Journal of Global Optimization **10:** 351–365, 1997.
© 1997 *Kluwer Academic Publishers. Printed in the Netherlands.*

On the Complexity of Semidefinite Programs[⋆]

LORANT PORKOLAB
RUTCOR, Rutgers University, P.O. Box 5062, New Brunswick, NJ 08903-5062, U.S.A. (email: porkolab@rutcor.rutgers.edu)

LEONID KHACHIYAN
Department of Computer Science, Rutgers University, New Brunswick, NJ 08903, U.S.A.

Abstract. We show that the feasibility of a system of m linear inequalities over the cone of symmetric positive semidefinite matrices of order n can be tested in $mn^{O(\min\{m,n^2\})}$ arithmetic operations with $ln^{O(\min\{m,n^2\})}$-bit numbers, where l is the maximum binary size of the input coefficients. We also show that any feasible system of dimension (m, n) has a solution $\mathbf{X}$ such that $\log \|\mathbf{X}\| \leq ln^{O(\min\{m,n^2\})}$.

Key words: Semidefinite programming, complexity, bounds on solutions.

1. Introduction

This paper is concerned with the general *semidefinite feasibility problem* $(\mathbf{F})$:

Given integral $n \times n$ symmetric matrices $\mathbf{A}_1, \ldots, \mathbf{A}_m$ and integers $b_1, \ldots, b_m$, determine whether there exists a real $n \times n$ symmetric matrix $\mathbf{X}$ such that

$$\mathbf{A}_i \cdot \mathbf{X} \leq b_i, \quad i = 1, \ldots, m, \quad \mathbf{X} \succeq 0, \tag{1}$$

where $\mathbf{A} \cdot \mathbf{X} = tr(\mathbf{AX})$ 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 also consider the following (polynomially equivalent) problem $(\mathbf{G})$:

Given integral $n \times n$ symmetric matrices $\mathbf{Q}_0, \mathbf{Q}_1, \ldots, \mathbf{Q}_m$, determine whether there are real numbers $x_1, \ldots, x_m$ such that

$$\mathbf{Q}_0 + \mathbf{x}_1\mathbf{Q}_1 + \cdots + \mathbf{x}_m\mathbf{Q}_m \succeq 0. \tag{2}$$

The complexity status of problems $(\mathbf{F})$ and $(\mathbf{G})$ is a fundamental open issue in the theory of semidefinite programming. For the standard bit model of computation, it is known [7] that either these problems belong to the complexity class $NP \cap coNP$, or they are not in $NP \cup coNP$. For the real number model of computation problems $(\mathbf{F})$ and $(\mathbf{G})$ are known to be in $NP \cap coNP$ [7], but the question of whether they can be solved in polynomial time remains open.

[⋆] Research supported by NSF grants CCR-9208371 and CCR-9208539, and ONR grant N00014-92-J.

We assume throughout the paper that $n \geq 2$, because for $n = 1$ the problems are trivial. The results of this paper are as follows. In Section 3, we obtain upper bounds on the norm of feasible solutions of (1) and (2). Specifically, we show that:

(i) Any feasible system (1) has a solution in the Euclidean ball $B = \{\mathbf{X} | \|\mathbf{X}\| \leq R\}$, where $\log R = ln^{O(\min\{m,n^2\})}$ and l is the maximum bitlength of the input coefficients. Moreover, the same bound applies to (2): any feasible system (2) has a solution $\mathbf{x}$ such that $\log \|\mathbf{x}\| = ln^{O(\min\{m,n^2\})}$.

If the solution sets of (1) or (2) are bounded, then the above bounds hold for any solution. In addition, we give examples of feasible systems (1) and (2) all of whose solutions have Euclidean norm at least R, where $\log R = l2^{\min\{m,n\}/2}$.

In Section 4, we state lower bounds on the discrepancy of infeasible systems (1) and (2):

(ii) If (1) is infeasible, then for any symmetric positive semidefinite matrix $\mathbf{X} \in B$, $-\log \max_{i=1,\ldots,m}\{\mathbf{A}_i \cdot \mathbf{X} - b_i\} = ln^{O(\min\{m,n^2\})}$. The corresponding result for an infeasible system (2) is that for any $\mathbf{x}$ that satisfies the upper bound of (i), the minimum eigenvalue λ_n of $\mathbf{Q}_0 + \mathbf{x}_1\mathbf{Q}_1 + \cdots + \mathbf{x}_m\mathbf{Q}_m$ is negative and $-\log(-\lambda_n) = ln^{O(\min\{m,n^2\})}$.

We also give examples of infeasible systems (1) and (2) for which the quantities $\log \max_{i=1,\ldots,m}\{\mathbf{A}_i \cdot \mathbf{X} - b_i\}$ and $\log(-\lambda_n(\mathbf{Q}_0 + \mathbf{x}_1\mathbf{Q}_1 + \cdots + \mathbf{x}_m\mathbf{Q}_m))$ do not exceed $-l2^{\min\{m,n\}/2}$.

We prove the bounds of (i) and (ii) by using some results of Renegar [9] on decision methods for the first order theory of the reals and an analogue of the fundamental theorem of linear inequalities for positive semidefinite matrices. These auxiliary results are briefly reviewed in Section 2.

In Section 5, we discuss the complexity of problems $(\mathbf{F})$ and $(\mathbf{G})$. Due to (i) and (ii), solving $(\mathbf{F})$ with the ellipsoid method requires $lmn^{O(\min\{m,n^2\})}$ arithmetic operations with $ln^{O(\min\{m,n^2\})}$-bit numbers. We use the decision method of Renegar [9] along with the derandomized version [2] of Clarkson's algorithm [3], [1] to improve this result as follows:

(iii) Problem $(\mathbf{F})$ can be solved in $mn^{O(\min\{m,n^2\})}$ arithmetic operations over $ln^{O(\min\{m,n^2\})}$-bit numbers.

In particular, $(\mathbf{F})$ can be solved in strongly polynomial time for any fixed number of variables or constraints. Note also that for $n = const$, the required number of arithmetic operations grows linearly with m.

In Section 5 we also argue that:

(iv) Problem $(\mathbf{G})$ can be solved in $O(mn^4) + n^{O(\min\{m,n^2\})}$ arithmetic operations over $ln^{O(\min\{m,n^2\})}$-bit numbers.

This extends the earlier result of Ramana [6] that for any fixed m the strict version $\mathbf{Q}_0 + \mathbf{x}_1\mathbf{Q}_1 + \cdots + \mathbf{X}_m\mathbf{Q}_m \succ 0$ of problem $(\mathbf{G})$ can be solved in polynomial time.

Note 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 bounds on the operations stated in (iii) and (iv) also apply to l-bit numbers.

Finally, in Section 6 we briefly discuss some extensions of (iii) and (iv) to semidefinite optimization problems.

2. Preliminaries

In this section we introduce some notation and record a few auxiliary propositions, which are used in Sections 3 and 5.

2.1. Notation

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

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

$\lambda_1(\mathbf{X}) \geq \cdots \geq \lambda_n(\mathbf{X})$ are the (real) eigenvalues of $\mathbf{X} \in S_n$. We write $\mathbf{X} \succ 0$ if $\lambda_n(\mathbf{X}) > 0$.

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

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

where:

- $\mathbf{y} = (y_1, \ldots, y_k) \in \mathbb{R}^k$ are free variables;
- each Q_i, $i = 1, \ldots, \omega$, is one of the quantifiers $\exists$ or $\forall$;
- $P(\mathbf{y}, \mathbf{x}^{[1]}, \ldots, \mathbf{x}^{[\omega]})$ is a quantifier free Boolean formula* with r “atomic predicates” of the form

  $$g_i(\mathbf{y}, \mathbf{x}^{[1]}, \ldots, \mathbf{x}^{[\omega]}) \Delta_i 0, i = 1, \ldots, r,$$

  where Δ_i is one of the “standard relations” $>$, $<$, $\geq$, $\leq$, $=$, $\neq$, and the g_i’s are real polynomials of degree at most $d \geq 2$.

Note that the above formula is in prenex form: all quantifiers in (SF) occur in front. Formulas without free variables are called sentences. We say that $\mathbf{y} \in \mathbb{R}^k$ is a solution of (SF) if the sentence obtained by substituting $\mathbf{y}$ into (SF) is true.

* In this paper, all formulae will be explicitly written using the standard connectives $\wedge$, $\vee$, and $\Longrightarrow$.

2.2. Auxiliary Propositions

PROPOSITION 2.1 (Renegar [8]). *If a formula (SF) has only integer coefficients, each of bit length at most B, then every connected component of the set of its solutions intersects the ball $\{\mathbf{y} \in \mathbb{R}^k \,|\, \|\mathbf{y}\| \leq R\}$, where R satisfies*

$$\log R \leq B(rd)^{2^{O(\omega)k \prod_i n_i}}.$$

A quantifier elimination method for the first-order theory of the reals constructs for any input formula (SF) an equivalent quantifier free formula.

PROPOSITION 2.2 (Renegar [9]). *There is an algorithm which, given a formula (SF), finds an equivalent quantifier free formula of the form*

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

where:

- $I \leq (rd)^{2^{O(\omega)k \prod_i n_i}}$,
- $J_i \leq (rd)^{2^{O(\omega)k \prod_i n_i}}$,
- *the degree of* $h_{ij}(\mathbf{y}) \leq (rd)^{2^{O(\omega)k \prod_i n_i}}$,
- Δ_{ij} *is one of the standard relations* $>, <, \geq, \leq, =, \neq$.

The algorithm requires $(rd)^{2^{O(\omega)k \prod_i n_i}}$ operations and $(rd)^{O(k+\sum_i n_i)}$ evaluations of the input formula. If the coefficients of the atomic polynomials g_i, $i = 1, \ldots, r$, are integers of bit length at most B, then the algorithm works with numbers of binary length

$$(B + k)(rd)^{2^{O(\omega)k \prod_i n_i}}.$$

This bound also holds for the binary length of the coefficients of the polynomials h_{ij}.

The following special case of the above result deals with the decision problem for the first-order theory of the reals: determine whether a sentence (SF) is true or false.

PROPOSITION 2.3 (Renegar [9]). *There is an algorithm for the decision problem of the first-order theory of the reals that requires*

$$(rd)^{2^{O(\omega)k \prod_i n_i}}$$

operations and $(rd)^{O(\sum_i n_i)}$ evaluations of the input formula. When restricted to sentences involving only polynomials with integer coefficients of bit length at most B, the procedure works with numbers of binary length $B(rd)^{2^{O(\omega)k \prod_i n_i}}$.

The inequality below is a well-known bound on nonzero roots of univariate polynomials (see, e.g. [5]).

PROPOSITION 2.4. *Let $p(x) = a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d$ be a univariate polynomial with integer coefficients, and let α be a nonzero root of $p(x)$. Then $|\alpha| \geq 1/(1+h)$, where $h = \max\{|a_0|, |a_1|, \ldots, |a_d|\}$ is the height of $p(x)$.*

We shall also need the following variant of the Fundamental Theorem of Linear Inequalities (see, e.g. [11]).

PROPOSITION 2.5. *Consider a system of linear inequalities*

$$\mathbf{a}_i^T\mathbf{x} \leq b_i, \quad i \in M = \{1, \ldots, m\},$$

where $\mathbf{a}_i \in \mathbb{R}^n$, $i \in M$, are non-zero vectors, $b_i \in \mathbb{R}$, $i \in M$, and let K be a convex set in $\mathbb{R}^n$. If $P \doteq K \cap \{\mathbf{x} \in \mathbb{R}^n \,|\, \mathbf{a}_i^T\mathbf{x} \leq b_i, i \in M\}$ is not empty, then there exists a subset $I \subseteq M$ such that:

$$\begin{array}{ll} (a) & |I| \leq \min\{m, n\}, \\ (b) & \emptyset \neq K \cap \{\mathbf{x} \in \mathbb{R}^n \,|\, \mathbf{a}_i^T\mathbf{x} = b_i, \quad i \in I\} \subseteq P. \end{array}$$

Finally, for any $R \geq 0$ we have:

$$\min\{\mathbf{A}\cdot\mathbf{X} |\, \mathbf{X} \succeq 0,\ \mathrm{tr}(\mathbf{X}) = R\} = R\lambda_n(\mathbf{A}), \tag{3}$$

$$\min\{\mathbf{A}\cdot\mathbf{X} |\, \mathbf{X} \succeq 0,\ \mathrm{tr}(\mathbf{X}) \leq R\} = \min\{0, R\lambda_n(\mathbf{A})\}. \tag{4}$$

To show the first of these identities, observe that

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

where the last equality follows from the fact that $\mathbf{A} - \lambda_n(\mathbf{A})\mathbf{I}_n$ is a symmetric positive semidefinite matrix whose minimum eigenvalue is zero. To see the second identity, note that if $\mathbf{A} \succeq 0$, then $\min\{\mathbf{A}\cdot\mathbf{X} |\, \mathbf{X} \succeq 0, \mathrm{tr}(\mathbf{X}) \leq R\} = 0$. Otherwise $\lambda_n(\mathbf{A}) < 0$, which means that the minimum on the l.h.s. of (4) is negative and hence it is attained at a matrix $\mathbf{X}$ such that $\mathrm{tr}(\mathbf{X}) = R$. Then (4) becomes a consequence of (3).

3. Upper Bounds on Feasible Solutions

THEOREM 3.1.

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

(ii) *Moreover, if the feasible set of (1) is bounded, then the above bound holds for any solution of (1).*

Proof. Suppose that system (1) is feasible, and let

$$\begin{aligned}\Omega_R &= \{\mathbf{X} \in C | \mathrm{tr}(\mathbf{X}) = R\},\\ \Delta_m &= \left\{\mathbf{y} \in \mathbb{R}^m | y_i \geq 0, i = 1, \ldots, m, \sum_{i=1}^m y_i = 1\right\},\\ \Theta(R) &= \min_{\mathbf{X}\in\Omega_R} \max\{\mathbf{A}_1 \cdot \mathbf{X} - b_1, \ldots, \mathbf{A}_m \cdot \mathbf{X} - b_m\}.\end{aligned}$$

(Recall that C is the cone of symmetric positive semidefinite matrices of order n.) From von Neumann's saddlepoint theorem (see, e.g., [10]) and (3), it follows that for any $R \geq 0$

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

Consider the formula

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

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

$$\begin{aligned}&\forall \mathbf{y} \in \mathbb{R}^m \quad \exists \lambda \in \mathbb{R} \Bigg\{ \Bigg\{ \left[y_1 \geq 0, \ldots, y_m \geq 0, \sum_{i=1}^m y_i = 1\right]\\ &\quad\Longrightarrow \left[\left(\det\left(\sum_{i=1}^m y_i \mathbf{A}_i - \lambda \mathbf{I}_n\right) = 0\right)\right.\\ &\quad\left.\wedge\left(R\lambda - \sum_{i=1}^m y_i b_i \leq 0\right)\right]\Bigg\} \wedge (R \geq 0)\Bigg\}.\end{aligned}$$

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

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

By our original assumption, (1) is feasible, and hence there is a non-negative R that satisfies $\Phi(R)$. Next, $\Phi(R)$ is a standard formula (SF) of degree at most $d = n$ with $k = 1$ free variable and $\omega = 2$ quantifiers. Furthermore, $\Phi(R)$ consists of $r = m + 4 = O(m)$ atomic polynomial inequalities in $m + 1 = O(m)$ variables. Since $\det(\sum_{i=1}^m y_i \mathbf{A}_i - \lambda \mathbf{I}_n)$ contains $n!$ products of linear forms in $m+1$ variables with integer coefficients of height at most 2^l, each coefficient in $\Phi(R)$ has binary length at most $b = n(l + \log(nm) + 1)$. Now from Proposition 2.1 it follows that $\Phi(R)$ can be satisfied by a positive number R such that

$$\log R = n(l + \log(nm) + 1)(nm)^{O(m)} = l(nm)^{O(m)}. \tag{5}$$

By Proposition 2.5, there is a set $I \subseteq M$ of size at most $n(n+1)/2$ such that the system

$$\mathbf{A}_i \cdot \mathbf{X} = b_i, \quad i \in I, \quad \mathbf{X} \succeq 0$$

is feasible, and any of its solutions solves the original system (1). For this reason, we can obtain a better bound on R by replacing m with $\min\{m, n^2\}$. Since $\|\mathbf{X}\| = (\sum_{i,j=1}^{n} \mathbf{X}_{ij}^2)^{1/2} \le \mathrm{tr}(\mathbf{X})$, part (i) of the theorem follows.

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

$$\begin{aligned}&\forall R' \in \mathbb{R} \quad \exists \mathbf{y} \in \mathbb{R}^m \quad \forall \lambda \in \mathbb{R}\Bigg\{\Bigg\{\Bigg[y_1 \ge 0, \ldots, y_m \ge 0, \sum_{i=1}^{m} y_i = 1\Bigg] \\ &\qquad \wedge \Bigg[\Bigg(\det\Bigg(\sum_{i=1}^{m} y_i \mathbf{A}_i - \lambda \mathbf{I}_n\Bigg) \ne 0\Bigg) \\ &\qquad \vee \Bigg(R'\lambda - \sum_{i=1}^{m} y_i b_i > 0\Bigg)\Bigg]\Bigg\} \vee (0 \le R' \le R)\Bigg\}.\end{aligned}$$

It is easy to see that $\Phi'(R)$ is satisfied if and only if

$$R \ge \max\{\mathrm{tr}(\mathbf{X}) | \mathbf{X} \text{ feasible for } (1)\}.$$

Hence, we can apply Proposition 2.1 to $\Phi'(R)$ to conclude that, similarly to (5), $\log\, R = l(nm)^{O(m)}$. It remains to show that m can be replaced by $\min\{m, n^2\}$. To this end, note that if the solution set of (1) is bounded, then there exists a system $\mathbf{A}_i \cdot \mathbf{X} \le b_i,\ i \in I, \mathbf{X} \succeq 0$ with at most $n(n+1)/2$ inequalities whose solution set is still bounded. This is because the solution set of (1) is bounded if and only if the recessive cone of (1) is trivial, i.e.,

$$C \cap_{i=1}^{m} H_i = \{0\}, \tag{6}$$

where H_i is the halfspace $\{\mathbf{X} \in S_n | \mathbf{A}_i \cdot \mathbf{X} \le 0\}$. Let $\Omega_1 = \{\mathbf{X} \in S_n | \mathbf{X} \succeq 0,\ \mathrm{tr}(\mathbf{X}) = 1\}$, then (6) 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., [10]) 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 3.2. The bounds of Theorems 3.1 apply to any mixed system of strict and/or nonstrict inequalities

$$\begin{aligned} \mathbf{A}_i \cdot \mathbf{X} &\le b_i, \quad i = 1, \dots, k, \\ \mathbf{A}_i \cdot \mathbf{X} &< b_i, \quad i = k+1, \dots, m, \\ \mathbf{X} &\succeq 0, \mathbf{X} \succ_L 0, \end{aligned} \tag{7}$$

where L is a linear subspace in $\mathbb{R}^n$, and the constraint $\mathbf{X} \succ_L 0$ means that $\mathbf{X}$ is positive definite on L. This fact follows from the observation that for any $t \in (0, 1)$ and any solutions $\mathbf{X}_1$ and $\mathbf{X}_2$ of systems (7) and (1), respectively, the convex combination $t\mathbf{X}_1 + (1-t)\mathbf{X}_2$ satisfies (7).

THEOREM 3.3.

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

(ii) Moreover, if the feasible set of (2) is bounded, then the above estimate holds for any solution of (2).

Proof. We can assume without loss of generality that the input matrices $\mathbf{Q}_1, \dots, \mathbf{Q}_m$ are linearly independent, and hence $m \le n(n+1)/2$. Suppose that (2) is feasible and consider the formula

$$\Psi(R) \doteq \exists \mathbf{x} \in \mathbb{R}^m \{(\mathbf{Q}_0 + x_1\mathbf{Q}_1 + \cdots + x_m\mathbf{Q}_m \succeq 0) \wedge (\|\mathbf{x}\| \le R)\}$$

or equivalently,

$$\begin{aligned} &\exists \mathbf{x} \in \mathbb{R}^m \quad \forall \lambda \in \mathbb{R}\{[(\det(\mathbf{Q}_0 + x_1\mathbf{Q}_1 + \cdots + x_m\mathbf{Q}_m - \lambda I_n) \neq 0) \\ &\quad \vee \ (\lambda \ge 0)] \wedge (\mathbf{x}^T\mathbf{x} \le R^2)\}. \end{aligned}$$

$\Psi(R)$ is a standard formula with $\omega = 2$ quantifiers in $n_1 = m$ and $n_2 = 1$ variables, respectively, which has $k = 1$ free variable and consists of $r = 3$ atomic polynomial inequalities of degree at most $d = n$, whose integer coefficients have at most $B = n(l + \log(nm) + 1)$ bits each. Hence $\Psi(R)$ can be satisfied by a number R such that $\log R = ln^{O(m)}$. But $m \le n^2$, which implies part (**i**) of the theorem.

To show part (**ii**), apply the above arguments to the modified formula

$$\Psi'(R) \doteq \forall \mathbf{x} \in \mathbb{R}^m \{(\mathbf{Q}_0 + x_1\mathbf{Q}_1 + \cdots + x_m\mathbf{Q}_m \succeq 0) \Longrightarrow (\|\mathbf{x}\| \le R)\}. \quad \square$$

Clearly, the bounds of Theorem 3.3 also hold for any strict and/or mixed system (2).

We close this section with examples of ill-posed feasible systems (1) and (2).

EXAMPLE 3.4. Let n be an even number. Consider $n \times n$ symmetric positive semidefinite matrices $\mathbf{X}$ satisfying the system of linear equations:

$$\begin{aligned} &\mathbf{X}_{11} = 1, \quad \mathbf{X}_{12} = 2^l, \\ &\mathbf{X}_{kk} = 1, \quad \mathbf{X}_{k,k+1} = \mathbf{X}_{k-1,k-1}, \quad \text{for} \quad k = 3, 5, \dots, n-1. \end{aligned}$$

It is easy to check that this instance of (1) is feasible and $\log \mathbf{X}_{n,n} \geq l2^{n/2}$ for any of its solutions. A similar example for problem (2) is given below.

EXAMPLE 3.5. Given two matrices $\mathbf{A} \in S_{n_1}$ and $\mathbf{B} \in S_{n_2}$, denote by

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

their direct sum. For $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{R}^m$, let

$$\mathbf{Q}_1(\mathbf{x}) = \begin{bmatrix} 1 & 2^l \\ 2^l & x_1 \end{bmatrix} \text{ and } \mathbf{Q}_k(\mathbf{x}) = \begin{bmatrix} 1 & x_{k-1} \\ x_{k-1} & x_k \end{bmatrix}, \quad k = 2, \ldots, m.$$

Then $\mathbf{Q}(\mathbf{x}) = \mathbf{Q}_1(\mathbf{x}) \oplus \mathbf{Q}_2(\mathbf{x}) \oplus \cdots \mathbf{Q}_m(\mathbf{x}) \succeq 0$ is a feasible instance of (2), any solution of which satisfies $\log x_m \geq l2^m$.

4. Lower Bounds on the Discrepancy

Let $R = R(n, m, l)$ be the bound of Theorem 3.1, and let $C_R = \{\mathbf{X} \in S_n | \mathbf{X} \succeq 0,\ \mathrm{tr}(\mathbf{X}) \leq R\}$. The *discrepancy* of (1) is the optimal value of the convex programming problem:

$$\theta^* = \min\{\theta | \mathbf{A}_i \cdot \mathbf{X} \leq b_i + \theta, \quad i \in M = \{1, \ldots, m\}, \quad \mathbf{X} \in C_R\}. \tag{8}$$

Note that because of the compactness of C_R, the minimum in (8) is always attained, and $\theta^* \leq 0$ if and only if system (1) is feasible.

REMARK 4.1. There exist infeasible systems (1) such that $\inf\{\theta | \mathbf{A}_i \cdot \mathbf{X} \leq b_i + \theta, i \in M, \mathbf{X} \succeq 0\} = 0$. For instance, this is true for the system of linear inequalities $\mathbf{X}_{11} \leq 0$, $\mathbf{X}_{12} \leq -1$, where $\mathbf{X} = (\mathbf{X}_{ij})$ is a symmetric positive semidefinite matrix of order 2.

THEOREM 4.2. *If (1) is infeasible, then* $-\log \theta^* = ln^{O(\min\{m,n^2\})}$.

Although Theorem 4.2 can be proved analogously to Theorem 3.1, it is convenient to postpone its proof until Section 5.

Now we consider systems (2). Let $R = R(n, m, l)$ be the bound of Theorem 3.3, and let $U_R = \{\mathbf{x} \in \mathbb{R}^m | \|\mathbf{x}\| \leq R\}$ be the m-dimensional ball of radius R centered at the origin. The discrepancy of (2) is the optimal value of the concave program:

$$\lambda^* = \max\{\lambda_n(\mathbf{Q}_0 + x_1\mathbf{Q}_1 + \cdots + x_m\mathbf{Q}_m) | \mathbf{x} = (x_1, \ldots, x_m) \in U_R\}. \tag{9}$$

Clearly, (2) is feasible if and only if $\lambda^* \geq 0$.

THEOREM 4.3. *If (2) is infeasible, then* $-\log(-\lambda^*) = ln^{O(\min\{m,n^2\})}$.

The proof of this theorem is also postponed until Section 5. We close this section with examples of infeasible systems (1) and (2) whose discrepancies are doubly exponentially small.

EXAMPLE 4.4. Let n be even, and consider $n \times n$ symmetric positive semidefinite matrices **X** satisfying the equations:

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

It is easy to check that this instance of (1) is infeasible and $-\log \theta^* \geq l2^{n/2}$.

EXAMPLE 4.5. For $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{R}^m$, let

$$\mathbf{Q}_1(\mathbf{x}) = \begin{bmatrix} 2^l x_1 & x_1 \\ x_1 & 2^l x_2 \end{bmatrix}, \quad \mathbf{Q}_m(\mathbf{x}) = \begin{bmatrix} -x_m & 0 \\ 0 & x_1 - 1 \end{bmatrix},$$

and

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

Then $\mathbf{Q}(\mathbf{x}) = \mathbf{Q}_1(\mathbf{x}) \oplus \mathbf{Q}_2(\mathbf{x}) \oplus \cdots \mathbf{Q}_m(\mathbf{x}) \succeq 0$ is an infeasible instance of (2), and it can be verified that $-\log(-\lambda^*) \geq l2^{m-1}$.

5. Complexity Bounds

By Theorems 3.1 and 4.2, the feasibility of (1) can be determined by computing the optimal value θ^* of program (8) 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. [4]), 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 (1). This result can be improved as follows:

THEOREM 5.1. *The feasibility of (1) can be tested in* $mn^{O(\min\{m,n^2\})}$ *arithmetic operations over* $ln^{O(\min\{m,n^2\})}$*-bit numbers.*

Proof. We start with a weaker result.

LEMMA 5.2. *The feasibility of (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

$$\exists \mathbf{X} \in S_n \quad \forall \lambda \in \mathbb{R} \Big\{ \bigwedge_{i=1}^{m} (\mathbf{A}_i \cdot \mathbf{X} \le b_i) \wedge \\ \wedge [(\det(\mathbf{X} - \lambda \mathbf{I}_n) \ne 0) \vee (\lambda \ge 0)] \Big\} \tag{10}$$

states that (1) is feasible. Since the characteristic polynomial $\det(\mathbf{X} - \lambda \mathbf{I}_n) \in \mathbb{Z}[\mathbf{X}, \lambda]$ has height 1, from Proposition 2.3 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 (1) can also be decided in $(mn)^{O(m)}$ operations with $l(mn)^{O(m)}$-bit numbers. Consider the sentence

$$\exists R \in \mathbb{R} \quad \Phi(R), \tag{11}$$

where $\Phi(R)$ is the formula defined in the proof of Theorem 3.1. This sentence also states that (1) is feasible. Observe that (11) consists of $r = O(m)$ polynomial inequalities of degree n in $O(m)$ variables and has integer coefficients of binary size at most $B = n(l + \log(nm) + 1)$. Since $\det(\sum_{i=1}^{m} y_i \mathbf{A}_i - \lambda \mathbf{I}_n)$ can be evaluated in poly(n, m) operations (or because all of its coefficients can be computed in $n^{O(m)}$ operations), the lemma follows from Proposition 2.3. □

We continue with the proof of Theorem 5.1. If m is bounded by a polynomial in n, the theorem follows from Lemma 5.2. We next show that for large m, determining the feasibility of (1) via Clarkson's algorithm [3] 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

$$\theta(I) = \min\{\theta |\, \mathbf{A}_i \cdot \mathbf{X} \le b_i + \theta, \quad i \in I,\, \mathbf{X} \in C_R\}, \tag{12}$$

where $R = R(n, m, l)$ is the bound of Theorem 3.1 for the entire system (1). With this notation, we have $\theta^* = \theta(M)$. Denote by $\mathbf{X}(I)$ the (unique) least norm solution of the system $\mathbf{A}_i \cdot \mathbf{X} \le b_i + \theta(I)$, $i \in I, \mathbf{X} \in C_R$, and let $V(I) = \{i \in M | \mathbf{A}_i \cdot \mathbf{X}(I) > b_i + \theta(I)\}$ be the set of constraints violated by $\mathbf{X}(I)$. A set I is called a *basis*, if $V(J) \ne V(I)$ 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

$$V(S) = V(M) = \emptyset, \text{ and consequently, } \theta(S) = \theta(M) = \theta^*. \tag{13}$$

From Helly's theorem it follows that $D \doteq \max\{|I| \mid I \text{ a basis}\} \le n(n+1)/2$. Given an optimal basis S, we can apply Lemma 5.2 to $\mathbf{A}_i \cdot \mathbf{X} \le b_i, i \in S, \mathbf{X} \succeq 0$ and determine the feasibility of the original system (1) in $n^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers. Clarkson's algorithm 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 checks whether $j \in V(I)$ for a sample set I of cardinality $O(D^2 \log D)$ and an index $j \in M \backslash I$.* Note that the inclusion $j \in V(I)$ can be written as the sentence

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

where $S_I(\mathbf{X}, \theta)$ is the quantifier free formula $\{\wedge_{i \in I}(\mathbf{A}_i \cdot \mathbf{X} \leq b_i + \theta) \wedge (\|\mathbf{X}\|^2 \leq R^2)\}$. Since the positive semidefiniteness of $\mathbf{X}$ can be expressed by the formula $\forall \lambda \in \mathbb{R}\, C(\mathbf{X}, \lambda)$, where $C(\mathbf{X}, \lambda) \doteq \{(\det(\mathbf{X} - \lambda \mathbf{I}_n) \neq 0) \vee (\lambda \geq 0)\}$, it follows that $V_{I,j}$ is equivalent to:

$$\begin{aligned} \forall (\mathbf{X}, \mathbf{X}', \theta, \theta') \in \mathbb{R}^{n(n+1)+2} \quad & \exists (\lambda, \lambda') \in \mathbb{R}^2 \{\{C(\mathbf{X}, \lambda) \wedge C(\mathbf{X}', \lambda') \\ & \wedge\ S_I(\mathbf{X}, \theta) \wedge [S_I(\mathbf{X}', \theta') \Longrightarrow (\theta \leq \theta')] \\ & \wedge\ [S_I(\mathbf{X}', \theta) \Longrightarrow (\|\mathbf{X}\|^2 \leq \|\mathbf{X}'\|^2)]\} \Longrightarrow (\mathbf{A}_j \cdot \mathbf{X} > b_j + \theta)\}. \end{aligned}$$

Each violation test can thus be represented by a sentence in prenex form with $r = O(|I|) \leq \text{poly}(n)$ polynomial inequalities of degree $d = n$ in $O(n^2)$ variables. Note also that the coefficients of these polynomial inequalities are integers of binary length $B \leq \max\{l, \log R\} = ln^{O(\min\{m,n^2\})}$. Now from Proposition 2.3 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 (1) requires expected $mn^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers.

Chazelle and Matousek [2] 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 $\mathbb{R}^n$. The analysis of their algorithm is based on an additional assumption which we state here in the following stronger form: there is a constant $\tilde{D}$ such that for any subset $I \subseteq M$, all subsets of I violated by some $(\mathbf{X}, \theta)$ can be computed in $O(|I|)^{\tilde{D}}$ operations. Since computing the above set system can be accomplished by constructing the arrangement of the hyperplanes $\mathbf{A}_i \cdot \mathbf{X} = b_i + \theta, i \in I$ (see the argument of [2] for linear programming), we have $\tilde{D} = O(n^2)$. Let $\mathcal{D} = \max\{D, \tilde{D}\}$. The algorithm of [2] computes an optimal basis of (8) 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 fact, by using the arguments of Section 4 in [3], one can verify 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) $V(I) \subseteq M \backslash I$ and (ii) $V(I \cup \{j\}) = V(I)$ for any $j \in M \backslash V(I)$.

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 5.3. *The complexity bounds of Theorem 5.1 apply to the problem of computing an optimal basis of (8).*

THEOREM 5.4. *Given an optimal basis S of (8), in $n^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers we can find a system of univariate polynomial inequalities with integer coefficients such that θ^* is the only real solution of the system. In particular, θ^* is a root of a nontrivial polynomial $h(\theta) \in \mathbb{Z}[\theta]$ such that* $\log \mathit{height}(h) = ln^{O(\min\{m,n^2\})}$.

Proof. Assume w.l.o.g. that the given basis S coincides with M. In particular, $m \le n(n+1)/2$. From von Neumann's saddlepoint theorem and (4), it follows that for $R \ge 0$

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

Consider the formula

$$\Lambda(\theta) \doteq \forall \mathbf{y} \in \Delta_m \left\{ \min\left[0, R\lambda_n\left(\sum_{i=1}^m y_i \mathbf{A}_i\right)\right] - \sum_{i=1}^m y_i(b_i+\theta) \le 0 \right\},$$

where R the bound of Theorem 3.1. This formula states that $\theta \ge \theta^*$, and it can be written as follows:

$$\begin{aligned}&\forall \mathbf{y} \in \mathbb{R}^m \quad \exists \lambda \in \mathbb{R} \Bigg\{ \left(y_1 \ge 0, \ldots, y_m \ge 0, \sum_{i=1}^m y_i = 1\right) \\ &\Longrightarrow \left[\left(\det\left(\sum_{i=1}^m y_i \mathbf{A}_i - \lambda \mathbf{I}_n\right) = 0\right)\right. \\ &\left.\wedge \left(\left(\sum_{i=1}^m y_i(b_i+\theta) \ge 0\right) \vee \left(R\lambda - \sum_{i=1}^m y_i(b_i+\theta) \le 0\right)\right)\right]\Bigg\}.\end{aligned}$$

Now the formula $\Lambda^*(\theta) \doteq \forall\theta'\{\Lambda(\theta) \wedge [\Lambda(\theta') \Longrightarrow (\theta \le \theta')]\}$ defines θ^* in the sense that θ^* is the only real solution of $\Lambda^*(\theta)$. By consecutively applying Proposition 2.2 to $\Lambda(\theta)$ and $\Lambda^*(\theta)$, the latter formula can be transformed into a quantifier free formula to $\Lambda^{**}(\theta)$. This requires $(mn)^{O(m)} \le n^{O(\min\{m,n^2\})}$ operations with $\max\{l, \log R\}(mn)^{O(m)} \le ln^{O(\min\{m,n^2\})}$-bit numbers. $\Lambda^{**}(\theta)$ is composed of univariate polynomial relations $h(\theta)\Delta 0$, where $\Delta \in \{\le, <, =, \ne, >, \ge\}$. Since θ^* is the only real solution of $\Lambda^{**}(\theta)$, this formula can be transformed into an equivalent system of polynomial inequalities, which must contain a polynomial h such that $h(\theta^*) = 0$. □

REMARK 5.5. Under the assumption of Theorem 5.4, 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 (see Theorem 1.2 in [8]). Note that unlike the upper bound on the operations stated in Theorem 5.1, this bound depends on l.

REMARK 5.6. The *minimal polynomial* of an algebraic number α is the primitive irreducible polynomial $p(x) \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$ and the leading coefficient of $p(x)$ is positive. The *height* of α is the height of its minimal polynomial. Theorem 5.4 and the well-known inequality of Mignotte (see [5], p. 261) show that $\log \text{height}(\theta^*) = ln^{O(\min\{m,n^2\})}$.

Theorem 5.4 immediately implies Theorem 4.2, whose proof was postponed in Section 4.

Proof of Theorem 4.2. Suppose that system (1) is infeasible. Then $\theta^* > 0$ and by Theorem 5.4, the positive algebraic number θ^* is a root of a nontrivial polynomial $h(x) \in \mathbb{Z}[x]$ with integer coefficients of bit length $ln^{O(\min\{m,n^2\})}$. Since Proposition 2.4 implies that $\theta^* \geq 1/(1 + \text{height}(h))$, the theorem follows. □

The following result deals with the complexity of testing the feasibility of (2).

THEOREM 5.7. *The feasibility of (2) can be determined in* $O(mn^4) + n^{O(\min\{m,n^2\})}$ *operations over* $ln^{O(\min\{m,n^2\})}$*-bit numbers, where* l *is the maximum bit length of the entries of* $\mathbf{Q}_0, \mathbf{Q}_1, \ldots, \mathbf{Q}_m$.

Proof. If $m > n(n+1)/2$, we can find a linearly independent subsystem of $\mathbf{Q}_0, \mathbf{Q}_1, \ldots, \mathbf{Q}_m$ in $O(mn^4)$ operations. We can thus assume that $m \leq n(n+1)/2$. The feasibility of (2) can be stated as the sentence

$$\exists \mathbf{x} \in \mathbb{R}^m \quad \forall \lambda \in \mathbb{R}\{(\lambda \geq 0) \vee \det(\mathbf{Q}_0 + x_1\mathbf{Q}_1 + \cdots + x_m\mathbf{Q}_m - \lambda\mathbf{I}_n) \neq 0)\}$$

By Proposition 2.3, the validity of the above sentence can be decided in $n^{O(m)}$ arithmetic operations with $ln^{O(m)}$-bit numbers. □

It is easy to see that the discrepancy λ^* of (2) satisfies $h(\lambda^*) = 0$ with a nontrivial polynomial $h(x) \in \mathbb{Z}[x]$ such that $\log \text{height}(h) = ln^{O(\min\{m,n^2\})}$. This result and Proposition 2.4 imply Theorem 4.3.

6. Concluding Remarks

Theorem 5.1 can be extended to the optimization version of problem (**F**):

$$\alpha^* = \inf\{\mathbf{D} \cdot \mathbf{X} | \mathbf{A}_i \cdot \mathbf{X} \leq b_i, i = 1, \ldots, m, \mathbf{X} \succeq 0\}, \tag{14}$$

where $\mathbf{D}$ is a given $n \times n$ integral symmetric matrix. Specifically, in addition to testing the feasibility of (14), each of the following problems can also be solved in $mn^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers:

Boundedness. Determine whether the objective function is bounded from below on the set of feasible solutions.

Attainment. Determine whether the infimum is attained, that is, whether (14) has an optimal solution.

Least Norm Optimal Solution. Find systems of univariate polynomials defining α^* and each component of the least norm optimal solution of (14).

REMARK 6.1. The boundedness problem readily reduces to the feasibility problem. Although the attainment problem can also be reduced to the feasibility problem via the duality result of [7], the latter reduction polynomially increases both n and m and cannot be used in fixed dimension.

Finally, for the optimization version of $(\mathbf{G})$ with a given integral m-vector **d**:

$$\beta^* = \inf\{\mathbf{d}^T\mathbf{x}|\mathbf{Q}_0 + X_1\mathbf{Q}_1 + \cdots + x_m\mathbf{Q}_m \succeq 0, \quad \mathbf{x} \in \mathbb{R}^m\}, \tag{15}$$

the above four problems can be solved in $O(mn^4) + n^{O(\min\{m,n^2\})}$ operations over $ln^{O(\min\{m,n^2\})}$-bit numbers.

We plan to address these and some other extensions of Theorems 5.1 and 5.7 in a subsequent paper.

References

1. Adler, I. and Shamir, R. (1990), A Randomized Scheme for Speeding Up Algorithms for Linear and Convex Quadratic Programming Problems with a High Constraints-to-Variables Ratio, *Math. Programming* **61** (1993), 39–52.
2. Chazelle, B. and Matousek, J. (1993), On Linear-Time Deterministic Algorithms for Optimization Problems in Fixed Dimension, *Proc. of the 4th ACM-SIAM Symp. on Discrete Algorithms*, 281–290.
3. Clarkson, K.L. (1995), Las Vegas Algorithms for Linear and Integer Programming When the Dimension Is Small, *J. of ACM* **42** (1995), 488–499.
4. Grötschel, M., Lovász, L. and Schrijver, A. (1988), *Geometric Algorithms and Combinatorial Optimization*, Springer, Berlin.
5. Mignotte, M. (1982), Some Useful Bounds, in Buchberger, B., Collins, G.E., and Loos, R. (eds.) in cooperation with Albrecht, R., *Computer Algebra, Symbolic and Algebraic Computation (Second Edition)*, Springer, Wien.
6. Ramana, M.V. (1993) An Algorithmic Analysis of Multiquadratic and Semidefinite Programming Problems, *Ph.D. Thesis*, The Johns Hopkins University, Baltimore.
7. Ramana, M.V. (1995) An Exact Duality Theory for Semidefinite Programming and its Complexity Implications, *DIMACS Technical Report 95-02*.
8. Renegar, J. (1992a) On the Computational Complexity of Approximating Solutions for Real Algebraic Formulae, *SIAM J. on Computing* **21** (1992), 1008–1025.
9. Renegar, J. (1992b) On the Computational Complexity and Geometry of the First Order Theory of the Reals. Part I: Introduction; Preliminaries; the Geometry of Semi-Algebraic Sets; the Decision Problem for the Existential Theory of the Reals, *J. of Symbolic Computation* **13** (1992), 255–299.
10. Rockafellar, T.R., *Convex Analysis,* Princeton University Press, NJ, 1970.
11. Schrijver, A. (1986) *Theory of Linear and Integer Programming,* Wiley, New York.