m+1$ variables with integer coefficients of binary size at most l, $\Phi(R)$ has bitlength at most $n(l + \log(nm) + 1)$. Now from Proposition 2.2.7 it follows that $\Phi(R)$ can be satisfied by a positive R such that

$$\log R = n(l + \log(nm) + 1)n^{O(m)} = ln^{O(m)}. \tag{2.11}$$

The property that (2.1) has a feasible solution in Ω_R can also be expressed by the formula

$$\begin{aligned} \exists X \in S_n \ \ \forall \lambda \in \mathbb{R} \quad \{ \ \ & \textstyle\bigwedge_{i=1}^{m} \ (A_i \cdot X \ \leq \ b_i) \ \wedge \ (I_n \cdot X = R) \wedge \\ & \wedge \ \ [\ (\ \det(X - \lambda I_n) \neq 0 \ ) \ \vee \ (\lambda \geq 0) \ ] \ \} \end{aligned} \tag{2.12}$$

of degree at most n with $k = 1$ free and $n_1 = O(n^2)$, $n_2 = 1$ quantified variables. The bitlength of this formula is l, since the height of the characteristic polynomial $\det(X - \lambda I_n)$ is 1. After replacing $\Phi(R)$ by (2.12) in the above argument, we conclude by Proposition 2.2.7 that there is a positive R such that (2.1) has a feasible solution X with $\mathrm{tr}(X) = R$, where

$$\log R = l n^{O(n^2)}. \tag{2.13}$$

Since $\|X\|_2 = (\sum_{i,j=1}^{n} X_{ij}^2)^{1/2} \leq \mathrm{tr}(X)$, part (i) of the theorem follows from (2.11) and (2.13).

To show part (ii), consider the formula $\Phi'(R) \doteq \forall R' \in \mathbb{R} \ \ \{ \ \Phi(R') \Longrightarrow (R' \leq R) \ \}$. Note that in prenex form $\Phi'(R)$ can be written as

$$\begin{aligned} \forall R' \in \mathbb{R} \ \exists y \in \mathbb{R}^m \quad \forall \lambda \in \mathbb{R} \ \{\{ \ & [\ y_1 \geq 0, \ldots, y_m \geq 0, \ \textstyle\sum_{i=1}^{m} y_i = 1] \wedge \\ & [\ (\ \det(\textstyle\sum_{i=1}^{m} y_i A_i - \lambda I_n) \neq 0 \ ) \ \ \vee \\ & (R'\lambda - \textstyle\sum_{i=1}^{m} y_i b_i \ > 0 \ ) \ ] \ \} \vee (0 \leq R' \leq R)\}, \end{aligned}$$

and that a positive number R satisfies $\Phi'(R)$ if and only if

$$R \geq \max\{\mathrm{tr}(X) \ \mid \ X \text{ feasible for (2.1)}\}.$$

Hence, we can apply Proposition 2.2.7 to $\Phi'(R)$ to conclude that, similar to (2.11), $\log R = l n^{O(m)}$. It remains to show that m can be replaced by $\min\{m, n^2\}$. To this end, note that if the solution set of (2.1) is bounded, then there exists a system $A_i \cdot X \leq b_i, \ \ i \in I, \ \ X \succeq 0$ of $I \leq n(n+1)/2$ inequalities whose solution set is still bounded. This is because the solution set of (2.1) is bounded if and only if the recessive cone of (2.1) is trivial, i.e.,

$$C \cap_{i=1}^{m} H_i = \{0\}, \tag{2.14}$$

where H_i is the halfspace $\{X \in S_n \mid A_i \cdot X \leq 0\}$. Let $\Omega_1 = \{X \in S_n \mid X \succeq 0,\ \mathrm{tr}(X) = 1\}$, then (2.14) is equivalent to the emptiness of the intersection of the $m+1$ convex sets $\Omega_1, H_1, \ldots, H_m \subset \mathbb{R}^{n(n+1)/2}$. By Helly's theorem (see, e.g., [31]) there exists a system of at most $1 + n(n+1)/2$ sets from $\Omega_1, H_1, \ldots, H_m$ whose intersection is still empty. Since any such system must contain Ω_1, the claim follows. □

Remark 2.3.1 *The bounds of Theorems 2.1.1 apply to any mixed system of strict and/or nonstrict inequalities*

$$\begin{aligned} A_i \cdot X &\leq b_i, \quad i = 1, \ldots, k, \\ A_i \cdot X &< b_i, \quad i = k+1, \ldots, m, \\ X &\succeq 0,\ X \succ_L 0, \end{aligned} \tag{2.15}$$

where L is a linear subspace in $\mathbb{R}^n$, and the constraint $X \succ_L 0$ means that X is positive definite on L.

This fact follows from the observation that for any $t \in (0,1)$, and any solutions X_1 and X_2 of systems (2.15) and (2.1), respectively, the convex combination $tX_1 + (1-t)X_2$ satisfies (2.15).

We close this section with an example of feasible systems (2.1) all of whose solutions are doubly-exponentially large in n.

Example 2.3.2 *Let n be a positive even integer. Consider $n \times n$ symmetric positive semidefinite matrices $X = (X_{ij})$ satisfying the system of linear equations:*

$$\begin{aligned} &X_{11} = 1, \quad X_{12} = 2^l, \\ &X_{kk} = 1, \quad X_{k,k+1} = X_{k-1,k-1}, \qquad \text{for } \ k = 3, 5, \ldots, n-1. \end{aligned}$$

It is easy to check that this instance of (2.1) is feasible and $\log X_{n,n} \geq l2^{n/2}$ for any of its solutions.

2.4 Lower Bounds on Discrepancies of Infeasible Systems

Let $R = R(n, m, l)$ be the bound of Theorem 2.1.1, and let

$$C_R = \{X \in S_n \mid X \succeq 0, \quad \mathrm{tr}(X) \leq R\}.$$

The *discrepancy* of (2.1) is defined as the optimal value of the convex programming problem:

$$\theta^* = \min\{\, \theta \mid A_i \cdot X \leq b_i + \theta, \quad i \in M = \{1, \ldots, m\}, \quad X \in C_R\}. \tag{2.16}$$

Note that because of the compactness of C_R, the minimum in (2.16) is always attained, and $\theta^* \leq 0$ if and only if system (2.1) is feasible.

Remark 2.4.1 *There exist infeasible systems* (2.1) *such that*

$$\inf\{\, \theta \mid A_i \cdot X \leq b_i + \theta, \quad i \in M, \quad X \succeq 0\} = 0.$$

For instance, this is true for the system of linear inequalities $X_{11} \leq 0, \quad X_{12} \leq -1$, *where* $X = (X_{ij})$ *is a symmetric positive semidefinite matrix of order* 2.

Theorem 2.4.2 *If* (2.1) *is infeasible, then* $-\log \theta^* = ln^{O(\min\{m, n^2\})}$.

Although Theorem 2.4.2 can be proved analogously to Theorem 2.1.1, it is convenient to postpone its proof until Section 2.5.

We close this section with an example of infeasible systems (2.1) whose discrepancies are doubly exponentially small.

Example 2.4.3 *Let* n *be even, and consider* $n \times n$ *symmetric positive semidefinite matrices* X *satisfying the equations:*

$$\begin{aligned}
&X_{11} - 2^l X_{12} = 0, \quad X_{22} - 2^l X_{34} = 0, \\
&X_{kk} - X_{12} = 0, \quad \textit{for} \quad k = 3, 5, \ldots, n-3, \\
&X_{kk} - X_{k+1,k+2} = 0, \quad \textit{for} \quad k = 4, 6, \ldots, n-4, \\
&X_{n-2,n-2} + X_{n-1,n-1} = 0, \quad X_{nn} - X_{12} = -1.
\end{aligned}$$

It is easy to check that this instance of (2.1) *is infeasible and* $-\log \theta^* \geq l 2^{n/2}$.

2.5 Linear-time Algorithm in Fixed Dimension

By Theorems 2.1.1 and 2.4.2, the feasibility of (2.1) can be determined by computing the optimal value θ^* of program (2.16) to an absolute accuracy of ϵ, where $\log(1/\epsilon) = ln^{O(\min\{m,n^2\})}$. This convex programming problem can be solved in $O(n^4 \log(2^l nR/\epsilon))$ iterations of the ellipsoid method (see, e.g., [17]), where each iteration requires $O(n^2(m+n))$ arithmetic operations over $\log(2^l nR/\epsilon)$-bit numbers. Hence, we obtain an upper bound of $lmn^{O(\min\{m,n^2\})}$ operations with $ln^{O(\min\{m,n^2\})}$-bit numbers for testing the feasibility of (2.1). Theorem 2.1.2 improves this bound on arithmetic operations by a factor of l.

Proof of Theorem 2.1.2. We start with a weaker result.

Lemma 2.5.1 *The feasibility of* (2.1) *can be tested in* $(mn)^{O(\min\{m,n^2\})}$ *arithmetic operations over* $l(mn)^{O(\min\{m,n^2\})}$*-bit numbers.*

Proof. The sentence

$$\begin{aligned} \exists X \in S_n \;\; \forall \lambda \in \mathbb{R} \; \{ \;\; & \textstyle\bigwedge_{i=1}^m \; (A_i \cdot X \;\leq\; b_i) \;\; \wedge \\ & \wedge \;\; [\; (\;\; \det(X - \lambda I_n) \neq 0 \;\;) \;\; \vee \;\; (\lambda \geq 0) \;] \; \} \end{aligned} \tag{2.17}$$

states that (2.1) is feasible. Since the characteristic polynomial $\det(X - \lambda I_n) \in \mathbb{Z}[X, \lambda]$ has height 1, from Proposition 2.2.2 it follows that the validity of the above sentence can be determined in $(mn)^{O(n^2)}$ operations over $l(mn)^{O(n^2)}$-bit numbers.

To finish the proof of the lemma, it remains to show that the feasibility of (2.1) can also be decided in $(mn)^{O(m)}$ operations with $l(mn)^{O(m)}$-bit numbers. Consider the sentence $\exists R \in \mathbb{R} \;\; \Phi(R)$, where $\Phi(R)$ is defined in the proof of Theorem 2.1.1. Observe that this sentence also states that (2.1) is feasible, and that it consists of $O(m)$ polynomial inequalities of degree at most n in $O(m)$ variables and has integer coefficients of binary size at most $n(l + \log(nm) + 1)$. Since $\det(\sum_{i=1}^m y_i A_i - \lambda I_n)$ can be evaluated in $\text{poly}(n, m)$ operations (or because all of its coefficients can be computed in $n^{O(m)}$ operations), the lemma follows from Proposition 2.2.2. □

We continue with the proof of Theorem 2.1.2. If m is bounded by a polynomial in n, the theorem follows from Lemma 2.5.1. We next show that for large m, determining

the feasibility of (2.1) via Clarkson's algorithm [10] requires an expected $mn^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers.

Given a set $I \subseteq M = \{1, \ldots, m\}$, let

$$\theta(I) = \min\{\ \theta \mid A_i \cdot X \leq b_i + \theta, \quad i \in I, \quad X \in C_R\}, \tag{2.18}$$

where $R = R(n, m, l)$ is the bound of Theorem 2.1.1 for the entire system (2.1). With this notation, we have $\theta^* = \theta(M)$. Denote by $X(I)$ the (unique) least norm solution of the system $A_i \cdot X \leq b_i + \theta(I),\ i \in I,\ X \in C_R$, and let $V(I) = \{i \in M \mid A_i \cdot X(I) > b_i + \theta(I)\}$ be the set of constraints violated by $X(I)$. A set $I \subseteq M$ is called a *basis*, if $V(J) \neq V(I)$ for any proper subset $J \subset I$. A basis J is a *basis for* I if $J \subseteq I$ and $V(J) = V(I)$. Any basis for M is called *optimal*. In particular, if S is an optimal basis, then

$$V(S) = V(M) = \emptyset, \quad \text{and consequently,} \quad \theta(S) = \theta(M) = \theta^*. \tag{2.19}$$

From Helly's theorem it follows that $D \doteq \max\{\ |I| \mid I \text{ a basis}\} \leq n(n+1)/2$. Given an optimal basis S, we can apply Lemma 2.5.1 to $A_i \cdot X \leq b_i,\ i \in S,\ X \succeq 0$ and determine the feasibility of the original system (2.1) in $n^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers. Clarkson's algorithm [10] finds an optimal basis by performing expected $N = O(Dm + D^3\sqrt{m \log m} \log m) \leq m\text{poly}(n)$ *violation tests*. Each of these tests checks whether $j \in V(I)$ for a sample set I of cardinality $O(D^2 \log D)$ and an index $j \in M \setminus I$.[1] Note that the inclusion $j \in V(I)$ can be written as the sentence

$$\begin{aligned} V_{I,j} \doteq \forall X, X' \in S_n \quad \forall \theta, \theta' \in \mathbb{R}\ \{\ \{\ (X, X' \succeq 0)\ \wedge\ S_I(X, \theta)\ \wedge \\ [\ S_I(X', \theta')\ \Longrightarrow\ (\theta \leq \theta')\ ]\ \wedge\ [\ S_I(X', \theta)\ \Longrightarrow \\ (\|X\|_2^2 \leq \|X'\|_2^2)\ ]\ \}\ \Longrightarrow\ (A_j \cdot X > b_j + \theta)\ \}, \end{aligned}$$

where $S_I(X, \theta)$ denotes the quantifier free formula

$$\{\ \bigwedge_{i \in I}\ (A_i \cdot X\ \leq\ b_i + \theta)\ \wedge\ (\|X\|_2^2 \leq R^2)\ \}.$$

[1] In fact, by using the arguments of Section 4 in [10], it can be verified [21] that the above bounds on the number of violation tests and the size of sample sets are valid for computing an optimal basis for any mapping $V : 2^M \to 2^M$ that satisfies the following two conditions: (i) $V(I) \subseteq M \setminus I$ and (ii) $V(I \cup \{j\}) = V(I)$ for any $j \in M \setminus V(I)$.

The positive semidefiniteness of X can be expressed by the formula $\forall\lambda \in \mathbb{R}\ \ C(X,\lambda)$, where $C(X,\lambda) = \{\ (\ \det(X - \lambda I_n) \neq 0\ )\ \vee\ (\lambda \geq 0)\ \}$. Therefore $V_{I,j}$ is equivalent to the following sentence:

$$\forall (X, X', \theta, \theta') \in \mathbb{R}^{n(n+1)+2} \quad \exists(\lambda, \lambda') \in \mathbb{R}^2\ \ \{\ \{C(X,\lambda)\ \wedge\ C(X',\lambda')\ \wedge$$
$$S_I(X,\theta)\ \wedge\ [\ S_I(X',\theta')\implies(\theta \leq \theta')\ ]\ \wedge\ [\ S_I(X',\theta)$$
$$\implies (\|X\|_2^2 \leq \|X'\|_2^2)\ ]\ \}\ \implies\ (A_j \cdot X > b_j + \theta)\ \}.$$

Each violation test can thus be represented by a sentence in prenex form with $O(|I|)\ \leq\ \text{poly}(n)$ polynomial inequalities of degree n in $O(n^2)$ variables. Note also that the coefficients of these polynomial inequalities are integers of binary length at most $\max\{l, \log R\} = ln^{O(\min\{m,n^2\})}$. Now from Proposition 2.2.2 it follows that each violation test can be accomplished in $n^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers. But the expected number of violation tests is bounded by $m\text{poly}(n)$. Hence we conclude that for all n and m, testing the feasibility of (2.1) requires expected $mn^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers.

Chazelle and Matoušek [9] derandomized Clarkson's algorithm for a wide subclass of *LP-type problems*, which includes linear programming and the problem of computing the minimum volume circumscribed ellipsoid for a given m-point set in $\mathbb{R}^n$. An *LP-type problem* is defined to be a pair (M, w), where M is a finite set, and $w : 2^M \to \mathcal{W}$ is a function with values in a linearly ordered set $(\mathcal{W}, \leq)$, satisfying the following two conditions:

Axiom 1. (Monotonicity) For any $J \subseteq I \subseteq M$, $w(J) \leq w(I)$.

Axiom 2. (Locality) For any $J \subseteq I \subseteq M$ with $w(J) = w(I)$ and any $i \in M$, $w(I \cup \{i\}) > w(I)$ implies that $w(J \cup \{i\}) > w(J)$.

Given an LP-type problem and a set $I \subseteq M$, the set of violated constraints $V(I)$ is defined as follows: $V(I) = \{i \in M \mid w(I \cup \{i\}) > w(I)\}$.

Observe that the problem of computing $\theta^* = \theta(M)$ can be viewed as an LP-type problem for the mapping $I \mapsto (\theta(I), \|X(I)\|_2)$ with the lexicographic ordering on $\mathbb{R}^2$, and that in this case, the above two definitions of $V(I)$ are equivalent. The derandomization in [9] is based on an additional assumption which we state here in the following

stronger form: for any subset $I \subseteq M$, one can compute in $O(|I|)^{\tilde{D}}$ operations a set system $\mathcal{R}_I$ which includes all of the sets $I' \subseteq I$ such that $I' = V(J)$ for some $J \subseteq M$. Note that for the LP-type problem of computing θ^*, a constraint $A_j \cdot X \leq b_j + \theta$ is violated at a point $\bar{P} = (\bar{X}, \bar{\theta})$ if the bounding hyperplane $h_j : A_j \cdot X = b_j + \theta$ lies above the point $\bar{P}$, i.e. if h_j intersects the open vertical semiline emanating from $\bar{P}$ upwards. Therefore, in this case, for any given $I \subseteq M$ a set system $\mathcal{R}_I$ satisfying the above requirement can be constructed in the following way. Consider the arrangement of the hyperplanes $A_i \cdot X = b_i + \theta,\ i \in I$, and compute a point in each of its cells. Then for all of the points check which inequalities of the system $A_i \cdot X \leq b_i + \theta,\ i \in I$, are satisfied, and output the sets of violated inequalities to obtain $\mathcal{R}_I$. It is easy to see that these steps can be carried out in

$$O(|I|)^{\bar{d}}(\bar{d}^3 + |I|\bar{d}) = O(|I|)^{O(\bar{d})}$$

operations, where $\bar{d} = n(n+1)/2+1$. Hence, the additional assumption is satisfied with some integer $\tilde{D} = O(n^2)$. Let $\mathcal{D} = \max\{D, \tilde{D}\}$. The derandomized algorithm of [9] computes an optimal basis of (2.16) by performing $m\mathcal{D}^{O(\mathcal{D})}$ operations and $m\text{poly}(\mathcal{D}) + \mathcal{D}^{O(\mathcal{D})}$ violation tests with subsets I of size at most $\mathcal{D}$. Since $\mathcal{D} = O(n^2)$ and each violation test can be accomplished in $n^{O(\min\{m,n^2\})}$ operations, we conclude that the derandomized algorithm still requires $mn^{O(\min\{m,n^2\})}$ operations with $ln^{O(\min\{m,n^2\})}$-bit numbers. □

Corollary 2.5.2 *The complexity bounds of Theorem 2.1.2 apply to the problem of computing an optimal basis of* (2.16).

Theorem 2.5.3 *Given an optimal basis S of* (2.16)*, one can find Thom's encoding* (2.7) *of θ^* in $n^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers.*

Proof. Assume without loss of generality that the given basis S coincides with M. In particular, $m \leq n(n+1)/2$. From von Neumann's saddlepoint theorem and (2.6), it follows that for $R \geq 0$,

$$\begin{aligned}\theta^* &= \max_{y \in \Delta_m} \min_{X \in C_R} \ \{\ (\textstyle\sum_{i=1}^m y_i A_i) \cdot X - \sum_{i=1}^m y_i b_i\ \} \\ &= \max_{y \in \Delta_m} \{\ \min[\ 0,\ R\lambda_n(\textstyle\sum_{i=1}^m y_i A_i)\ ] - \sum_{i=1}^m y_i b_i\ \}.\end{aligned}$$

Consider the formula

$$\Lambda(\theta) \doteq \forall y \in \Delta_m \ \{ \ \min[\ 0, R\lambda_n(\sum_{i=1}^{m} y_i A_i)\ ] - \sum_{i=1}^{m} y_i(b_i + \theta) \ \leq \ 0 \ \},$$

where R is the bound of Theorem 2.1.1. This formula states that $\theta \geq \theta^*$, and it can be written as follows:

$$\begin{aligned} \forall y \in \mathbb{R}^m \ \exists \lambda \in \mathbb{R} \ \{ \quad & (y_1 \geq 0, \ldots, y_m \geq 0, \ \textstyle\sum_{i=1}^{m} y_i = 1) \Longrightarrow \\ & [\ (\ \det(\textstyle\sum_{i=1}^{m} y_i A_i - \lambda I_n) = 0\ ) \ \wedge \\ & (\ (\textstyle\sum_{i=1}^{m} y_i(b_i + \theta) \geq 0) \ \vee \ (R\lambda - \textstyle\sum_{i=1}^{m} y_i(b_i + \theta) \leq 0\ )\ )\ ]\ \}. \end{aligned}$$

Now the formula

$$\Lambda^*(\theta) \ \doteq \ \forall \theta' \in \mathbb{R} \ \{\ \Lambda(\theta) \ \wedge \ [\Lambda(\theta') \ \Longrightarrow \ (\theta \leq \theta')\ ]\ \}$$

defines θ^* in the sense that θ^* is the only real solution of $\Lambda^*(\theta)$. By consecutively applying Proposition 2.2.3 to $\Lambda(\theta)$ and $\Lambda^*(\theta)$, the latter formula can be transformed into a quantifier free formula $\Lambda^{**}(\theta)$. This requires $(mn)^{O(m)} \leq n^{O(\min\{m,n^2\})}$ operations with $\max\{l, \log R\}(mn)^{O(m)} \leq l n^{O(\min\{m,n^2\})}$-bit numbers. $\Lambda^{**}(\theta)$ is composed of at most $n^{O(\min\{m,n^2\})}$ systems of univariate polynomial relations, each of degree $n^{O(\min\{m,n^2\})}$ and bitlength $l n^{O(\min\{m,n^2\})}$. Since θ^* is the only solution of $\Lambda^{**}(\theta)$, by applying Proposition 2.2.4 to $\Lambda^{**}(\theta)$, one can find Thom's encoding of θ^* in $n^{O(\min\{m,n^2\})}$ operations with $l n^{O(\min\{m,n^2\})}$-bit numbers. □

It is known that an ϵ-approximate solution for an arbitrary formula (F) can be computed in $(md)^{O(k)\Pi_i O(n_i)} \log\log(3 + R/\epsilon)$ arithmetic operations with $l(md)^{O(k)\Pi_i O(n_i)}$-bit numbers and $(md)^{O(k)\Pi_i O(n_i)}$ evaluations of the Boolean function $P(\cdot)$, where R is an upper bound on the Euclidean norm of an exact solution (see Renegar [30], Theorem 1.2). Therefore we obtain the following bound:

Corollary 2.5.4 *Under the assumption of Theorem 2.5.3, θ^* can be approximated to an accuracy of $\varepsilon > 0$ in $n^{O(\min\{m,n^2\})}[\log l + \log\log(3 + 1/\varepsilon)]$ arithmetic operations.*

It should be mentioned that unlike the upper bound on arithmetic operations stated in Theorem 2.1.2, the above bound depends on l.

Theorem 2.5.3 immediately implies Theorem 2.4.2, whose proof was postponed in Section 2.4.

Proof of Theorem 2.4.2. Suppose that system (2.1) is infeasible. Then $\theta^* > 0$ and by Theorem 2.5.3, the positive algebraic number θ^* is a root of a nontrivial polynomial $h(x) \in \mathbb{Z}[x]$ with integer coefficients of binary length $ln^{O(\min\{m,n^2\})}$. Since Cauchy's inequality (2.2) implies that $\theta^* \geq 1/(1+|h|)$, the theorem follows. □

2.6 Concluding Remarks

Consider semidefinite programs of the form

$$Q(x) \doteq Q_0 + x_1 Q_1 + \ldots + x_m Q_m \succeq 0, \tag{2.20}$$

where $Q_0, Q_1, \ldots, Q_m$ are given integral $n \times n$ symmetric matrices, and $x = (x_1, \ldots, x_m)$ is the vector of real unknowns. Let l denote the maximum binary length of the input coefficients.

The proofs of the following results (Theorems 2.6.1, 2.6.3 and 2.6.5) are similar to those presented above, and they can be found in [27].

Theorem 2.6.1

(i) *Any feasible system* (2.20) *has a solution* $x \in \mathbb{R}^m$ *such that* $\|x\|_2 \leq R$, *where* $\log R = ln^{O(\min(m,n^2))}$.

(ii) *If the feasible set of* (2.20) *is bounded, then the above estimate holds for any solution of* (2.20).

Example 2.6.2 *For matrices* $A \in S_{n_1}$ *and* $B \in S_{n_2}$, *let* $A \oplus B \in S_{n_1+n_2}$ *be their direct sum, i.e.*

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

Let

$$Q_1(x) = \begin{bmatrix} 1 & 2^l \\ 2^l & x_1 \end{bmatrix} \quad \textit{and} \quad Q_k(x) = \begin{bmatrix} 1 & x_{k-1} \\ x_{k-1} & x_k \end{bmatrix}, \quad k = 2, \ldots, m.$$

Then $Q(x) = Q_1(x) \oplus Q_2(x) \oplus \ldots Q_m(x) \succeq 0$ *is a feasible instance of* (2.20)*, any solution of which satisfies* $\log\ x_m \geq l2^m$.

As before, the bounds of Theorem 2.6.1 and Example 2.6.2 also apply to any semidefinite system of the form $Q(x) \succeq 0,\ Q(x) \succ_L 0$, where L is a linear subspace of $\mathbb{R}^n$.

Let $R = R(n, m, l)$ be the bound of Theorem 2.6.1, and let $U_R = \{x \in \mathbb{R}^m \mid \|x\|_2 \leq R\}$ be the m-dimensional ball of radius R centered at the origin. The discrepancy of (2.20) is defined as the optimal value of the concave program:

$$\lambda^* = \max\{\lambda_n(Q_0 + x_1Q_1 + \ldots + x_mQ_m) \mid x = (x_1, \ldots, x_m) \in U_R\}. \tag{2.21}$$

Clearly, (2.20) is feasible if and only if $\lambda^* \geq 0$.

Theorem 2.6.3 *If* (2.20) *is infeasible, then* $-\log(-\lambda^*) = ln^{O(\min\{m,n^2\})}$.

Example 2.6.4 *For* $x = (x_1, \ldots, x_m) \in \mathbb{R}^m$*, let*

$$Q_1(x) = \begin{bmatrix} 2^l x_1 & x_1 \\ x_1 & 2^l x_2 \end{bmatrix}, \quad Q_m(x) = \begin{bmatrix} -x_m & 0 \\ 0 & x_1 - 1 \end{bmatrix},$$

$$\textit{and} \quad Q_k(x) = \begin{bmatrix} x_1 & x_k \\ x_k & x_{k+1} \end{bmatrix}, \quad k = 2, \ldots, m-1.$$

Then $Q(x) = Q_1(x) \oplus Q_2(x) \oplus \ldots Q_m(x) \succeq 0$ *is an infeasible instance of* (2.20)*, and it can be verified that* $-\log(-\lambda^*) \geq l2^{m-1}$.

Theorem 2.6.5 *The feasibility of* (2.20) *can be determined in* $O(mn^4) + n^{O(\min\{m,n^2\})}$ *operations with* $ln^{O(\min\{m,n^2\})}$*-bit numbers.*

Chapter 3

Computing Integral Points in Convex Semi-algebraic Sets

3.1 Results

Recall that a first-order formula $F(y)$ over the reals is 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

  $$g_i(y, x^{[1]}, \ldots, x^{[\omega]}) \triangle_i 0, \quad i = 1, \ldots, m,$$

  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.

Also recall that d and l are called the degree and bitlength of $F(y)$, respectively.

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

Theorem 3.1.1 *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 $|y| \leq R$, where* $\log R = ld^{\,O(k^4)\Pi_{i=1}^{\omega} O(n_i)}$.

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

Theorem 3.1.2 *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 3.1.2 is a generalization of the well-known theorem of Lenstra [23] 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 a fixed number of integer variables [20],[3]. Theorem 3.1.2, however, applies to a wider class of 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 $A \cdot X = \mathrm{tr}(AX)$ 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 3.1.3 *For each fixed n, there exists a polynomial-time algorithm which finds an integer symmetric positive semidefinite $n \times n$-matrix X satisfying a given system of linear inequalities $A_i \cdot X \leq b_i, \quad i = 1, \ldots, m$, 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 [4] 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 $[1, a]$).

This chapter is organized as follows. The next section reviews Kronecker's theorem on simultaneous Diophantine approximations. In Sections 3.3 and 3.4 we prove Theorems 3.1.1 and 3.1.2.

3.2 Kronecker's Theorem on Simultaneous Diophantine Approximations

Recall that $\|\xi\| = \min\{\ |\xi - x|\ :\ x \in \mathbb{Z}^k\ \}$ denotes the l_∞-distance from a real vector $\xi = (\xi_1, \ldots, \xi_k)$ to the integral lattice $\mathbb{Z}^k$.

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 $\|\alpha + \sum_{i=1}^s x_i\beta_i\| \le \epsilon$;*

(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 [8].) The fact that (i) implies (ii) is trivial. Proposition 3.2.1 below can be regarded as a quantitative version of the reverse implication.

Proposition 3.2.1 ([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*

$$\|\alpha + \sum_{i=1}^{s} x_i\beta_i\| \le \epsilon, \quad |x| \le X \tag{3.1}$$

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

$$\|\alpha u\| \le \gamma \max\{\ \epsilon|u|,\ X\|\beta_1 u\|, \ldots, X\|\beta_s u\|\ \} \tag{3.2}$$

for all $u = (u_1, \ldots, u_k)^T \in \mathbb{Z}^k$ with $\gamma = 2^{k-1}/[(k+s)!]^2$.

Since $\|\alpha u\| \le 1/2$, from Proposition 3.2.1 it follows that (3.1) can be satisfied for *any* α provided that the right-hand side of (3.2) 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 (3.1) 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

$$\|\alpha + \sum_{i=1}^s x_i\beta_i\| \leq \epsilon, \quad 0 \leq x_i \leq X = \frac{2}{\min\{\max_j \|\beta_j u\| : u \in B'_{1/\gamma\epsilon}\}}, \ i = 1, \ldots, s, \quad (3.3)$$

can always be satisfied by some integral x provided that the expression for X on the right-hand side of (3.3) is finite.

Corollary 3.2.2 *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*

$$\|\alpha + \sum_{i=1}^s \lambda_i\beta_i\| \leq \epsilon, \quad 0 \leq \lambda_i \leq \Lambda = \frac{2}{\min\{\max_j |\beta_j u| \ : \ u \in B'_{1/\gamma\epsilon}\}}, \ i = 1, \ldots, s. \quad (3.4)$$

Proof. First, 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 $\|\alpha + \tau\sum_{i=1}^s x_i\beta_i\| \leq \epsilon$ for 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. (3.3) and (3.4)). 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 3.2.3 *Let $\beta_1, \ldots, \beta_s \in \mathbb{R}^k$ satisfy the assumption of Corollary 3.2.2. Suppose that the components of $\beta_1, \ldots, \beta_s$ are algebraic integers represented in the form (2.8), i.e.:*

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_s \end{pmatrix} = \sum_{j=0}^{D-1} \theta^j B_j, \quad g(\theta) = 0, \quad (3.5)$$

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 3.2.2 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 $\beta_i u = 0$, $u = (u_1, \ldots, u_k)^T \in \mathbb{Z}^k$ is equivalent to the system of D Diophantine equations $B_0[i]u = \ldots = B_{D-1}[i]u = 0$, $u = (u_1, \ldots, u_k)^T \in \mathbb{Z}^k$, where $B_j[i]$ is the i-th row of the matrix B_j. This means that the assumption of Corollary 3.2.2 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 $\nu = \min\{\max_i |\beta_i u| \ : \ u \in B'_{1/\gamma\epsilon}\}$; then $\nu = |\beta_{i^*} u^*|$ for some $i^* \in \{1, \ldots, s\}$ and $u^* = (u_1^*, \ldots, u_k^*)^T \in B'_{1/\gamma\epsilon}$. By (3.5), $\nu = v(\theta)$, where $v(t) \in \mathbb{Z}[t]$ is a polynomial of height $|v| \leq k 2^L/(\gamma\epsilon)$. 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

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

Since $\theta_1, \ldots, \theta_D$ are the roots of the polynomial $g(t)$, by Landau's inequality (2.3)

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

Hence $|U| \leq (|g||v|D)^{O(D)}$. But $\nu = v(\theta)$ is a positive root of $U(t) \in \mathbb{Z}[t]$. By Cauchy's inequality (2.2) this implies that $\nu \geq 1/(1 + |U|)$. Consequently, $\log \Lambda = \log(2/\nu) = O(D[L + \log D + \log(k/(\gamma\epsilon))])$. □

3.3 Upper Bounds on Integral Points in Convex Semi-algebraic Sets

In this section we prove Theorem 3.1.1. We start with the following result.

Theorem 3.3.1 *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 $\mathbb{Z}^k \cap int\ Y \neq \emptyset$, then Y contains an interior integral point $\bar{y}$ such that*

$$\log|\bar{y}| = ld^{\,ck^3(n+k)}, \tag{3.6}$$

where $c > 0$ is an absolute constant[1]*;*

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

$$Y \subseteq \{\ y \in \mathbb{R}^k \mid b_1 \leq ya \leq b_2\}, \tag{3.7}$$

$$\log\max\{|a|, |b_1|, |b_2|\} = ld^{\,ck^2(n+k)}. \tag{3.8}$$

Proof of Theorem 3.3.1. 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 2.2.3 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 int $Y \cap \mathbb{Z} \neq \emptyset$, then $|\bar{y} - y^*| \leq 1$ for some $\bar{y} \in$ int $Y \cap \mathbb{Z}$, which gives (3.6). Otherwise the length of Y is at most 1, which implies (3.7) and (3.8).

For convenience, we separately consider another special case of Theorem 3.3.1.

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

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

[1] we assume that $\log 0 = -\infty$

The solution set of this formula is the interval $[R^*, +\infty)$, where $R^* = \sup\{\ |y|\ \ : y \in Y\} < +\infty$. By Proposition 2.2.3, R^* satisfies a univariate polynomial equation with integral coefficients of bitlength $ld^{O(k+n)}$. Hence

$$\log |y| = ld^{O(k+n)} \quad \text{for all} \quad y \in Y, \tag{3.9}$$

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 $\mathcal{L} = \textit{lin.hull } C$ 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 $\textit{lin.hull}\{\beta_1, \ldots, \beta_s\} = \mathcal{L}$.

Lemma 3.3.2 *The recessive cone* C *has an algebraic integer spanning set* $\beta_1, \ldots, \beta_s$ *of the form*

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_s \end{pmatrix} = \sum_{j=0}^{D-1} \theta^j B_j, \quad g(\theta) = 0, \tag{3.10}$$

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

$$D = d^{\,O(sk(n+\log s))}, \tag{3.11}$$

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

$$\log \max\{|g|, |B_0|, \ldots, |B_{D-1}|\} = ld^{\,O(sk(n+\log s))}. \tag{3.12}$$

Proof of Lemma 3.3.2. By Corollary 2.2.9, 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

$$\forall\, \lambda \in \mathbb{R}\ \{\ (\ \lambda < 0\ )\ \vee\ \Phi(p/q + \lambda y)\ \}. \tag{3.13}$$

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, (3.13) can be written as

$$(\forall\ \lambda \in \mathbb{R})\ (\exists\ x \in \mathbb{R}^n)\ \{\ (\ \lambda < 0\ )\ \vee\ P_*(\lambda,y,x)\ \}, \tag{3.14}$$

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 2.2.3, (3.14) 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 2.2.5 and Remark 2.2.6.

□

We continue with the proof of Theorem 3.3.1.

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 3.3.2,

$$\mathcal{M}_I = \{\ u \in \mathbb{Z}^k \mid \beta_1 u = \ldots = \beta_s u = 0\} = \{\ u \in \mathbb{Z}^k \mid Mu = 0\}, \tag{3.15}$$

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

$$\log|M| = ld^{\,O(sk(n+\log s))}. \tag{3.16}$$

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 3.2.3 with $D = d^{\,O(sk(n+\log s))}$ and $L = ld^{\,O(sk(n+\log s))}$. By Corollary 2.2.9, Y contains an open box $\mathcal{B} = \{y \in \mathbb{R}^k \ : \ |y - \alpha| < 1/R\}$ such that $|\alpha| \le R$ 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 3.2.3 with $\epsilon = (2R)^{-1}$ we conclude that there are nonnegative scalars $\lambda_1^*, \ldots, \lambda_s^*$ for which the conditions

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

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 (3.10) 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 (3.11) and (3.12) 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 the bound of (3.6).

Induction. Let $p = \dim \mathcal{M}_I \ge 1$. Then $p \in \{1, \ldots, k - s\}$, where $s = \dim\ C \ge 1$. By (3.15), $\mathcal{M}_I = \{\ u \in \mathbb{Z}^k \mid Mu = 0\ \}$ for some integral $(k - p) \times k$-matrix M of full row rank. The lattice $\mathcal{M}_I$ is invariant under all transformation $M \to VM$, where V is a nondegenerate rational matrix of order $k - p$. Next, for any unimodular matrix U of order k, the change of variables

$$y = y'U \tag{3.17}$$

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, (3.17) 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 $M' = VMU^{-T} = (0, I)$, 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. [32], Ch. 5), from ([25]) it follows that we may assume without loss of generality that

$$\log |U| = ld^{\,O(sk(n+\log s))}. \tag{3.18}$$

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

$$M = \begin{pmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \tag{3.19}$$

for the *original* formula $\Phi(y)$, and that the bitlength of $\Phi(y)$ has been increased to $ld^{\,O(sk(n+\log s))}$. By (3.19), $\mathcal{M}_I = (\mathbb{Z}^p, 0)$ and hence

$$\beta_i = (0, \bar{\beta}_i), \quad i = 1, \dots, s, \tag{3.20}$$

where the vectors $\bar{\beta}_i \in \mathbb{R}^{k-p}$ satisfy the assumption of Corollary 3.2.3:

$$\{\, u = (u_1, \dots, u_k)^T \in \mathbb{Z}^{k-p} \mid \bar{\beta}_1 u = \dots = \bar{\beta}_s u = 0\} = \{0\}. \tag{3.21}$$

Consider the partition $y = (y^{[1]}, y^{[2]})$, where $y^{[1]} = (y_1, \dots, y_p)$ and $y^{[2]} = (y_{p+1}, \dots, y_k)$. 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 3.3.3 *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 3.3.3. 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 $\mathcal{B} = \{ (y^{[1]}, y^{[2]}) \ : \ | \ y^{[1]} - \bar{y}^{[1]} \ | < \epsilon, \ \ | \ y^{[2]} - \xi \ | < \epsilon \ \}$ belongs to Y. In view of (3.21), 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 s vectors $\beta_1, \ldots, \beta_s$ in (3.20) 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 3.3.1 by induction.

(i) Suppose that $\mathbb{Z}^k \cap \text{int } Y \neq \emptyset$. This implies that $\Phi^{[1]}(y^{[1]})$ has an interior integral solution $\bar{y}^{[1]}$ whose binary length can be bounded by applying the induction hypothesis (3.6) 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 3.3.3, $\mathbb{Z}^{k-p} \cap \text{int } Y^{[2]} \neq \emptyset$. Hence we can use the induction hypothesis (3.6) 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 (3.17).) 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 (3.6) in k dimensions it remains to show that if $k \geq 2$, then

$$cp^3(n+k) + c(k-p)^3(n+k-p) + sk(n+\log s) \leq ck^3(n+k) \qquad (3.22)$$

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

$$cp^3(n+k) + c(k-p)^3(n+k-p) + sk(n+\log s) \;\le$$
$$c[p^3 + (k-p)^3](n+k) + k^2(n+\log k) \;\le\; [c(k-1)^3 + c + k^2](n+k).$$

Hence (3.22) holds for $c \ge 2/3$.

(ii) Suppose that $\mathbb{Z}^k \cap \text{ int } Y = \emptyset$. By Lemma 3.3.3, $\mathbb{Z}^p \cap \text{ int } Y^{[1]} = \emptyset$. Inductively applying part (ii) of the theorem to $\Phi^{[1]}(y^{[1]})$ we conclude that $Y^{[1]} \subseteq \{\, y^{[1]} \in \mathbb{R}^p \mid b_1 \le y^{[1]}a^{[1]} \le b_2\}$, 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 (3.7) with

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

By (3.18),

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

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

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

This shows (3.8) and completes the proof of Theorem 3.3.1. □

Corollary 3.3.4 *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 $d \ge 2$ with coefficients of bitlength l. Suppose that the set $Y = \{\, y \in \mathbb{R}^k \mid P(y)$ 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 $a \ne 0$ and integers b_1, b_2 such that*

$$Y \cap \mathbb{Z}^k \subseteq \{\ y \in \mathbb{Z}^k \mid b_1 \le ya \le b_2\ \}, \tag{3.23}$$

$$\log \max\{|a|, |b_1|, |b_2|\} = ld^{\,O(k^3)}. \tag{3.24}$$

Proof of Corollary 3.3.4. 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 3.3.4 is thus a special case of Theorem 3.3.1 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 $(u, v) \in \mathbb{R}^{k+1}$ satisfying 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 2.2.5 and Remark 2.2.6 it follows that $H(u, v)$ has a solution of the form

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

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 (3.23) and (3.24) with $a = u_j^*$ and $b_1 = b_2 = v_j^*$. □

Corollary 3.3.5 *Let $P(y)$ satisfy the assumptions of Corollary 3.3.4, 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*

$$\log |y| = ld^{\,ck^4}, \tag{3.25}$$

where $c > 0$ is an absolute constant.

Proof of Corollary 3.3.5. We prove the corollary by induction on k, the number of free variables. The case $k = 1$ is trivial. Suppose that $k \ge 2$. In view of Corollary 3.3.4,

we can assume without loss of generality that there exists an integral vector $a \neq 0$ and an integer b such that

$$Y \cap \{\ y \in \mathbb{Z}^k \mid ya = b\} \neq \emptyset \tag{3.26}$$

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

$$\log\max\{|T|, |t|\} = ld^{\,O(k^3)}. \tag{3.27}$$

(See e.g. [32], 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:

$$d' \leq d, \quad l' = ld^{\,O(k^3)}, \quad k' \leq k - 1. \tag{3.28}$$

Moreover, by (3.26), $P'(y')$ has an integer solution $\bar{y}'$. By the induction hypothesis, $\log|\bar{y}'|$ can be bounded by $l'(d')^{ck'^4}$. In view of (3.28) and since $k' \leq k - 1$, we obtain $\log|\bar{y}'| = ld^{c(k-1)^4 + O(k^3)}$, 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 (3.27) yields

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

This inductively proves (3.25). □

Proof of Theorem 3.1.1. By Proposition 2.2.3, any input formula (F) with $\omega \geq 1$ quantifiers can be transformed into an equivalent quantifier-free formula (QF) of degree $d_{QF} = d^{\prod_{i=1}^{\omega} O(n_i)}$ and bitlength $l_{QF} = ld^{\,(k+1)\prod_{i=1}^{\omega} O(n_i)}$. Substituting d_{QF} and l_{QF} for d and l in (3.25) results in the required bound for (F) stated in Theorem 3.1.1. □

3.4 Polynomial-time Algorithm in Fixed Dimension

In this section, we prove Theorem 3.1.2.

We start with a few simple observations. First, due to Proposition 2.2.3, it suffices to prove the theorem for quantifier-free formulae (QF). 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 the formula $P(y)$ is full-dimensional, for otherwise we can reduce the number of variables by using the arguments presented in the proof of Corollary 3.3.4.

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

$$y \rightarrow a + yA$$

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

Lemma 3.4.1 *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 of Lemma 3.4.1. It is well known that any bounded convex full-dimensional set in $\mathbb{R}^k$ can be k-rounded [18]. 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 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

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

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 (3.9), $\log R^* = ld^{O(k)}$. 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 2.2.9, 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 $R(a, A)$.

Since 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 (see Renegar [30], Theorem 1.2), the lemma follows. □

Remark 3.4.2 *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 [17], [32].*

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 $a \in \mathbb{R}^k$ 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 $Y_i = Y \cap \{y \in \mathbb{R}^k \mid ya = i\}$ (see [2]; and also [23], [17], [32]). By Lemma 3.4.1, 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. The recursive application of the algorithm leads to the following result:

Corollary 3.4.3 *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 3.1.1, 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 an appropriate constant such that $\log R = ld^{O(k^4)}$. This means that Theorem 3.1.2 follows from Corollary 3.4.3. $\square$

References

[1] F. Alizadeh. Interior point methods in semidefinite programming with applications to combinatorial optimization. *SIAM Journal on Optimization*, 5:13–51, 1995.

[2] L. Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.

[3] B. Bank, T. Krick, R Mandel, and P. Solerno. A geometrical bound for integer programming with polynomial constraints. In L. Budach, editor, *Fundamentals of Computation Theory, Lecture Notes in Computer Science*, volume 529, pages 121–125. Springer, Berlin, 1991.

[4] A.I. Barvinok. A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Mathematics of Operations Research*, 19:769–779, 1994.

[5] S. Basu, R. Pollack, and M.-R. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of ACM*, 43:1002–1045, 1996.

[6] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan. *Linear Matrix Inequalities in System and Control Theory.* SIAM, Philadelphia, 1994.

[7] W.S. Brown and J.F. Traub. On Euclid's algorithm and the theory of subresultants. *Journal of ACM*, 18:505–514, 1971.

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

[9] B. Chazelle and J. Matoušek. On linear-time deterministic algorithms for optimization problems in fixed dimension. *Journal of Algorithms*, 21(3):579–597, 1996.

[10] K.L. Clarkson. Las Vegas algorithms for linear and integer programming when the dimension is small. *Journal of ACM*, 42:488–499, 1995.

[11] G.E. Collins. Polynomial reminder sequences and determinants. *American Mathematical Monthly*, 73:708–712, 1966.

[12] R. Fletcher. A nonlinear programming problem in statistics (educational testing). *SIAM Journal on Scientific and Statistical Computing*, 2:257–267, 1981.

[13] R. Fletcher. Semidefinite matrix constraints in optimization. *SIAM Journal on Control and Optimization*, 23:493–513, 1985.

[14] A. Frieze and M. Jerrum. Improved approximation algorithms for MAX k-CUT and MAX BISECTION. *Algorithmica*, 18(1):67–81, 1997.

[15] M.X. Goemans. Semidefinite programming in combinatorial optimization. Preprint, March 1997.

[16] M.X. Goemans and D.P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of ACM*, 42:1115–1145, 1995.

[17] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer, Berlin, 1988.

[18] F. John. Extremum problems with inequalities as subsidiary conditions. In *Studies and Essays, presented to R. Courant on his 60th Birthday January 8th, 1948*, pages 187–204. Wiley Interscience, New York, 1948.

[19] D. Karger, R. Motwani, and M. Sudan. Approximate graph coloring by semidefinite programming. In *Proceedings of the 35th Symposium on the Foundation of Computer Science*, pages 2–13, 1994.

[20] L.G. Khachiyan. Convexity and complexity in polynomial programming. In *Proceedings of the International Congress of Mathematicians*, pages 1569–1577, Warszawa, August 16-24 1983.

[21] L.G. Khachiyan. Lecture notes. Department of Computer Science, Rutgers University, 1992.

[22] A.K. Lenstra, H.W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[23] H.W. Lenstra Jr. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8:538–548, 1983.

[24] N. Megiddo. Linear programming in linear time when the dimension is fixed. *Journal of ACM*, 31:114–127, 1984.

[25] M. Mignotte. Some useful bounds. In B. Buchberger, G.E. Collins, and R. Loos, editors, *Computer Algebra, Symbolic and Algebraic Computation*, pages 259–263. Springer, Wien, 1982.

[26] Y. Nesterov and A. Nemirovski. *Interior Point Polynomial Methods for Convex Programming: Theory and Applications*. SIAM, Philadelphia, 1994.

[27] L. Porkolab and L. Khachiyan. On the complexity of semidefinite programming. *Journal of Global Optimization*, 10(4):351–365, 1997.

[28] M.V. Ramana. An exact duality theory for semidefinite programming and its complexity implications. *Mathematical Programming*, 77(2):129–162, 1997.

[29] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. part i: Introduction; preliminaries; the geometry of semialgebraic sets; the decision problem for the existential theory of the reals. *Journal of Symbolic Computation*, 13:255–299, 1992.

[30] J. Renegar. On the computational complexity of approximating solutions for real algebraic formulae. *SIAM Journal on Computing*, 21:1008–1025, 1992.

[31] T.R. Rockafellar. *Convex Analysis*. Princeton University Press, NJ, 1970.

[32] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley, New York, 1986.

[33] A. Shapiro. Weighted minimum trace factor analysis. *Psychometrika*, 47:243–264, 1982.

[34] A. Tarski. *A Decision method for Elementary Algebra and Geometry*. University of California Press, 1951.

[35] G.A. Watson. Algorithms for minimum trace factor analysis. *SIAM Journal on Matrix Analysis and Applications*, 13:1039–1053, 1992.

Vita

Lorant Porkolab

1985 Graduated from Verseghy Ferenc High School, Szolnok, Hungary.

1986-87 Attended Technical University of Ilmenau, Germany.

1987-92 Attended University of Szeged, Hungary. Majored in Computer Science.

1992 M.S. in Computer Science, University of Szeged, Hungary.

1992-97 Graduate Work in Operations Research, Rutgers, The State University of New Jersey, New Brunswick, New Jersey.

1992-93 Fellow of Soros Foundation, Rutgers Center for Operations Research.

1993-96 Teaching Assistant, Rutgers University, New Brunswick.

1996-97 Research Assistant, Department of Computer Science and Rutgers Center for Operations Research.

1997 L. Porkolab and L. Khachiyan. On the Complexity of Semidefinite Programming. *Journal of Global Optimization*, Vol. 10, No. 4, 351-365, 1997.

L. Porkolab and L. Khachiyan. Testing the Feasibility of Semidefinite Programs. To appear in *Topics in Semidefinite and Interior-Point Methods*, Fields Institute Communications Series, AMS.

L. Khachiyan and L. Porkolab. Computing Integral Points in Convex Semialgebraic Sets. To appear in *Proc. of 38th IEEE Annual Symposium on the Foundations of Computer Science (FOCS '97)*.

1997 Ph.D. in Operations Research, Rutgers University.