Complexity, Exactness, and Rationality in Polynomial Optimization*

Daniel Bienstock[1], Alberto Del Pia[2], and Robert Hildebrand[3]

[1] Department of Industrial Engineering and Operations Research, Columbia University
dano@columbia.edu
[2] Department of Industrial and Systems Engineering & Wisconsin Institute for Discovery, University of Wisconsin-Madison
delpia@wisc.edu
[3] Grado Department of Industrial and Systems Engineering, Virginia Tech
rhil@vt.edu

Abstract. We focus on rational solutions or nearly-feasible rational solutions that serve as certificates of feasibility for polynomial optimization problems. We show that, under some separability conditions, certain cubic polynomially constrained sets admit rational solutions. However, we show in other cases that it is NP Hard to detect if rational solutions exist or if they exist of any reasonable size. Lastly, we show that in fixed dimension, the feasibility problem over a set defined by polynomial inequalities is in NP.

Keywords: Polynomial Optimization · Rational solutions · NP

1 Introduction

This paper addresses basic questions of precise certification of feasibility and optimality, for optimization problems with polynomial constraints, in polynomial time, under the Turing model of computation. Recent progress in polynomial optimization and mixed-integer nonlinear programming has produced elegant methodologies and effective implementations; however such implementations may produce *imprecise* solutions whose actual quality can be difficult to rigorously certify, even approximately. The work we address is motivated by these issues, and can be summarized as follows:

Question: given a polynomially constrained problem, what can be said about the existence of feasible or approximately feasible rational solutions of polynomial size (bit encoding length)[4], and more generally the existence of rational,

* A. Del Pia is partially funded by ONR grant N00014-19-1-2322. D. Bienstock is partially funded by ONR grant N00014-16-1-2889. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

[4] Throughout we will use the concept of *size* of rational numbers, vectors, linear inequalities, and formulations. For these standard definitions we refer the reader to Section 2.1 in [20]

feasible or approximately-feasible solutions that are also approximately-optimal for a given polynomial objective?

As is well-known, Linear Programming is polynomially solvable [11,13], and, moreover, every face of a rational polyhedron contains a point of polynomial size. [20]. If we instead optimize a quadratic function over linear constraints, the problem becomes NP-Hard [16], but perhaps surprisingly, Vavasis [22] proved that a feasible system consisting of linear inequalities and just one quadratic inequality, all with rational coefficients, always has a rational feasible solution of polynomial size. This was extended by Del Pia, Dey, and Molinaro [7] to show that the same result holds in the mixed-integer setting.

On the negative side, there are classical examples of SOCPs all of whose feasible solutions require exponential size [2], [18], [14], or all of whose feasible solutions are irrational (likely, a folklore result. See full paper). In the nonconvex setting, there are examples of quadratically constrained, linear objective problems, on n bounded variables, and with coefficients of magnitude $O(1)$, that admit solutions with maximum additive infeasibility $O(2^{-2^{\Theta(n)}})$ but multiplicative (or additive) superoptimality $\Theta(1)$ (see full paper). O'Donnell [15] questions whether SDPs associated with fixed-rank iterates of sums-of-squares hierarchies (which relax nonconvex polynomially constrained problem) can be solved in polynomial time, because optimization certificates might require exponential size. The issue of accuracy in solutions is not just of theoretical interest. As an example, [23] describes instances of SDPs (again, in the sums-of-squares setting) where a solution is very nearly certified as optimal, and yet proves substantially suboptimal.

Vavasis' result suggests looking at systems of two or more quadratic constraints, or (to some extent equivalently) optimization problems where the objective is quadratic, and at least one constraint is quadratic, with all other constraints linear. The problem of optimizing a quadratic subject to one quadratic constraint (and no linear constraints) can be solved in polynomial time using semidefinite-programming techniques [17], to positive tolerance. When the constraint is positive definite (i.e. a ball constraint) the problem can be solved to tolerance ϵ in time $\log\log\epsilon^{-1}$ [24], [12] (in other words $O(k)$ computations guarantee accuracy 2^{-2^k}). Vavasis [21] proved, on the other hand, that *exact* feasibility of a system of two quadratics can be tested in polynomial time.

With regards to systems of more than two quadratic constraints, Barvinok [3] proved a fundamental result: for each fixed integer m there is an algorithm that, given $n \times n$ rational matrices A_i ($1 \leqslant i \leqslant m$) tests, in polynomial-time, feasibility of the system of equations

$$x^T A_i x = 0 \quad \text{for } 1 \leqslant i \leqslant m, \quad x \in \mathbb{R}^n, \; \|x\|_2 = 1.$$

A feature of this algorithm is that certification does not rely on producing a feasible vector; indeed, all feasible solutions may be irrational. As a corollary of this result, [5] proves that, for each fixed integer m there is an algorithm that solves, in polynomial time, an optimization problem of the form

$$\min f_0(x), \quad \text{s.t.} \quad f_i(x) \leqslant 0 \quad \text{for } 1 \leqslant i \leqslant m$$

where for $0 \leqslant i \leqslant m$, $f_i(x)$ is an n-variate quadratic polynomial, and we assume that the quadratic part of $f_1(x)$ positive-definite; moreover a rational vector that is (additively) both ϵ-feasible and -optimal can be computed in time polynomial in the size of the formulation and $\log \epsilon^{-1}$. An important point with regards to [3] and [5] is that the analyses do not apply to systems of arbitrarily many *linear* inequalities and just two quadratic inequalities.

De Loera et. al. [6] use the *Nullstellensatz* to provide feasibility and infeasibility certificates to systems of polynomial equations through solving a sequence of large linear equations. Bounds on the size of the certificates are obtained [9]. This technique does not seem amenable to systems with a large number of linear inequalities due to the necessary transformation into equations and then blow up of the number of variables used.

Our Results. The main topic we address in this paper is whether a system of polynomial inequalities admits rational, feasible or near-feasible solutions of polynomial size. First, we show that in dimension 2, with one separable cubic inequality and linear inequalities, there exists a rational solution of polynomial size (Theorem 2). In the next section, we show that this result fails without separability. Using this motivating example, we show that it is strongly NP-hard to test if a system of quadratic inequalities that has feasible rational solutions, admits feasible rational solutions of polynomial size (Theorem 4). And it is also hard to test if a feasible system of quadratic inequalities has a rational solution (Theorem 5).

We next show that, given a system of polynomial inequalities on n variables that is known to have a bounded, nonempty feasible region, we can produce as a certificate of feasibility a rational, near-feasible vector that has polynomial size, for fixed n (Theorem 7). This certificate yields a direct proof that, in fixed dimension, the feasibility problem over a system of polynomial inequalities is in NP.

2 Existence of rational feasible solutions

Local Minimizers of Cubic Polynomials. We will prove results about the rationality of local minimizers of cubic polynomials. This will be used in the next section to argue that rational solutions exist to certain feasibility problems.

We first show that local minimizers of separable cubic polynomials are rational provided that the function value is rational.

We will need the following 3 lemmas. The first result is known by Nicolo de Brescia, a.k.a., Tartaglia. It shows that in a univariate cubic polynomial, shifting by a constant allows us to assume that the x^2 term has a zero coefficient.

Lemma 1 (Rational shift of cubic). *Let* $f(x) = ax^3 + bx^2 + cx + d$. *Then* $f(y - \frac{b}{3a}) = ay^3 + \tilde{c}y + \tilde{d}$ *where* $\tilde{c} = \frac{27a^2c - 9ab^2}{27a^2}$ *and* $\tilde{d} = \frac{27a^2d - 9abc + 2b^3}{27a^2}$.

Proof. Consider an assignment of variables $x = y - s$ where y is a new variable and s is the shift.

$$\begin{aligned} f(y-s) &= a(y-s)^3 + b(y-s)^2 + c(y-s) + d && (1)\\ &= ay^3 + (b-3as)y^2 + \left(3as^2 - 2bs + c\right) y - as^3 + bs^2 - cs + d && (2) \end{aligned}$$

Hence, setting $s = \frac{b}{3a}$, we have

$$f\left(y - \frac{b}{3a}\right) = ay^3 + \frac{27a^2c - 9ab^2}{27a^2} y + \frac{27a^2d - 9abc + 2b^3}{27a^2}. \quad (3)$$

□

The next lemma provides bounds on the roots of a univariate polynomial.

Lemma 2 (Cauchy - size of roots). *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$, where $a_n, a_0 \neq 0$. Let $\bar{x} \neq 0$ such that $f(\bar{x}) = 0$. Then $L \leqslant |\bar{x}| \leqslant U$, where*

$$U = 1 + \max\left\{\left|\tfrac{a_0}{a_n}\right|, \ldots, \left|\tfrac{a_{n-1}}{a_n}\right|\right\}, \quad \frac{1}{L} = 1 + \max\left\{\left|\tfrac{a_1}{a_0}\right|, \ldots, \left|\tfrac{a_n}{a_0}\right|\right\}.$$

The next lemma is a special case of Theorem 2.9 in [1].

Lemma 3. *Let $n \geqslant 1$. Let $r_i \in \mathbb{Q}_+$ for $i = 0, 1, \ldots, n$, $q_i \in \mathbb{Q}_+$ for $i = 1, \ldots, n$. If $\sum_{i=1}^n r_i \sqrt{q_i} = r_0$, then $\sqrt{q_i} \in \mathbb{Q}$ for all $i = 1, \ldots, n$. Furthermore, the size of $\sqrt{q_i}$ is polynomial in the size of q_i.*

Theorem 1 (Rational local minimum). *Let $f(x) = \sum_{i=1}^n f_i(x_i)$ where $f_i(x_i) = a_i x_i^3 + b_i x_i^2 + c_i x_i + d_i \in \mathbb{Z}[x_i]$ and $a_i \neq 0$ for all $i \in [n]$. Assume that the absolute value of the coefficients of f is at most H. Suppose x^* is the unique local minimum of f and $\gamma^* := f(x^*)$ is rational. Then x^* is rational and has size that is polynomial in $\log H$ and in the size of γ^*.*

Proof. For every $i \in [n]$, Let $\tilde{c}_i, \tilde{d}_i$ be defined as in Lemma 1, let $g_i(y_i) := a_i y_i^3 + \tilde{c}_i y_i$, and define $g(y) = \sum_{i=1}^n g_i(y_i)$. Then $y^* \in \mathbb{R}^n$ defined by $y_i^* := x_i^* + \frac{b_i}{3a_i}$, $i \in [n]$, is the unique local minimum of $g(y)$ and $g(y^*) = \gamma^* - \sum_{i=1}^n \tilde{d}_i$.

We now work with the gradient. Since y^* is a local minimum of g, we have $\nabla g(y^*) = 0$. Since $g(y)$ is separable, we obtain that for every $i \in [n]$,

$$g_i'(y_i^*) = 0 \quad \Rightarrow \quad y_i^* = \pm\sqrt{\frac{-\tilde{c}_i}{3a_i}}. \quad (4)$$

Furthermore, we will need to look at the second derivative. Since y^* is a local minimizer, then $\nabla^2 g(y^*) \geqslant 0$. Again, since $g(y)$ is separable, this implies that $g_i''(y_i) \geqslant 0$ for every $i \in [n]$. Hence we have

$$g_i''(y_i) \geqslant 0 \quad \Rightarrow \quad 6a_i y_i^* \geqslant 0 \quad \Rightarrow \quad a_i \left(\pm\sqrt{\frac{-\tilde{c}_i}{3a_i}}\right) \geqslant 0. \quad (5)$$

Also, notice that we must have $\frac{-\tilde{c}_i}{3a_i} \geqslant 0$ for $\sqrt{\frac{-\tilde{c}_i}{3a_i}}$ to be a real number. Thus,

$$\operatorname{sign}(-\tilde{c}_i) = \operatorname{sign}(a_i) = \operatorname{sign}\left(\pm\sqrt{\frac{-\tilde{c}_i}{3a_i}}\right). \tag{6}$$

Finally, we relate this to $g(y^*)$.

$$\gamma^* - \sum_{i=1}^n \tilde{d}_i = g(y^*) = \sum_{i=1}^n \left(a_i(\tfrac{-\tilde{c}_i}{3a_i})\left(\pm\sqrt{\tfrac{-\tilde{c}_i}{3a_i}}\right) + \tilde{c}_i\left(\pm\sqrt{\tfrac{-\tilde{c}_i}{3a_i}}\right)\right) = -\tfrac{2}{3}\sum_{i=1}^n |\tilde{c}_i|\sqrt{\frac{-\tilde{c}_i}{3a_i}}, \tag{7}$$

where the last equality comes from comparing the signs of the data from (6). Hence, we have

$$\sum_{i=1}^n |\tilde{c}_i|\sqrt{\frac{-\tilde{c}_i}{3a_i}} = -\tfrac{3}{2}(\gamma^* - \sum_{i=1}^n \tilde{d}_i). \tag{8}$$

By Lemma 3, for every $i \in [n]$, $\sqrt{\frac{-\tilde{c}_i}{3a_i}}$ is rational and has size polynomial in $\log H$ and in the size of γ^*. From (4), so does y^*, and hence x^*. □

Rational solutions to nice cubic feasibility problems. We denote by $\mathbb{Z}[x_1, \ldots, x_n]$ the set of all polynomial functions from $\mathbb{R}^n$ to $\mathbb{R}$ with integer coefficients. For ease of notation, in the remainder of the paper we will write a polynomial $g \in \mathbb{Z}[x_1, \ldots, x_n]$ of degree d in the form $g(x) = \sum_{I \in \mathbb{N}^n, \|I\|_1 \leqslant d} c_I x^I$, where each $c_I \in \mathbb{Z}$ and $x^I := \prod_{i=1}^n x_i^{I_i}$. We next provide a standard result about Lipschitz continuity of a polynomial on a bounded region.

Lemma 4 (Lipschitz continuity of a polynomial on a box). *Let $g \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial of degree at most d with coefficients of absolute value at most H. Let $y, z \in [-M, M]^n$ for some $M > 0$. Then*

$$|g(y) - g(z)| \leqslant L\|y - z\|_\infty \tag{9}$$

where $L := ndHM^{d-1}(n+d)^{d-1}$.

Proof. Let $g(x) = \sum_{I \in \mathbb{N}^n, \|I\|_1 \leqslant d} c_I x^I$. By the fundamental theorem of calculus,

$$g(z) = g(y) + \int_{\lambda=0}^{\lambda=1} \nabla g(y + \lambda(z-y))^\top (z-y)\, d\lambda.$$

Therefore, an upper bound on $|g(y) - g(z)|$ can be obtained by bounding the quantity $|\nabla g(y+\lambda(z-y))^\top (z-y)|$ with $\lambda \in [0,1]$. In the remainder of the proof we derive such a bound.

Note that, for every $i = 1, \ldots, n$, we can write

$$(\nabla g(x))_i = \sum_{I \in \mathbb{N}^n, \|I\|_1 \leqslant d-1} \tilde{c}_{I,i} x^I, \tag{10}$$

where $|\tilde{c}_{I,i}| \leqslant dH$. Hence, for any $I \in \mathbb{N}^n$ with $\|I\|_1 \leqslant d-1$ and $x \in [-M,M]^n$, we have $|\tilde{c}_{I,i}x^I| \leqslant dHM^{d-1}$.

Next we bound the number of terms in the summation in (10). A *weak composition* of an integer q into p parts is a sequence of p non-negative integers that sum up to q. Two sequences that differ in the order of their terms define different weak compositions. It is well-known that the number of weak compositions of a number q into p parts is $\binom{q+p-1}{p-1} = \binom{q+p-1}{q}$. For more details on weak compositions see, for example, [10]. We obtain that the number of terms in the summation in (10) is bounded by

$$\sum_{i=0}^{d-1} \binom{i+n-1}{i} \leqslant \sum_{i=0}^{d-1} \binom{d+n-2}{i} \leqslant (d+n-1)^{d-1} \leqslant (n+d)^{d-1},$$

where in the second inequality we used the binomial theorem.

We obtain that for every $x \in [-M,M]^n$,

$$\|\nabla g(x)\|_\infty \leqslant dHM^{d-1}(n+d)^{d-1}.$$

Therefore, for any $\lambda \in [0,1]$,

$$\begin{aligned} |\nabla g(y+\lambda(z-y))^\top (z-y)| &\leqslant n \cdot \|\nabla g(y+\lambda(z-y))\|_\infty \cdot \|y-z\|_\infty \\ &\leqslant n \cdot dHM^{d-1}(n+d)^{d-1} \cdot \|y-z\|_\infty. \end{aligned}$$

□

Next, we present a result that employs Lemma 4 and that will be used in a couple of proofs in the remainder of the paper.

Proposition 1. *Let $f_i \in \mathbb{Z}[x_1,\dots,x_n]$, for $i \in [m]$, of degree one. Let $g_j \in \mathbb{Z}[x_1,\dots,x_n]$, for $j \in [\ell]$, of degree bounded by an integer d. Assume that the absolute value of the coefficients of f_i, $i \in [m]$, and of g_j, $j \in [\ell]$, is at most H. Let δ be a positive integer. Let $P := \{x \in \mathbb{R}^n \mid f_i(x) \leqslant 0, i \in [m]\}$ and consider the sets*

$$R := \{x \in P \mid g_j(x) \leqslant 0, j \in [\ell]\},\ \ S := \{x \in P \mid \ell\delta g_j(x) \leqslant 1, j \in [\ell]\}.$$

Assume that P is bounded. If R is nonempty, then there exists a rational vector in S of size bounded by a polynomial in $n, d, \log\ell, \log H, \log\delta$.

Proof. Since P is bounded, it follows from Lemma 8.2 in [4] that $P \subseteq [-M,M]^n$, where $M = (nH)^n$. Let L be defined as in Lemma 4, i.e.,

$$L := ndHM^{d-1}(n+d)^{d-1} = ndH(nH)^{n(d-1)}(n+d)^{d-1}.$$

Note that $\log L$ is bounded by a polynomial in $n, d, \log H$. Let $\varphi := \lceil LM\ell\delta \rceil$. Therefore $\log\varphi$ is bounded by a polynomial in $n, d, \log\ell, \log H, \log\delta$.

We define the following $(2\varphi)^n$ boxes in $\mathbb{R}^n$ with $j_1,\dots,j_n \in \{-\varphi,\dots,\varphi-1\}$:

$$\mathcal{C}_{j_1,\dots,j_n} := \left\{ x \in \mathbb{R}^n \mid \frac{M}{\varphi} j_i \leqslant x_i \leqslant \frac{M}{\varphi}(j_i+1), i \in [n] \right\}. \quad (11)$$

Note that the union of these $(2\varphi)^n$ boxes is the polytope $[-M, M]^n$ which contains the polytope P. Furthermore, each of the $2n$ inequalities defining a box (11) has size polynomial in $n, d, \log \ell, \log H, \log \delta$.

Let $\tilde{x}$ be a vector in R, according to the statement of the theorem. Since $\tilde{x} \in P$, there exists a box among (11), say $\tilde{\mathcal{C}}$, that contains $\tilde{x}$. Let $\bar{x}$ be a vertex of the polytope $P \cap \tilde{\mathcal{C}}$. Since each inequality defining P or $\tilde{\mathcal{C}}$ has size polynomial in $n, d, \log \ell, \log H, \log \delta$, it follows from Theorem 10.2 in [20] that also $\bar{x}$ has size polynomial in $n, d, \log \ell, \log H, \log \delta$.

To conclude the proof of the theorem we only need to show $\bar{x} \in S$. Since $\bar{x}, \tilde{x} \in \tilde{\mathcal{C}}$, we have $\|\bar{x} - \tilde{x}\|_\infty \leqslant \frac{M}{\varphi}$. Then, from Lemma 4 we obtain that for each $j \in [\ell]$,

$$|g_j(\bar{x}) - g_j(\tilde{x})| \leqslant L\|\bar{x} - \tilde{x}\|_\infty \leqslant \frac{LM}{\varphi} \leqslant \frac{1}{\ell\delta}.$$

If $g_j(\bar{x}) \leqslant 0$ we directly obtain $g_j(\bar{x}) \leqslant \frac{1}{\ell\delta}$ since $\frac{1}{\ell\delta} > 0$. Otherwise we have $g_j(\bar{x}) > 0$. Since $g_j(\tilde{x}) \leqslant 0$, we obtain $g_j(\bar{x}) \leqslant |g_j(\bar{x}) - g_j(\tilde{x})| \leqslant \frac{1}{\ell\delta}$. We have shown that $\bar{x} \in S$, and this concludes the proof of the theorem. □

We are now ready to prove our main result of this section.

Theorem 2. *Let $n \in \{1, 2\}$. Let $f_i \in \mathbb{Z}[x_1, \ldots, x_n]$, for $i \in [m]$, of degree one. Let $g(x) = \sum_{i=1}^n (a_i x_i^3 + b_i x_i^2 + c_i x_i + d_i) \in \mathbb{Z}[x_1, \ldots, x_n]$ with $a_i \neq 0$ for $i \in [n]$. Assume that the absolute value of the coefficients of g, f_i, $i \in [m]$, is at most H. Consider the set*

$$R := \{x \in \mathbb{R}^n \mid g(x) \leqslant 0,\ f_i(x) \leqslant 0, i \in [m]\}.$$

If R is nonempty, then it contains a rational vector of size bounded by a polynomial in $\log H$. This vector provides a certificate of feasibility for R that can be checked in a number of operations that is bounded by a polynomial in $m, \log H$.

Proof. Define $P := \{x \in \mathbb{R}^n \mid f_i(x) \leqslant 0, i \in [m]\}$, let x^* be a vector in P minimizing $g(x)$, and let $\gamma^* := g(x^*)$. We prove separately the cases $n = 1, 2$.

First we consider the case $n = 1$. If x^* is in the boundary of P, then, since P is an interval described by rational data, we must have x^* is an endpoint of this interval and hence is rational and of size bounded by a polynomial in $\log H$. Thus, in the remainder of the proof we suppose that x^* is in the interior of P. In particular, x^* is the unique local minimum of g.

Since R is nonempty, we have $\gamma^* \leqslant 0$. If we have $\gamma^* = 0$, then Theorem 1 implies that the size of x^* is bounded by a polynomial in $\log H$, thus the result holds. Therefore, in the remainder of the proof we assume $\gamma^* < 0$.

Let $\tilde{c}, \tilde{d}$ be defined as in Lemma 1. Following the calculation of Theorem 1, (8) $\gamma^* - \tilde{d} = -\frac{2}{3}|\tilde{c}| \left(\pm\sqrt{\frac{-\tilde{c}}{3a}}\right)$. Hence, $(\gamma^* - \tilde{d})^2 = -\frac{4\tilde{c}^3}{27a}$, that is, γ^* is a non-zero root of the above quadratic equation. From Lemma 2, we have that $|\gamma^*| \geqslant \frac{1}{\delta}$, where δ is an integer and $\log \delta$ is bounded by a polynomial in $\log H$. Since $\gamma^* < 0$, we have thereby shown that x^* is a vector in P satisfying $g(x^*) \leqslant -\frac{1}{\delta}$.

Clearly x^* is a root of the quadratic equation $g'(x) = 0$, thus using again Lemma 2 we obtain that $-M \leqslant x^* \leqslant M$, where M is an integer and $\log M$ is bounded by a polynomial in $\log H$. We apply Proposition 1 to the polytope $\{x \in \mathbb{R} \mid f_i(x) \leqslant 0, i \in [m],\ -M \leqslant x \leqslant M\}$, with $j := 1$, and with $g_1(x) := g(x) + \frac{1}{\delta}$. Proposition 1 then implies that there exists a vector $\bar{x} \in P$ with $g_1(\bar{x}) \leqslant \frac{1}{\delta}$, or equivalently $g(\bar{x}) \leqslant 0$, of size bounded by a polynomial in $\log H$. Such a vector is our certificate of feasibility.

Next, we consider the case $n = 2$. If x^* is in the boundary of P, then we can restrict to a face of P and reformulate the problem in dimension one. Then the first part of the proof ($n = 1$) secures the result. Thus, in the remainder of the proof we suppose that x^* is in the interior of P. In particular, x^* is the unique local minimum of g. As in the proof of the case $n = 1$, due to Theorem 1, we can assume $\gamma^* < 0$.

For every $i \in [n]$, let $\tilde{c}_i, \tilde{d}_i$ be defined as in Lemma 1. Following the calculation of Theorem 1, (8) $\sum_{i=1}^{2} |\tilde{c}_i|\sqrt{\frac{-\tilde{c}_i}{3a_i}} = -\frac{3}{2}(\gamma^* - \sum_{i=1}^{2} \tilde{d}_i)$. Squaring both sides we obtain

$$\sum_{i=1}^{2} \frac{-\tilde{c}_i^3}{3a_i} + 2|\tilde{c}_1||\tilde{c}_2|\sqrt{\frac{\tilde{c}_1\tilde{c}_2}{9a_1a_2}} = \frac{9}{4}(\gamma^* - \sum_{i=1}^{2} \tilde{d}_i)^2.$$

If we isolate the square root, and then square again both sides of the equation, we obtain that γ^* is a non-zero root of a quartic equation with rational coefficients. From Lemma 2, we have that $|\gamma^*| \geqslant \frac{1}{\delta}$, where δ is an integer and $\log \delta$ is bounded by a polynomial in $\log H$. Since $\gamma^* < 0$, we have thereby shown that x^* is a vector in P satisfying $g(x^*) \leqslant -\frac{1}{\delta}$.

Clearly, for $i \in [2]$, x_i^* is a root of the quadratic equation

$$(a_i x_i^3 + b_i x_i^2 + c_i x_i + d_i)' = 3a_i x_i^2 + 2b_i x_i + c_i = 0,$$

thus using again Lemma 2 we obtain that $-M \leqslant x_i^* \leqslant M$, where M is an integer and $\log M$ is bounded by a polynomial in $\log H$. We apply Proposition 1 to the polytope $\{x \in \mathbb{R}^2 \mid f_i(x) \leqslant 0, i \in [m],\ -M \leqslant x_i \leqslant M, i \in [2]\}$, with $j := 1$, and with $g_1(x) := g(x) + \frac{1}{\delta}$. Proposition 1 then implies that there exists a vector $\bar{x} \in P$ with $g_1(\bar{x}) \leqslant \frac{1}{\delta}$, or equivalently $g(\bar{x}) \leqslant 0$, of size bounded by a polynomial in $\log H$. Such a vector is our certificate of feasibility.

To conclude the proof for both cases $n = 1$ and $n = 2$, we bound the number of operations needed to check if $\bar{x}$ is in R by substituting $\bar{x}$ in the $m+1$ inequalities defining R. It is simple to check that $\bar{x}$ satisfies these $m+1$ inequalities in a number of operations that is bounded by a polynomial in $m, \log H$. □

In Example 1 in Section 3, we will see that Theorem 2 is best possible. We also remark that Theorem 2 implies that the corresponding feasibility problem is in the complexity class NP.

3 NP-Hardness of determining existence of rational feasible solutions

We begin with two, previously unknown, motivating examples.

Example 1 (Feasible system with no rational feasible vector). Define

$$h(y) := 2y_1^3 + y_2^3 - 6y_1y_2 + 4, \quad R_\gamma := [1.259 - \gamma, 1.26] \times [1.587, 1.59]. \qquad (12)$$

Then $\{y \in R_0 : h(y) \leqslant 0\} = \{y^*\}$ where $y^* = (2^{\frac{1}{3}}, 2^{\frac{2}{3}}) \approx (1.2599, 1.5874)$.

In particular, for this bi-variate set described by one cubic constraint and linear inequalities there is a unique feasible solution, and it is irrational. ◇

Observation 3 *(1) The point $y^* \in R_\gamma$ for all $\gamma \geqslant 0$. (2) y^* is the unique minimizer of $h(y)$ for $y \in \mathbb{R}^2_+$. (3) For $y \in R_4$, $h(y) > -12$. (4) The point $\bar{y} = (-2.74, 1.588) \in R_4$ attains $h(\bar{y}) < -7$.*

Proof. (1) is clear. (2) On the curve defined by $y_2 = y_1^2$, which includes the point y^*, $h(y) = y_1^6 - 4y_1^3 + 4$ whose sole minimizer is at $y_1 = 2^{1/3} = y_1^*$. Moreover, $\frac{\partial A}{\partial y_1} = 6(y_1^2 - y_2)$. These two facts imply that, for any $y \in \mathbb{R}^2_+$, $h(y) \geqslant A(y_2^{1/2}, y_2) \geqslant A(y^*)$, with at least one of the two inequalities strict unless $y = y^*$as desired. (3) By (2), if $y \in \mathbb{R}^2_+$ then $h(y) \geqslant h(y^*) = 0$. Otherwise, $y_1 < 0$. Then $\frac{\partial h}{\partial y_1} = 6(y_1^2 - y_2)$ and so either (when $y_1^2 < y_2$) $h(y) \geqslant h(0, y_2) > 0$, or (when $y_1^2 \geqslant y_2$) $h(y) \geqslant h(1.259 - 4, y_2) > -12 + y_2^3 > -12$. (4) is clear. □

Example 2 (Exponentially Small Solutions). Next, consider the following system of quadratic inequalities on variables $d_1, \ldots, d_N$ and s such that

$$d_1 \leqslant \frac{1}{2}, s \leqslant d_N^2, \quad s \geqslant 0, \quad d_{k+1} \leqslant d_k^2 \text{ for } k \in [N-1],\ d_k \geqslant 0 \text{ for } k \in [N]. \quad (13)$$

In any feasible solution to system (13) we either have $s = 0$, or $0 < s \leqslant 2^{-2^N}$ and in this case if s is rational then we need more than 2^N bits to represent it. Further, there are rational solutions to system (13) with $s > 0$. ◇

NP-hardness construction. We will show that it is strongly NP-hard to test whether a system of quadratic inequalities which is known to have feasible rational solutions, admits feasible rational solutions of polynomial size (Theorem 4). The same proof technique shows that it is hard to test whether a feasible system of quadratic inequalities has a rational solution (Theorem 5).

The main reduction is from the problem 3SAT. An instance of this problem is defined by n *literals* $w_1, \ldots, w_n$ as well as their negations $\bar{w}_1, \ldots, \bar{w}_n$, and a set of m clauses $C_1, \ldots C_m$ where each clause C_i is of the form $(u_{i1} \vee u_{i2} \vee u_{i3})$. Here, each u_{ij} is a literal or its negation, and $\vee$ means 'or'. The problem is to find 'true' or 'false' values for each literal, and corresponding values for their negations, so that the formula

$$C_1 \wedge C_2 \ldots \wedge C_m \qquad (14)$$

is true, where $\wedge$ means 'and'.

Let $N \geqslant 1$ be an integer. For now N is generic; below we will discuss particular choices. Given an instance of 3SAT as above, we construct a system of quadratic inequalities on the following $2n + N + 7$ variables:

– For each literal w_j we have a variable x_j; for $\bar{w}_j$ we use variable x_{n+j}.
– Additional variables $\gamma, \Delta, y_1, y_2, s$, and $d_1, \ldots, d_N$.

We describe the constraints in our quadratically constrained problem[5]. For each clause $C_i = (u_{i_1} \vee u_{i_2} \vee u_{i_3})$ associate the variable x_{i_k} is with u_{i_k} for $1 \leqslant k \leqslant 3$.

$$-1 \leqslant x_j \leqslant 1 \text{ for } j \in [2n], \quad x_j + x_{n+j} = 0, \quad \text{for } j \in [n]. \tag{15a}$$

$$x_{i_1} + x_{i_2} + x_{i_3} \geqslant -1 - \Delta, \text{ for each clause } C_i = (u_{i_1} \vee u_{i_2} \vee u_{i_3}) \tag{15b}$$

$$0 \leqslant \gamma, \; 0 \leqslant \Delta \leqslant 2, \; \Delta + \frac{\gamma}{2} \leqslant 2, \; (y_1, y_2) \in R_\gamma, \tag{15c}$$

$$-n^5 \textstyle\sum_{j=1}^n x_j^2 \; + \; h(y) - s \leqslant -n^6. \tag{15d}$$

$$d_1 \leqslant \frac{1}{2}, s \leqslant d_N^2, \quad s \geqslant 0, \quad d_{k+1} \leqslant d_k^2 \text{ for } k \in [N-1], \; d_k \geqslant 0 \;\text{ for } k \in [N], \tag{15e}$$

Theorem 4. *The formula* (14) *is satisfiable if and only if there is a rational solution to* (15) *of size polynomial in n, m and N. As a result, it is strongly NP-hard to test if a system of quadratic inequalities has a rational feasible solution of polynomial size, even if the system admits rational feasible solutions.*

Comment. The choice $N = n$ in the above construction is natural and yields a result directly interpretable in terms of the formula (14).

Proof. **Claim 1:** *System* (15) *has a rational feasible solution.* To see this, set $x_j = 1 = -x_{n+j}$ for $j \in [n]$, $\Delta = 2, \gamma = 0, d_k = 2^{-2^{k-1}}$ for $k \in [N]$ and $s = 2^{-2^N}$. By inspection these rational values satisfy (15a), (15b), (15c), and (15e). Since y^* and y^* is in the interior of R_0, there exists a small ball $B \subseteq R_0$ containing y^*. Since h is continuous, y^* is the unique local minimizer of h, $h(y^*) = 0$, and the set $\mathbb{Q}^2$ is dense in $\mathbb{R}^2$, there exists a feasible rational choice of y such that $h(y) \leqslant s$. Hence, (15d) is also satisfied.

Claim 2: *Suppose $(x, \gamma, \Delta, y, d, s)$ is feasible for* (15)*. Then for $1 \leqslant j \leqslant 2n$, $|x_j| \geqslant 1 - \frac{12}{n^6} - \frac{2^{-2^N}}{n^6}$.*

To begin, let $\sigma^2 \coloneqq \min_j\{x_j^2\}$. Then $-n^6\sigma^2 \; + h(y) - s \leqslant n^6$, so $\sigma^2 \geqslant 1 + (h(y)-s)/n^6 \geqslant 1 - \frac{12}{n^6} - \frac{2^{-2^N}}{n^6}$, where the last inequality follows from Observation 3 and the fact that (15d) implies that $s \leqslant 2^{-2^N}$. □

Claim 3: *Suppose formula* (14) *is satisfiable. Then* (15) *has a rational feasible solution of polynomial size.*
For $1 \leqslant j \leqslant n$ set $x_j = 1 = -x_{n+j}$ if w_j is true, else set $x_j = -1 = -x_{n+j}$. Set $\Delta = 0$, $\gamma = 4$, and $d_1 = \ldots = d_N = s = 0$. Finally (Observation 3) we set $(y_1, y_2) = (-2.74, 1.588)$. □

The next result concludes the proof of Theorem 4.

[5] Constraint (15e) as written is cubic, but is equivalent to three quadratic constraints by defining new variables $y_1^2 = y_{12}$, $y_2^2 = y_{22}$, and rewriting the constraint as $-n^5 \sum_{j=1}^n x_j^2 \; + \; y_{12}y_1 + y_{22}y_2 - 6y_1y_2 + 4 \; - \; s \; \leqslant \; -n^6$

Claim 4: *Suppose formula* (14) *is not satisfiable. Then in every feasible rational solution to* (15)*, s has size at least 2^N.*
Let $(x, \gamma, \Delta, y, d, s)$ be feasible. For $1 \leqslant j \leqslant n$ set w_j to be true if $x_j > 0$ and false otherwise. It follows that there is at least one clause $C_i = (u_{i1} \vee u_{i2} \vee u_{i3})$ such that every u_{ik} (for $1 \leqslant k \leqslant 3$) is false, i.e. each $x_{ik} < 0$. Using constraint (15b) and Claim 2, we obtain

$$-3 + \frac{36}{n^6} + 3\frac{2^{-2^N}}{n^6} \geqslant -1 - \Delta, \text{ and by (15c)} \quad \gamma \leqslant \frac{72}{n^6} + 6\frac{2^{-2^N}}{n^6} < 1.$$

This fact has two implications. First, since $(y_1, y_2) \in R_\gamma \subset \mathbb{R}^2_+$, Observation 3 implies $h(y) > 0$ (because y is rational). Second, constraint (15d) implies $-n^5 \sum_{j=1}^n x_j^2 + h(y) - s \leqslant -n^6$ and, therefore, $h(y) \leqslant s$. So $s > 0$ and since $s \leqslant 2^{-2^N}$ (by constraint (15c)) the proof is complete. □

As an (easy) extension of Theorem 4 we have the following theorem.

Theorem 5. *It is strongly NP-hard to test if there exists a rational solution to a system of for form*

$$f(x) \leqslant 0, \quad Ax \leqslant b,$$

where $f \in \mathbb{Z}[x_1, \dots, x_n]$ is of degree 3*, and $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$.*

Proof sketch. We proceed with a transformation from 3SAT just as above, except that we dispense with the variables $d_1, \dots, d_N$ and s and, rather than constraint (15d) we impose

$$-n^5 \sum_{j=1}^{n} x_j^2 + h(y) \leqslant -n^6. \tag{16}$$

In the analog of Claim 4 we conclude that $y \in \mathbb{R}^2_+$ while also $h(y) \leqslant 0$ (no term $-s$) which yields that $y = y^*$. □

4 Short certificate of feasibility: an almost feasible point

In this section we are interested in the existence of *short* certificates of feasibility for systems of polynomial inequalities, i.e., certificates of feasibility of size bounded by a polynomial in the size of the system.

We will be using several times the functions ϵ and δ defined as follows:

$$\epsilon(n, m, d, H) := (2^{4-\frac{n}{2}} \max\{H, 2n + 2m\} d^n)^{-n2^n d^n},$$
$$\delta(n, m, d, H) := \lceil 2\epsilon^{-1}(n, m, d, H) \rceil = \lceil 2(2^{4-\frac{n}{2}} \max\{H, 2n + 2m\} d^n)^{n2^n d^n} \rceil.$$

A fundamental ingredient in our arguments is the following result by Geronimo, Perrucci, and Tsigaridas, which follows from Theorem 1 in [8].

Theorem 6. *Let $n \geqslant 2$. Let $g, f_i \in \mathbb{Z}[x_1, \dots, x_n]$, for $i \in [m]$, of degree bounded by an even integer d. Assume that the absolute value of the coefficients of g, f_i, $i \in [m]$, is at most H. Let $T := \{x \in \mathbb{R}^n \mid f_i(x) \leqslant 0, i \in [m]\}$, and let C be a compact connected component of T. Then, the minimum value that g takes over C, is either zero, or its absolute value is greater than or equal to $\epsilon(n, m, d, H)$.*

Using Theorem 6 we obtain the following lemma.

Lemma 5. *Let $n \geqslant 2$. Let $g, f_i \in \mathbb{Z}[x_1, \dots, x_n]$, for $i \in [m]$, of degree bounded by an even integer d. Assume that the absolute value of the coefficients of g, f_i, $i \in [m]$, is at most H. Let $\delta := \delta(n, m, d, H)$. Let $T := \{x \mid f_i(x) \leqslant 0, i \in [m]\}$ and consider the sets*

$$R := \{x \in T \mid g(x) \leqslant 0\}, \ S := \{x \in T \mid \delta g(x) \leqslant 1\}.$$

Assume that T is bounded. Then R is nonempty if and only if S is nonempty.

Proof. Since $\delta > 0$ we have $R \subseteq S$, therefore if R is nonempty also S is nonempty. Hence we assume that S is nonempty and we show that R is nonempty.

Since S is nonempty, there exists a vector $\bar{x} \in T$ with $g(\bar{x}) \leqslant 1/\delta < \epsilon(n, m, d, H)$. Let C be a connected component of T containing $\bar{x}$. Since T is compact, we have that C is compact as well. In particular, the minimum value that g takes over C is less than $\epsilon(n, m, d, H)$. The contrapositive of Theorem 6 implies that the minimum value that g takes over C is less than or equal to zero. Thus there exists $\tilde{x} \in C$ with $g(\tilde{x}) \leqslant 0$. Hence the set R is nonempty. □

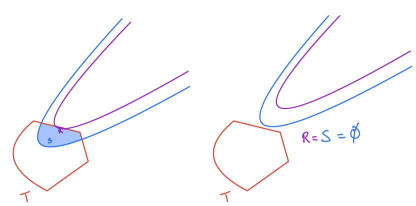

Fig. 1. Structure of sets in Lemmas 5 and Proposition 2. When T is bounded, with

From Lemma 5 we obtain the following result.

Proposition 2. *Let $n \geqslant 2$. Let $f_i, g_j \in \mathbb{Z}[x_1, \dots, x_n]$, for $i \in [m]$, $j \in [\ell]$, of degree bounded by an even integer d. Assume that the absolute value of the coefficients of f_i, $i \in [m]$, and of g_j, $j \in [\ell]$, is at most H. Let $\delta := \delta(n, m + \ell, 2d, \ell H^2)$. Let $T := \{x \mid f_i(x) \leqslant 0, i \in [m]\}$ and consider the sets*

$$R := \{x \in T \mid g_j(x) \leqslant 0, j \in [\ell]\}, \ S := \{x \in T \mid \ell \delta g_j(x) \leqslant 1, j \in [\ell]\}.$$

Assume that T is bounded. Then R is nonempty if and only if S is nonempty.

Proof. Since $\ell\delta > 0$ we have $R \subseteq S$, therefore if R is nonempty also S is nonempty. Hence we assume that S is nonempty and we show that R is nonempty.

Let $\bar{x} \in S$, and define the index set $J := \{j \in [\ell] : g_j(\bar{x}) > 0\}$. We introduce the polynomial function $g \in \mathbb{Z}[x_1, \dots, x_n]$ defined by $g(x) := \sum_{j \in J} g_j^2(x)$. Note that the degree of g is bounded by $2d$. The absolute value of the coefficients of each g_j^2 is at most H^2, hence the absolute value of the coefficients of g is at most ℓH^2. Next, let $T' := \{x \in T \mid g_j(x) \leqslant 0, j \in [\ell] \backslash J\}$ and

$$R' := \{x \in T' \mid g(x) \leqslant 0\}, \quad S' := \{x \in T' \mid \delta g(x) \leqslant 1\}.$$

First, we show that the vector $\bar{x}$ is in the set S', implying that S' is nonempty. Clearly $\bar{x} \in T$, and for every $j \in [\ell] \backslash J$ we have that $g_j(\bar{x}) \leqslant 0$, thus we have $\bar{x} \in T'$. For every $j \in J$, we have $0 < g_j(\bar{x}) \leqslant \frac{1}{\ell\delta}$, and since $\ell\delta \geqslant 1$, we have $0 < g_j^2(\bar{x}) \leqslant \frac{1}{\ell\delta}$. Thus, we obtain $g(\bar{x}) \leqslant \frac{\ell}{\ell\delta} = \frac{1}{\delta}$. We have thus proved $\bar{x} \in S'$, and so S' is nonempty.

Next, we show that the set R' is nonempty. To do so, we apply Lemma 5 to the sets T', R', S'. The number of inequalities that define T' is a number m' with $m \leqslant m' \leqslant m + \ell$. The degree of f_i, g_j, g, for $i \in [m]$, $j \in [\ell] \backslash J$, is bounded by $2d$. The absolute value of the coefficients of f_i, g_j, g, for $i \in [m]$, $j \in [\ell] \backslash J$, is at most ℓH^2. Since the function $\delta(n, m, d, H)$ is increasing in m and $m' \leqslant m + \ell$, we obtain from Lemma 5 that R' is nonempty if and only if S' is nonempty. Since S' is nonempty, we obtain that R' is nonempty.

Finally, we show that the set R is nonempty. Since R' is nonempty, let $\tilde{x} \in R'$. From the definition of R' we then know $\tilde{x} \in T$, $g_j(\tilde{x}) \leqslant 0$, for $j \in [\ell] \backslash J$, and $g(\tilde{x}) \leqslant 0$. Since g is a sum of squares, $g(\tilde{x}) \leqslant 0$ implies $g(\tilde{x}) = 0$, and this in turn implies $g_j(\tilde{x}) = 0$ for every $j \in J$. Hence $\tilde{x} \in R$, and R is nonempty. □

Proposition 2 and Proposition 1 directly yield our following main result.

Theorem 7 (Certificate of polynomial size). *Let $n \geqslant 2$. Let $f_i \in \mathbb{Z}[x_1, \dots, x_n]$, for $i \in [m]$, of degree one. Let $g_j \in \mathbb{Z}[x_1, \dots, x_n]$, for $j \in [\ell]$, of degree bounded by an even integer d. Assume that the absolute value of the coefficients of f_i, $i \in [m]$, and of g_j, $j \in [\ell]$, is at most H. Let $\delta := \delta(n, m + \ell, 2d, \ell H^2)$. Let $P := \{x \in \mathbb{R}^n \mid f_i(x) \leqslant 0, i \in [m]\}$ and consider the sets*

$$R := \{x \in P \mid g_j(x) \leqslant 0, j \in [\ell]\}, \; S := \{x \in P \mid \ell\delta g_j(x) \leqslant 1, j \in [\ell].$$

Assume that P is bounded. Denote by s the maximum number of terms of g_j, $j \in [\ell]$, with nonzero coefficients. If R is nonempty, then there exists a rational vector in S of size bounded by a polynomial in $d, \log m, \log \ell, \log H$, for n fixed. This vector is a certificate of feasibility for R that can be checked in a number of operations that is bounded by a polynomial in $s, d, m, \ell, \log H$, for n fixed.

Proof. From the definition of δ, we have that $\log \delta$ is bounded by a polynomial in $d, \log m, \log \ell, \log H$, for n fixed. From Proposition 1, there exists a vector $\bar{x} \in S$ of size bounded by a polynomial in $d, \log m, \log \ell, \log H$, for n fixed. Such a vector is our certificate of feasibility. In fact, from Proposition 2 (applied to the sets $T = P, R, S$), we know that S nonempty implies R nonempty.

To conclude the proof we bound the number of operations needed to check if the vector $\bar{x}$ is in S by substituting $\bar{x}$ in the $m + \ell$ inequalities defining S.

The absolute value of the coefficients of $f_i(x) \leqslant 0$, $i \in [m]$, is at most H. Thus, it can be checked that $\bar{x}$ satisfies these m inequalities in a number of operations that is bounded by a polynomial in $d, m, \log \ell, \log H$, for n fixed.

Next, we focus on the inequalities $\ell\delta g_j(x) \leqslant 1$, $j \in [\ell]$. Note that the total number of terms of $\ell\delta g_j$, $j \in [\ell]$, with nonzero coefficients is bounded by $s\ell$. The logarithm of the absolute value of each nonzero coefficient of $\ell\delta g_j(x)$, $j \in [\ell]$, is bounded by $\log(\ell\delta H)$, which in turn is bounded by a polynomial in $d, \log m, \log \ell, \log H$, for n fixed. Therefore, it can be checked that $\bar{x}$ satisfies these ℓ inequalities in a number of operations that is bounded by a polynomial in $s, d, \ell, \log m, \log H$, for n fixed. □

In particular, Theorem 7 implies that polynomial optimization is in NP, provided that we fix the number of variables. This fact is not new. In fact, it follows from Theorem 1.1 in Renegar [19] that the problem of deciding whether the set R, as defined in Theorem 7, is nonempty can be solved in a number of operations that is bounded by a polynomial in $s, d, m, \ell, \log H$, for n fixed. Therefore, Renegar's algorithm, together with its proof, provides a certificate of feasibility of size bounded by a polynomial in the size of the system, which in turns implies that the decision problem is in NP.

The main advantages of Theorem 7 over Renegar's result are that (i) our certificate of feasibility is simply a vector in S of polynomial size, and (ii) the feasibility of the system can be checked by simply plugging the vector into the system of inequalities defining S. The advantages of Renegar's result over our Theorem 7 are: (iii) Renegar does not need to assume that the feasible region is bounded, while we do need that assumption, and (iv) Renegar shows that the decision problem is in P, while we show that it is in the larger class NP.

Appendix

5 Examples

Example 3 (System of convex quadratics all of whose feasible solutions are large). Consider the system of inequalities $y_1 \geqslant 2$, $y_{i+1} - y_i^2 \geqslant 0$ for $i = 1, \ldots, n-1$. Then each feasible vector satisfies $y_n \geqslant 2^{2^{n-1}}$. Attributed to Ramana [18] and Khachiyan, see [14], [2]. ◇

Example 4 (A bounded feasible region QCQP whose solution requires exponentially many bits).

Consider the optimization problem

$$\begin{aligned} \max \quad & x_2 \\ \text{s.t.} \ & (x_1 - 1)^2 + \ x_2^2 \ - \ d_N^2 \ \geqslant \ 3 & \text{(17a)} \\ & (x_1 + 1)^2 + \ x_2^2 \ \geqslant \ 3 & \text{(17b)} \\ & \frac{x_1^2}{10} + x_2^2 \ \leqslant \ 2 & \text{(17c)} \\ & d_1 + d_N = \frac{1}{2}, \quad 0 \leqslant d_1, \quad d_i^2 \leqslant d_{i+1} \ (1 \leqslant i \leqslant N-1) & \text{(17d)} \end{aligned}$$

Suppose we allow for ϵ-feasible solutions, in the additive sense. We will show that unless $\epsilon < 2^{-2^N}$, there is an ϵ-feasible solution to problem (17) that attains value $\sqrt{2}$, whereas the true value of the problem is less than 1.23.

We begin with the latter statement. First, it is clear that (17d) implies that $d_N > 0$. Armed with this fact, we will show that (17a)-(17c) imply that $x_2 < 1.3$. To see this, note that (17b) and (17c) together imply that

$$3 \leqslant (x_1 + 1)^2 + 2 - \frac{x_1^2}{10},$$

or $0 \leqslant x_1(\frac{9}{10}x_1 + 2)$. Hence, if $x_1 < 0$ then $x_1 \leqslant -20/9$ and so by (17c), $x_2 < \sqrt{2 - (20/9)^2/10} \approx 1.228$. Likewise, (17a) and (17c) together imply that

$$3 + d_N^2 \leqslant (x_1 - 1)^2 + 2 - \frac{x_1^2}{10},$$

or $d_N^2 \leqslant x_1(\frac{9}{10}x_1 - 2)$. Hence, if $x_1 \geqslant 0$, then $x_1 > 0$ (because $d_N > 0$) and $x_1 \geqslant 20/9$, and as above by (17c), $x_2 < \sqrt{2 - (20/9)^2/10} \approx 1.228$. Thus, in any case, $x_2 \leqslant 1.228$.

At the same time, the vector given by $x_1 = 0$, $x_2 = \sqrt{2}$, $d_1 = \frac{1}{2}$, $d_i = \frac{1}{2^i}$ $(2 \leqslant i \leqslant N-1)$ and $d_N = 0$ satisfies (exactly) all constraints (17a)-(17d), except for $d_{N-1}^2 \leqslant d_N$, which it violates by 2^{-2^N}. This concludes the proof.

Example 5 (An SOCP all of whose feasible solutions are irrational).

Consider the sysem

$$\begin{aligned} \sqrt{x_0^2 + x_1^2 + x_2^2} \ &\leqslant \ 4 & \text{(18a)} \\ \sqrt{x_3^2 + x_4^2 + x_5^2} \ &\leqslant \ x_0 & \text{(18b)} \\ 3 \leqslant x_1,\ 2 \leqslant x_2,\ 1 \leqslant x_3,\ 1 &\leqslant x_4,\ 1 \leqslant x_5 & \text{(18c)} \end{aligned}$$

In any feasible solution we have

$$16 = 9 + 4 + 3 \leqslant \sum_{j=1}^{5} x_j^2 \leqslant x_1^2 + x_2^2 + x_0^2 \leqslant 16,$$

from which we conclude $x_1 = 3$, $x_2 = 2$ and $x_0 = \sqrt{3}$. Likely, examples of this type are already known.

References

1. Albu, T.: The irrationality of sums of radicals via cogalois theory. Analele stiintifice ale Universitatii Ovidius Constanta **19(2)**, 15–36 (2011)
2. Alizadeh, F.: Interior point methods in semidefinite programming with applications to combinatorial optimization. SIAM Journal on Optimization **5**, 13–51 (1995)
3. Barvinok, A.: Feasibility testing for systems of real quadratic equations. Disc. Comput. Geometry **10**, 1–13 (1993)
4. Bertsimas, D., Tsitsiklis, J.: Introduction to Linear Optimization. Athena Scientific (1997)
5. Bienstock, D.: A note on polynomial solvability of the CDT problem. SIAM J. Optimization **26**, 486–496 (2016)
6. De Loera, J.A., Lee, J., Malkin, P.N., Margulies, S.: Computing infeasibility certificates for combinatorial problems through Hilbert's nullstellensatz. Journal of Symbolic Computation **46**(11), 1260 – 1283 (2011). https://doi.org/https://doi.org/10.1016/j.jsc.2011.08.007, `http://www.sciencedirect.com/science/article/pii/S0747717111001192`
7. Del Pia, A., Dey, S.S., Molinaro, M.: Mixed-integer quadratic programming is in NP. Mathematical Programming **162**(1-2), 225–240 (Jun 2016). https://doi.org/10.1007/s10107-016-1036-0, `https://doi.org/10.1007/s10107-016-1036-0`
8. Geronimo, G., Perrucci, D., Tsigaridas, E.: On the minimum of a polynomial function on a basic closed semialgebraic set and applications. SIAM Journal on Optimization **23**(1), 241–255 (2013). https://doi.org/10.1137/110857751, `https://doi.org/10.1137/110857751`
9. Grigoriev, D., Vorobjov, N.: Complexity of null- and positivstellensatz proofs. Annals of Pure and Applied Logic **113**(1), 153 – 160 (2001). https://doi.org/https://doi.org/10.1016/S0168-0072(01)00055-0, `http://www.sciencedirect.com/science/article/pii/S0168007201000550`, first St. Petersburg Conference on Days of Logic and Computability
10. Heubach, S., Mansour, T.: Combinatorics of Compositions and Words. Discrete Mathematics and Its Applications, CRC Press (2009)
11. Karmarkar, N.: A new polynomial-time algorithm for linear programming. Combinatorica **4**(4), 373–395 (Dec 1984). https://doi.org/10.1007/bf02579150, `https://doi.org/10.1007/bf02579150`
12. Karmarkar, N.: An interior-point approach to NP-complete problems (1989), manuscript
13. Khachiyan, L.: Polynomial algorithms in linear programming. USSR Computational Mathematics and Mathematical Physics **20**(1), 53 – 72 (1980). https://doi.org/https://doi.org/10.1016/0041-5553(80)90061-0, `http://www.sciencedirect.com/science/article/pii/0041555380900610`
14. Letchford, A., Parkes, A.J.: A guide to conic optimisation and its applications. RAIRO-Oper. Res. pp. 1087–1106 (2018)
15. O'Donnell, R.: SOS Is Not Obviously Automatizable, Even Approximately. In: Papadimitriou, C.H. (ed.) 8th Innovations in Theoretical Computer Science Conference (ITCS 2017). Leibniz International Proceedings in Informatics (LIPIcs), vol. 67, pp. 59:1–59:10. Dagstuhl, Germany (2017). https://doi.org/10.4230/LIPIcs.ITCS.2017.59, `http://drops.dagstuhl.de/opus/volltexte/2017/8198`

16. Pardalos, P.M., Vavasis, S.A.: Quadratic programming with one negative eigenvalue is np-hard. Journal of Global Optimization **1**(1), 15–22 (Mar 1991). https://doi.org/10.1007/BF00120662, https://doi.org/10.1007/BF00120662
17. Pólik, S., Terlaky, T.: A survey of the S-lemma. SIAM Review **49**, 371 – 418 (200)
18. Ramana, M.: An exact duality theory for semidefinite programming and its complexity implications. Mathematical Programming **77**, 129–162 (1997)
19. Renegar, J.: 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. Journal of Symbolic Computation **13**, 255–299 (1992)
20. Schrijver, A.: Theory of Linear and Integer Programming. John Wiley & Sons, Inc., New York, NY, USA (1986)
21. Vavasis, S., Zippel, R.: Proving polynomial-time for sphere-constrained quadratic programming. Tech. rep., Tech. Report 90-1182, Department of Computer Science, Cornell University (1990)
22. Vavasis, S.A.: Quadratic programming is in NP. Information Processing Letters **36**(2), 73 – 77 (1990). https://doi.org/https://doi.org/10.1016/0020-0190(90)90100-C, http://www.sciencedirect.com/science/article/pii/002001909090100C
23. Waki, H., Nakata, M., Muramatsu, M.: Strange behaviors of interior-point methods for solving semidefinite programming problems in polynomial optimization
24. Ye, Y.: A new complexity result on minimization of a quadratic function with a sphere constraint. In: Floudas, A., Pardalos, P. (eds.) Recent Advances in Global Optimization, pp. 19–31. Princeton University Press, Princeton (1992)