Advances in Applied Mathematics 156 (2024) 102670

Contents lists available at ScienceDirect

Advances in Applied Mathematics

journal homepage: www.elsevier.com/locate/yaama

On the complexity of analyticity in semi-definite optimization

Saugata Basu[a], Ali Mohammad-Nezhad[b,*]

[a] *Department of Mathematics, Purdue University, West Lafayette, IN 47905, USA*
[b] *Department of Statistics and Operations Research, University of North Carolina at Chapel Hill, Chapel Hill, NC 27599, USA*

ARTICLE INFO

Article history:
Received 23 February 2023
Received in revised form 18 October 2023
Accepted 18 January 2024
Available online xxxx

MSC:
primary 14P10
secondary 90C22, 90C51

Keywords:
Semi-definite optimization
Central path
Real univariate representation
Quantifier elimination
Newton-Puiseux theorem

ABSTRACT

It is well-known that the central path of semi-definite optimization, unlike linear optimization, has no analytic extension to $\mu = 0$ in the absence of the strict complementarity condition. In this paper, we consider a reparametrization $\mu \mapsto \mu^\rho$, with ρ being a positive integer, that recovers the analyticity of the central path at $\mu = 0$. We investigate the complexity of computing ρ using algorithmic real algebraic geometry and the theory of complex algebraic curves. We prove that the optimal ρ is bounded by $2^{O(m^2+n^2m+n^4)}$, where n is the matrix size and m is the number of affine constraints. Our approach leads to a symbolic algorithm, based on the Newton-Puiseux algorithm, which computes a feasible ρ using $2^{O(m+n^2)}$ arithmetic operations.

Contents

* Corresponding author.
E-mail addresses: sbasu@purdue.edu (S. Basu), alimn@unc.edu (A. Mohammad-Nezhad).

https://doi.org/10.1016/j.aam.2024.102670
0196-8858/

1. Introduction

1.1. *Semi-definite optimization*

We denote by $\mathbb{S}^n$ the inner product space of $n \times n$ symmetric matrices with entries in $\mathbb{R}$ and with the inner product $\langle C, X\rangle = \mathrm{Tr}(CX)$. A pair of primal-dual *semi-definite optimization* (SDO) problems is defined as

$$\text{(P)} \qquad v_p^* := \inf_{X \in \mathbb{S}^n} \left\{\langle C, X\rangle \mid \langle A^i, X\rangle = b_i, \quad i = 1, \dots, m, \ X \succeq 0\right\},$$

$$\text{(D)} \qquad v_d^* := \sup_{(y,S) \in \mathbb{R}^m \times \mathbb{S}^n} \Big\{b^T y \mid \sum_{i=1}^m y_i A^i + S = C, \ S \succeq 0, \ y \in \mathbb{R}^m\Big\},$$

where $A^i \in \mathbb{S}^n$ for $i = 1, \dots, m$, $C \in \mathbb{S}^n$, $b \in \mathbb{R}^m$, and $\succeq 0$ means positive semi-definite. A primal-dual vector (X, y, S) is called a *solution* if $(X, y, S) \in \mathrm{Sol(P)} \times \mathrm{Sol(D)}$, where

$$\mathrm{Sol(P)} := \Big\{X \mid \langle A^i, X\rangle = b_i, \quad i = 1, \dots, m, \quad X \succeq 0, \quad \langle C, X\rangle = v_p^*\Big\},$$

$$\mathrm{Sol(D)} := \left\{(y,S) \mid \sum_{i=1}^{m} y_i A^i + S = C, \quad S \succeq 0,\ b^T y = v_d^*\right\}.$$

Notation 1. We adopt the notation $(\cdot,\cdot,\cdots,\cdot)$ to represent vectors or side by side arrangement of matrices. We sometimes identify a symmetric matrix $X = (X_{ij})_{n\times n}$ with a column vector x by stacking the columns of the matrix on the top of each other, i.e., we use the vector isomorphism

$$\begin{aligned} \mathrm{vec}: \mathbb{S}^n &\to \mathbb{R}^{n^2} \\ X &\mapsto \big(X_{11},\ldots,X_{1n},X_{21},\ldots,X_{2n},\ldots,X_{n1},\ldots,X_{nn}\big)^T. \end{aligned} \tag{1.1}$$

Following this notation, we also define $\mathbf{A} := \big(\mathrm{vec}(A^1),\ldots,\mathrm{vec}(A^m)\big)^T$.

1.2. Central path

SDO problems can be solved "efficiently" using path-following interior point methods (IPMs) [35], where the *central path* plays a prominent role. The central path is an analytic semi-algebraic function $\xi(\mu): (0,\infty) \to \mathbb{S}^n \times \mathbb{R}^m \times \mathbb{S}^n$ whose graph $(\mu, \xi(\mu))$ satisfies

$$\big\{\mathbf{A}\,\mathrm{vec}(X) = b,\ \mathbf{A}^T y + \mathrm{vec}(S - C) = 0,\ \mathrm{vec}(XS - \mu I_n) = 0,\ X, S \succ 0\big\}, \tag{1.2}$$

where I_n is the identity matrix of size n, and $\succ 0$ means positive definite. For every fixed positive μ, following Notation 1, there exists a unique $(X(\mu), y(\mu), S(\mu))$, so-called a *central solution*, satisfying (1.2) [14, Theorem 3.1]. The analyticity of the central path is immediate from the application of the analytic implicit function theorem to the nonsingular Jacobian at a central solution [14, Theorem 3.3]. Due to its semi-algebraicity and the boundedness of $\xi\,|_{(0,1]}$ [14, Lemma 3.2], the central path converges[1] as $\mu \downarrow 0$ [23, Theorem A.3] to a solution (X^{**}, y^{**}, S^{**}) in the relative interior of the solution set [18, Lemma 4.2], see also [4, Page 301] for an alternative proof.

Definition 1.1. A solution (X, y, S) is called *strictly complementary* if $X + S \succ 0$. The *strict complementarity condition* is said to hold if there exists a strictly complementary solution for (P) − (D).

The following assumption is made throughout to guarantee the existence of the central path. This also guarantees that Sol(P) × Sol(D) is non-empty and compact [46, Corollary 4.2].

Assumption 1. The matrices A^i for $i = 1,\ldots,m$ are linearly independent, and there exists a feasible (X, y, S) such that $X, S \succ 0$.

[1] The first proof of convergence was given in [23, Theorem A.3] based on the curve selection lemma [30, Lemma 3.1].

The central path in case of SDO is analytic at $\mu = 0$ if and only if the limit point of the central path is strictly complementary [18,22]. Unfortunately, the failure of analyticity impairs the convergence rate of path-following IPMs, see e.g., [50]. This problem has been extensively studied for linear optimization, linear complementarity problems, and also SDO in the presence of the strict complementarity condition. We will survey some of these results in Section 3. Our paper addresses the case for SDO regardless of the strict complementarity condition.

Notation 2. Using the identification (1.1), the limit point (X^{**}, y^{**}, S^{**}) and a central solution $(X(\mu), y(\mu), S(\mu))$ are identified by vectors $v^{**} := (x^{**}; y^{**}; s^{**})$ and $v(\mu) := (x(\mu); y(\mu); s(\mu))$, respectively. Furthermore, the coordinates of the central path are denoted by $v_i(\mu)$ for $i = 1, \dots, \bar{n}$, where

$$\bar{n} := m + 2n^2.$$

Notation 3. The indeterminates of the polynomials defining the semi-algebraic set (1.2) are denoted by $V_1, \dots, V_{\bar{n}}$.

2. Main results

In this paper, we explore the issue of analyticity in the absence of the strict complementarity condition. Our main motivation behind studying the analyticity of the central path is the following key question, as originally stated in [37, Page 519]. This is the analog of the problem on the central path in the case of linear complementarity problems [43,44].

Problem 1. Does there exist an integer $\rho > 0$ such that $\xi(\mu^\rho)$ is analytic at $\mu = 0$?

We should indicate that an affirmative answer to Problem 1 has been already provided in [24, Section 2.2], where ρ is the cycle number of the central path. It is also stated in [24] that the cycle number of the central path can be determined using the endgame technique in [33,34], see also [7, Chapter 3]. In this paper, we adopt a symbolic approach to explicitly derive ρ from the Puiseux expansions of the polynomials in a semi-algebraic description of the central path. Furthermore, we investigate the complexity of computing a feasible ρ and prove an upper bound on the optimal value of ρ.

2.1. Upper bound on the ramification index

For the purpose of complexity analysis, we assume the integrality of the data in (P) − (D).

Assumption 2. The entries in A^i for $i = 1, \dots, m$, b, and C are all integers.

Notation 4. A bound on the bitsizes of the entries of A^i, C, b is denoted by τ.

In Section 5.2, we show that ρ attains its optimal value at the least common multiple of the ramification indices of the Puiseux expansions of $v_i(\mu)$, which we denote by q, see Notation 2. As a consequence, we show that $\rho \in \mathbb{Z}_+ q$, i.e., any positive integer multiple (≥ 1) of the ramification index would be also a feasible solution to Problem 1. In particular, we prove an upper bound on the optimal ρ.

Theorem 1. *The optimal ρ is the least common multiple of the ramification indices of the Puiseux expansions of $v_i(\mu)$ for $i = 1, \ldots, \bar{n}$. Furthermore, the optimal ρ is bounded by $2^{O(m^2+n^2m+n^4)}$.*

Remark 1. If we also take into account $m = O(n^2)$ from Assumption 1 (because $A_1, \ldots, A_m$ are assumed to be linearly independent), then the optimal ρ is $2^{O(n^4)}$.

Remark 2 *(Designing higher-order IPMs).* Our analytic reparametrization has the advantage that it is independent of the strict complementarity condition. In the words of the author in [22], this approach might be helpful in designing higher-order IPMs for SDO, and second-order conic optimization, with better local convergence than regular primal-dual IPMs.

2.2. A symbolic procedure for computing ρ

Our main contribution is a symbolic procedure, see Algorithm 2, for computing a feasible ρ in Problem 1. Using algorithmic real algebraic geometry and the theory of complex algebraic curves, we propose a symbolic algorithm, based on the Newton-Puiseux algorithm, which computes a feasible ρ using $2^{O(m+n^2)}$ arithmetic operations, see Algorithm 2. In the sequel, we prove that ρ from Algorithm 2 is bounded by $2^{2^{O(m+n^2)}}$. The following theorem summarizes one of the main results of this paper.

Theorem 2. *Given the central path equations in (1.2) with coefficients in $\mathbb{Z}$, Algorithm 2 computes a feasible ρ using $2^{O(m+n^2)}$ arithmetic operations, where ρ is bounded by $2^{2^{O(m+n^2)}}$.*

2.3. Outlines of the procedures and proofs

We now briefly state the ideas behind our symbolic algorithm and the proof of our main results.

In order to prove Theorem 1, we use degree bounds from the parameterized bounded algebraic sampling [5, Algorithm 12.18] and the quantifier elimination (see Theorem 3), and then we apply the result of the Newton-Puiseux theorem (see Proposition 4.3).

In the next step, we elaborate on the proof technique of Theorem 1 to develop a symbolic algorithm (Algorithm 2) for computing ρ. Our symbolic algorithm consists of the following basis elements in order:

- Computing a real univariate representation of the central path (Algorithm 1);
- Developing a formula which describes the graph of the i^{th} coordinate of the central path based on the real univariate representation;
- Applying quantifier elimination to the preceding formula to develop a quantifier-free $\mathcal{P}_i$-formula;
- Applying the univariate sign determination to identify $P_i \in \mathcal{P}_i$ whose zero set contains the graph of the i^{th} coordinate of the central path;
- Applying the Newton-Puiseux algorithm (Algorithm 2) to P_i to compute a feasible ρ.

Algorithm 1 invokes the parameterized bounded algebraic sampling [5, Algorithm 12.18] and the quantifier elimination algorithm [5, Algorithm 14.5] to compute the real univariate representation of the central path for sufficiently small μ, see Lemma 5.2. The output is an $(\bar{n}+3)$-tuple of polynomials in $\mathbb{Z}[\mu, T]$ along with a Thom encoding σ which describes the tail end of the central path, see Section 4.1. By applying the quantifier elimination algorithm to a quantified formula derived from the output of Algorithm 1 (i.e., real univariate representations, see (5.6)), and then applying the univariate sign determination algorithm [5, Algorithm 10.13], Algorithm 2 identifies a polynomial $P_i \in \mathbb{Z}[\mu, V_i]$, for $i = 1, \dots, \bar{n}$, whose zero set contains the graph of the i^{th} coordinate of the central path. Algorithm 2 invokes a symbolic Newton-Puiseux algorithm from [49, Algorithm 1] (see Proposition 4.2) to compute ramification indices of all Puiseux expansions of $P_i = 0$ near $\mu = 0$, for every $i = 1, \dots, \bar{n}$, which converge to the i^{th} coordinate of the limit point of the central path. Here, we also utilize the real univariate representation of the limit point of the central path from [4, Algorithm 3.2]. As a consequence, Algorithm 2 outputs a feasible ρ by computing the least common multiple, over $i = 1, \dots, \bar{n}$, of the product of all distinct ramification indices corresponding to the above Puiseux expansions of $P_i = 0$. The reason for taking the "product" of all ramification indices in Algorithm 2 will be made clear in Section 6.3.

The proof of Theorem 2 is determined based on the complexity of the parameterized bounded algebraic sampling, the quantifier elimination, and the symbolic Newton-Puiseux algorithm in [49, Algorithm 1]. Although Theorem 1 gives a singly exponential upper bound on ρ, in Algorithm 2 we can only guarantee a doubly exponential upper bound on a feasible ρ, because we take the product of all ramification indices.

Remark 3. Notice that a feasible ρ can be immediately derived using the degree of P_i with respect to V_i, and without the use of Newton-Puiseux algorithm in Algorithm 2. However, our goal here is to compute the best feasible ρ, if not optimal. This is also important for computational optimization purposes, because higher values of ρ will result in ill-conditioning of the Jacobian matrix of the central path equations, see also [24, Remark 2].

Remark 4. We should indicate that Algorithm 2 will return the optimal ρ when the branch containing the graph of the i^{th} coordinate of the central path is isolated from the other branches for every $i = 1, \dots, \bar{n}$. In particular, Algorithm 2 returns the optimal ρ if P_i for all $i = 1, \dots, \bar{n}$ are irreducible over $\mathbb{C}\{\mu\}$.

The rest of this paper is organized as follows. In Section 3, we review prior results on the complexity of SDO, convergence, and analyticity of the central path in cases of linear optimization, linear complementarity problems, and SDO. In Section 4, we provide the preliminaries to real algebraic geometry, the theory of complex algebraic curves, and the central path. Our main results are presented in Sections 5 and 6. In Section 5.1, we present the basis of Algorithm 1 for the real univariate representation of the central path, when μ is sufficiently small. In Section 5.2, we explain our theoretical approach and prove Theorem 1. In Section 6, we present Algorithm 2 and then prove its complexity stated in Theorem 2. Finally, we end with concluding remarks and topics for future research in Section 7.

3. Prior and related work

3.1. Complexity

The convex nature of SDO by no means implies polynomial solvability, in contrast to linear optimization. In the bit/real number model of computation, the complexity of SDO and polynomial optimization is well-known: there is no polynomial-time algorithm yet for an exact solution of these classes of optimization problems, see [3, Section 4.2] or [38,39]. In the bit model of computation, a semi-definite feasibility problem either belongs to $\mathbf{NP} \cap \mathbf{co} - \mathbf{NP}$ or it does not belong to $\mathbf{NP} \cup \mathbf{co} - \mathbf{NP}$ [38]. In the real number model of computation [12], a semi-definite feasibility problem belongs to $\mathbf{NP} \cap \mathbf{co} - \mathbf{NP}$. Thus, the intrinsic non-linearity of SDO makes it no easier to solve than a general polynomial optimization problem. In terms of algorithmic real algebraic geometry, there exists an algorithm to describe a primal-dual solution of SDO using

$$\max\left\{(n+m)^{O(n^2)}, n^{O(m)}\right\}$$

arithmetic operations, see [5, Algorithm 14.9] and [11, Proposition A1(5)]. Under Assumption 1, this bound improves to $2^{O(m+n^2)}$ [4, Theorem 3.9].

3.2. Convergence

On the computational optimization side, there exist efficient primal-dual IPM solvers to compute an approximate solution of SDO [14,35]. However, even for an approximate solution, one can find well-structured pathological instances which IPM solvers either fail to solve or solve at a very slow convergence rate, see e.g., [50]. By analogy with linear optimization, this poor performance can be linked to analytic or algebro-geometric properties of the central path [8,9,15,16,18,22,23,29]. To mention but a few, there is a body of research efforts that deal with limiting behavior of the central path under the stronger condition of strict complementarity, see Definition 1.1. Among other outstanding results, it is well-known that the central path is analytic at $\mu = 0$ [22, Theorem 1], and converges to the limit point $\left(X^{**}, y^{**}, S^{**}\right)$ at the rate of 1 [29, Theorem 3.5]:

$$\|X(\mu) - X^{**}\| = O(\mu) \text{ and } \|S(\mu) - S^{**}\| = O(\mu). \tag{3.1}$$

This in turn accounts for the superlinear convergence of IPMs. On the other hand, both the analyticity at $\mu = 0$ and the Lipschitzian bounds (3.1) fail to hold in the absence of the strict complementarity condition [18], see also Example 4. In [4], the authors investigated the degree and the convergence rate of the central path from the perspective of algorithmic real algebraic geometry [5]. The authors provided a lower bound on the convergence rate of the central path.

Proposition 3.1 *(Theorem 1.1 in [4]). Let (X^{**}, y^{**}, S^{**}) be the limit point of the central path. Then for sufficiently small μ we have*

$$\|X(\mu) - X^{**}\| = O(\mu^{1/\gamma}) \text{ and } \|S(\mu) - S^{**}\| = O(\mu^{1/\gamma}), \tag{3.2}$$

where $\gamma = 2^{O(m+n^2)}$.

3.3. Analyticity

Variants of Problem 1 have been also studied for linear optimization and linear complementarity problems, see e.g., [20,32,43,44]. For linear complementarity problems with no strictly complementary solution, the central path with reparametrization $\mu \mapsto \mu^2$ can be analytically extended to $\mu = 0$ [43,44]. This is mainly due to the fact that variables along the central path have magnitudes $O(1)$, $O(\mu)$, or $O(\sqrt{\mu})$ [25]. However, such a classification does not necessarily hold for SDO, as shown in [31, Theorem 3.8]. In fact, the only studies of Problem 1 for SDO are either under the assumption that a strictly complementary solution exists [22,37] or under very restrictive conditions [36].

Very recently, Hauenstein et al. [24] adopted numerical algebraic geometry techniques (adaptive precision path tracking, endgames, projective spaces, see e.g., [7,42]) for an accurate solution of SDO (with or without Assumption 1). The central path in [24] is viewed as a bilinear homotopy parameterized by μ and an IPM as a path tracking for this bilinear homotopy. They applied an analytic reparametrization to the central path (using possibly a non-optimal ρ) to improve the performance of the endgame technique.

4. Background

We briefly review the concepts of semi-algebraic sets, power and Puiseux series, complex algebraic curves, and the analyticity of the central path. Our notation for real closed fields, Puiseux series, formal power series, algebraic curves, and semi-definite optimization is consistent with those in [4,5,17,40,47]. For an exposition of algebraic curve theory and algebraic functions, the reader is referred to [10,17,19,26,47].

Definition of complexity By complexity of an algorithm we will mean the number of arithmetic operations in the ring $\mathbb{Z}$ including comparisons needed by the algorithm (see [5, Chapter 8]). The complexity will be bounded in terms of the number of variables, the number of polynomials in the input and the degrees of polynomials. More specifically, the input to Algorithms 1 and 2 is an integral polynomial, see (5.2), formed by taking the sum of squares of polynomials in (1.2).

4.1. Puiseux series, real closed fields and semi-algebraic sets

In this section we recall some relevant notions from real algebraic geometry (the reader can consult [5, Chapter 2] for more details). From now on, for an integral domain D, we denote by $\mathrm{D}[Y_1, \dots, Y_\ell]_{\leq d}$ the subset of polynomials in the ring $\mathrm{D}[Y_1, \dots, Y_\ell]$ with degrees $\leq d$. Furthermore, $\mathrm{D}(Y_1, \dots, Y_\ell)$ denotes the field of fractions of $\mathrm{D}[Y_1, \dots, Y_\ell]$.

Notation 5. Let K be a field of characteristic zero. A polynomial $P \in \mathrm{K}[X]$ is called *separable* if $\gcd(P, P') \in \mathrm{K} \setminus \{0\}$, where $\gcd(P, P')$ denotes the greatest common divisor of P and its derivative P'. If there is no non-constant polynomial $A \in \mathrm{K}[X]$ such that A^2 divides P, then P is called *square-free*.

If K is a field with characteristic zero, then P is separable if and only if it is square-free.

4.1.1. Puiseux series

A *Puiseux series* with coefficients in $\mathbb{C}$ (resp. $\mathbb{R}$) is a Laurent series with fractional exponents, i.e., a series of the form $\sum_{i=r}^{\infty} c_i \varepsilon^{i/q}$ where $c_i \in \mathbb{C}$ (resp. $c_i \in \mathbb{R}$), $i, r \in \mathbb{Z}$, and q is a minimal positive integer, which is called the *ramification index* of the Puiseux series. Note that the minimality of q indicates that for every prime divisor p of q there exists an index i with $c_i \neq 0$ such that i is not divided by p.

Puiseux series appear naturally in algebraic geometry if we want to express the roots of a polynomial $F(X, Y)$, parametrized by X in a neighborhood of 0. In this paper, they appear in the proof of Theorem 1, when we express the roots of a polynomial $P_i \in \mathbb{Z}[\mu, V_i]$ near $\mu = 0$, where the zero set of P_i contains the graph of the i^{th} coordinate of the central path.

The set of Puiseux series in ε with coefficients in $\mathbb{C}$ (resp. $\mathbb{R}$) is a field, which we denote by $\mathbb{C}\langle\langle\varepsilon\rangle\rangle$ (resp. $\mathbb{R}\langle\langle\varepsilon\rangle\rangle$). It is a classical fact that the field $\mathbb{C}\langle\langle\varepsilon\rangle\rangle$ (resp. $\mathbb{R}\langle\langle\varepsilon\rangle\rangle$) is algebraically closed (resp. real closed).

The subfield of $\mathbb{R}\langle\langle\varepsilon\rangle\rangle$ of elements which are algebraic over $\mathbb{R}(\varepsilon)$ is called the field of algebraic Puiseux series with coefficients in $\mathbb{R}$, and is denoted by $\mathbb{R}\langle\varepsilon\rangle$. It is the real closure of the ordered field $\mathbb{R}(\varepsilon)$ in which ε is positive but smaller than every positive element of $\mathbb{R}$. An alternative description of $\mathbb{R}\langle\varepsilon\rangle$ is that it is the field of germs of semi-algebraic functions to the right of the origin. Thus, each element of $\mathbb{R}\langle\varepsilon\rangle$ is represented by a continuous semi-algebraic function $(0, t_0) \to \mathbb{R}$ (see [5, Chapters 2 and 3]), and this is the reason why the field $\mathbb{R}\langle\varepsilon\rangle$ plays an important role in the study of germs of semi-algebraic curves (for example, the germ of the central path which is a semi-algebraic curve). We let $o(\cdot)$ denote the order of a Puiseux series, and it is defined as $o(\sum_{i=r}^{\infty} c_i\varepsilon^{i/q}) = r/q$ if $c_r \neq 0$, see [5, Section 2.6]. We denote by $\mathbb{R}\langle\varepsilon\rangle_b$ the subring of $\mathbb{R}\langle\varepsilon\rangle$ of elements which are bounded over $\mathbb{R}$ (i.e. all Puiseux series in $\mathbb{R}\langle\varepsilon\rangle$ whose orders are non-negative). We denote by $\lim_\varepsilon : \mathbb{R}\langle\varepsilon\rangle_b \to \mathbb{R}$ a ring homomorphism which maps a bounded Puiseux series $\sum_{i=0}^{\infty} c_i\varepsilon^{i/q}$ to c_0 (i.e. to the value at 0 of the continuous extension of the corresponding curve).

In terms of germs, the elements of $\mathbb{R}\langle\varepsilon\rangle_b$ are represented by semi-algebraic functions $(0, t_0) \to \mathbb{R}$ which can be extended continuously to 0, and $\lim_\varepsilon$ maps such an element to the value at 0 of the continuous extension.

4.1.2. Real closed fields

While for the most part we will be concerned with the field of real numbers, at some points we will need to consider the non-Archimedean real closed extensions of $\mathbb{R}$ – namely, the field of algebraic Puiseux series with coefficients in $\mathbb{R}$. Recall from [5, Chapter 2] that a real closed field R is an ordered field in which every positive element is a square and every polynomial having an odd degree has a root in R.

Given a real closed field R and a finite set $\mathcal{P} \subset \mathrm{R}[Y_1, \ldots, Y_\ell]$, a *quantifier-free $\mathcal{P}$-formula* $\Phi(Y_1, \ldots, Y_\ell)$ with coefficients in R is a Boolean combination of atoms $P > 0$, $P = 0$, or $P < 0$ where $P \in \mathcal{P}$, and $\{Y_1, \ldots, Y_\ell\}$ are the *free variables* of Φ. A quantified $\mathcal{P}$-formula is given by

$$\Psi = (\mathrm{Q}_1 X_1) \cdots (\mathrm{Q}_k X_k)\ \Phi(X_1, \ldots, X_k, Y_1, \ldots, Y_\ell),$$

in which $\mathrm{Q}_i \in \{\forall, \exists\}$ are quantifiers and Φ is a quantifier-free $\mathcal{P}$-formula with $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k, Y_1, \ldots, Y_\ell]$. A formula with no free variable is called a *sentence*. The set of all $(y_1, \ldots, y_\ell) \in \mathrm{R}^\ell$ satisfying Ψ is called the R-realization of Ψ, and it is denoted by $\mathcal{R}(\Psi, \mathrm{R}^\ell)$. A $\mathcal{P}$-*semi-algebraic* subset of R^ℓ is defined as the R-realization of a quantifier-free $\mathcal{P}$-formula.

It is a classical result due to Tarski [45] that the first order theory of real closed fields is decidable and admits quantifier elimination. Thus every quantified formula is equivalent modulo the theory of real closed fields to a quantifier-free formula. Later in the paper we will use an effective version of this theorem [5, Theorem 14.16] equipped with complexity estimates, as stated below.

Theorem 3 *(Quantifier Elimination). Let $\mathcal{P} \subset \mathrm{R}[X_{[1]}, \ldots, X_{[\omega]}, Y]_{\leq d}$ be a finite set of s polynomials, where $X_{[i]}$ is a block of k_i variables, and Y is a block of ℓ variables. Consider the quantified formula*

$$\Psi(Y) = (Q_1 X_{[1]}) \cdots (Q_\omega X_{[\omega]})\ \Phi(X_{[1]}, \ldots, X_{[\omega]}, Y)$$

where Φ is a quantifier-free $\mathcal{P}$-formula. Then there exists a quantifier-free formula

$$\Theta(Y) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} \Big(\bigvee_{n=1}^{N_{ij}} \mathbf{sign}(P_{ijn}(Y)) = \sigma_{ijn} \Big)$$

equivalent to Ψ, where $P_{ijn}(Y)$ are polynomials in the variables Y, $\sigma_{ijn} \in \{-1, 0, 1\}$, and

$$\mathbf{sign}(P_{ijn}(Y)) := \begin{cases} -1 & P_{ijn}(Y) < 0, \\ 0 & P_{ijn}(Y) = 0, \\ 1 & P_{ijn}(Y) > 0. \end{cases}$$

Furthermore, we have

$$\begin{aligned} I &\le s^{(k_\omega+1)\cdots(k_1+1)(\ell+1)} d^{O(k_\omega)\cdots O(k_1)O(\ell)}, \\ J_i &\le s^{(k_\omega+1)\cdots(k_1+1)} d^{O(k_\omega)\cdots O(k_1)}, \\ N_{ij} &\le d^{O(k_\omega)\cdots O(k_1)}, \end{aligned}$$

and the degrees of the polynomials $P_{ijn}(y)$ are bounded by $d^{O(k_\omega)\cdots O(k_1)}$. Moreover, there exists an algorithm ([5, Algorithm 14.5] (Quantifier Elimination)) to compute $\Theta(Y)$ with complexity

$$s^{(k_\omega+1)\cdots(k_1+1)(\ell+1)} d^{O(k_\omega)\cdots O(k_1)O(\ell)}$$

in D, where D denotes the ring generated by the coefficients of the polynomials in $\mathcal{P}$. If $\mathrm{D} = \mathbb{Z}$ and τ denotes an upper bound on bitsizes of $\mathcal{P}$, then the bitsizes of the integers in the intermediate computations and the output are bounded by $\tau d^{O(k_\omega)\cdots O(k_1)O(\ell)}$.

We also state here the complexity of the quantifier elimination for deciding the truth or falsity of a sentence from [5, Theorem 14.14].

Theorem 4 *(General Decision). Let $\mathcal{P} \subset \mathrm{R}[X_{[1]}, \ldots, X_{[\omega]}]_{\le d}$ be a finite set of s polynomials, where $X_{[i]}$ is a block of k_i variables. Given a sentence Ψ, there exists an algorithm which decides the truth of Ψ using*

$$s^{(k_\omega+1)\cdots(k_1+1)} d^{O(k_\omega)\cdots O(k_1)}$$

arithmetic operations in D, where D denotes the ring generated by the coefficients of the polynomials in $\mathcal{P}$.

4.1.3. Sign conditions, univariate representations, and Thom encodings

In our algorithms we will need to represent points symbolically whose coordinates are algebraic over the ground field R. We follow the representation used in the book [5].

Let R be a real closed field. Given a finite family $\mathcal{P} \subset \mathrm{R}[Y_1, \ldots, Y_\ell]$, a *sign condition* on $\mathcal{P}$ is an element of $\{-1, 0, 1\}^{\mathcal{P}}$, i.e., a mapping $\mathcal{P} \to \{-1, 0, 1\}$. The *realization of a sign condition* σ *on a set* $Z \subset \mathrm{R}^\ell$ is defined as

$$\mathcal{R}(\sigma, Z) := \Big\{ y \in Z \mid \bigwedge_{P \in \mathcal{P}} \mathbf{sign}(P(y)) = \sigma(P) \Big\}.$$

If $\mathcal{R}(\sigma, Z) \neq \emptyset$, then σ is said to be *realized by* $\mathcal{P}$ *on* Z. The set of all sign conditions realized by $\mathcal{P}$ on Z is denoted by $\mathrm{SIGN}(\mathcal{P}, Z)$.

An *ℓ-univariate representation* is an $(\ell + 2)$-tuple of polynomials $u = \big(f, g_0, \ldots, g_\ell\big) \in \mathrm{R}[T]^{\ell+2}$, where f and g_0 are coprime. A *real ℓ-univariate representation* of an $x \in \mathrm{R}^\ell$ is a pair (u, σ) of an ℓ-univariate representation u and a *Thom encoding* σ of a real root t_σ of f such that

$$x = \left(\frac{g_1(t_\sigma)}{g_0(t_\sigma)}, \ldots, \frac{g_\ell(t_\sigma)}{g_0(t_\sigma)} \right) \in \mathrm{R}^\ell.$$

Let $\mathrm{Der}(f) := \big\{ f, f^{(1)}, f^{(2)}, \ldots, f^{(\deg(f))} \big\}$ denote a list of polynomials in which $f^{(i)}$ for $i > 0$ is the formal i^{th}-order derivative of f and $\deg(f)$ stands for the degree of f. The Thom encoding σ of t_σ is a sign condition on $\mathrm{Der}(f)$ such that $\sigma(f) = 0$.

The notion of Thom encoding of real roots of a polynomial will be extensively used in this paper. The following proposition [5, Proposition 2.27] indicates that for any $P \in \mathrm{R}[X]$ and a root $x \in \mathrm{R}$ of P, the sign condition σ realized by $\mathrm{Der}(P)$ at x characterizes the root x.

Proposition 4.1 *(Thom's Lemma). Let $P \subset \mathrm{R}[X]$ be a univariate polynomial and $\sigma \in \{-1, 0, 1\}^{\mathrm{Der}(P)}$. Then the realization of the sign condition σ is either empty, a point, or an open interval.*

4.2. Local parametrization of complex algebraic curves

In this section, we recall basic definitions of affine and projective complex algebraic curves and some facts about their local parametrizations that will play a role later in the paper.

4.2.1. Algebraic curves and local parametrization

An *algebraic* subset of $\mathbb{C}^\ell$ is the zero set of a set $\mathcal{P}$ of polynomials in $\mathbb{C}[Y_1, \ldots, Y_\ell]$. We denote

$$\mathbf{zero}(\mathcal{P}, \mathbb{C}^\ell) := \Big\{ y \in \mathbb{C}^\ell \mid \bigwedge_{P \in \mathcal{P}} P(y) = 0 \Big\}.$$

As a special case, an *affine complex algebraic curve* $\mathcal{C}$ is defined as the zero set of a non-constant bivariate polynomial $F \in \mathbb{C}[X, Y]$, i.e.,

$$\mathcal{C} := \mathbf{zero}(F, \mathbb{C}^2) = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}. \tag{4.1}$$

If $G \in \mathbb{C}[X, Y, Z]$ is a non-zero homogeneous polynomial we call the subset of $\mathbb{P}^2(\mathbb{C})$

$$\mathcal{D} := \{(x : y : z) \in \mathbb{P}^2(\mathbb{C}) \mid G(x, y, z) = 0\}$$

projective complex algebraic curve.

Let $\mathbb{C}[[T]]$ be the ring of formal power series in T over $\mathbb{C}$, and let $\mathbb{C}((T))$ denote its field of fractions. Let $\phi = \sum_{i=r}^{\infty} c_i T^i \in \mathbb{C}((T))$, where $c_i \in \mathbb{C}$ and $r \in \mathbb{Z}$. If $c_r \neq 0$, the integer r is defined to be the order of ϕ, denoted by $o(\phi) = r$. If $\phi = 0$, we define $o(\phi) = \infty$. We call a *projective local parametrization* of $\mathcal{D}$ a point $(\phi) := \big(\phi_1(T) : \phi_2(T) : \phi_3(T)\big) \in \mathbb{P}^2\big(\mathbb{C}((T))\big)$ such that

$$G\big(\phi_1(T), \phi_2(T), \phi_3(T)\big) = 0,$$

and for every non-zero $\psi \in \mathbb{C}((T))$ it holds that $\psi \cdot \phi_i \notin \mathbb{C}$ for some i. Given an affine algebraic curve $\mathcal{C}$ and a projective local parametrization for its projective closure $\mathcal{C}^*$ (defined by the homogenization of F in (4.1)), we define an *affine local parametrization* of $\mathcal{C}$ as

$$(\phi_1(T)/\phi_3(T), \phi_2(T)/\phi_3(T)) \in \mathbb{C}((T))^2.$$

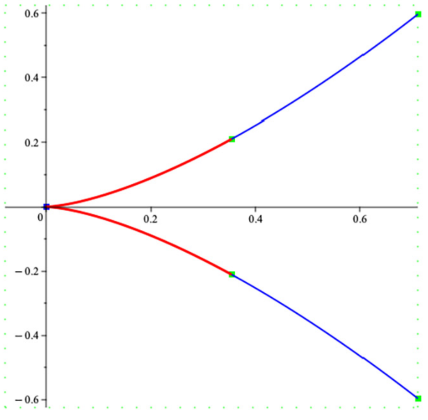
If $\min_{i \in \{1,2,3\}}\{o(\phi_i)\} = 0$,[2] then the *center* of a projective local parametrization is defined to be $(\phi_1(0) : \phi_2(0) : \phi_3(0))$. Furthermore, if $o(\phi_3) = 0$, then $(\phi_1(T)/\phi_3(T), \phi_2(T)/\phi_3(T))$ is an affine local parametrization of $\mathcal{C}$ with a finite affine center.

A local parametrization of $\mathcal{D}$ is called *reducible* if $\phi_i \in \mathbb{C}((T^s))$ for some integer $s > 1$ and every $i = 1, 2, 3$. Two local parametrizations $(\phi_1 : \phi_2 : \phi_3)$ and $(\psi_1 : \psi_2 : \psi_3)$ are called *equivalent* if there exists a $\varphi \in \mathbb{C}((T))$ with $o(\varphi) = 1$ such that $\phi_i = \psi_i(\varphi)$ for $i = 1, 2, 3$. A *place* of $\mathcal{C}$ (resp. $\mathcal{D}$) is an equivalence class of all its affine (resp. projective) irreducible local parametrizations.

The center of a place is the common center of its local parameterizations. A place of $\mathcal{C}$ with a center at a finite affine point p is often referred to as a *branch* of $\mathcal{C}$ at p, i.e., the set of all points $(\phi_1(t), \phi_2(t)) \in \mathcal{C}$ for t in a neighborhood of zero, where ϕ_1 and ϕ_2 are germs[3] of holomorphic functions at zero.

[2] Such a projective local parametrization always exists [47, Page 94].

[3] A germ of holomorphic functions at x_0 means an equivalence class of all holomorphic functions which yield the same values in a neighborhood of x_0.



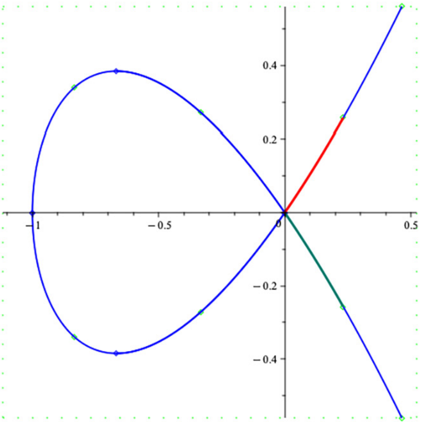


Fig. 1. The branches of cusp (left) and nodal cubic (right) at **0**.

Example 1. The affine complex algebraic curve (so-called cusp) defined by

$$F_1(X, Y) = Y^2 - X^3$$

has a single branch at $(0, 0)$, which is locally parameterized by (t^2, t^3). On the other hand, the complex curve (so-called nodal cubic) defined by

$$F_2(X, Y) = Y^2 - X^3 - X^2 = (Y - X\sqrt{X+1})(Y + X\sqrt{X+1})$$

has 2 branches at $(0, 0)$, which are locally parameterized by $(t, \phi_1(t))$ and $(t, \phi_2(t))$, see Fig. 1. Notice that $\phi_1(t)$ and $\phi_2(t)$ are power series expansions of $X\sqrt{X+1}$ and $-X\sqrt{X+1}$, respectively.

We should also note that a point of a parametrization might be a center for more than one branch of $\mathcal{C}$.

Example 2 *(Example 2.66 in [40]).* Consider the algebraic curve $\mathcal{C}$ defined by

$$F(X, Y) = Y^5 - 4Y^4 + 4Y^3 + 2X^2Y^2 - XY^2 + 2X^2Y + 2XY + X^4 + X^3.$$

The curve $\mathcal{C}$ has two branches at **0**. The roots corresponding to these branches have ramification indices 1 and 2, see Fig. 2.

Notation 6. In this paper, a complex number is denoted by $a + b\sqrt{-1}$, where $a, b \in \mathbb{R}$, and $\exp(it) = \cos(t) + i\sin(t)$ is the complex exponential function. We use upper case letters for indeterminates of polynomials and (convergent) power series, while lower case letters are used for the arguments of (holomorphic) functions.

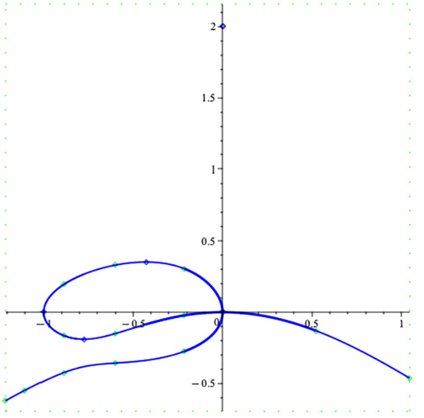


Fig. 2. In this example, **0** is the center of two places of $\mathcal{C}$.

4.2.2. Newton-Puiseux theorem

Let $\mathbb{C}\{T\}$ denote the ring of convergent power series in T, and assume without loss of generality that $(0,0) \in \mathcal{C}$. If $\partial F/\partial Y(0,0) \neq 0$, then the implicit function theorem provides an affine local parametrization $(T, \phi(T))$ of $F = 0$ with center $(0,0)$, where $\phi(T) \in \mathbb{C}\{T\}$. In general, the Newton-Puiseux theorem [47, Theorem 3.1 of Chapter IV] shows that an affine complex algebraic curve $\mathcal{C}$ has an affine local parameterization of the type $(T^q, \phi(T))$ for some positive integer q. The proof of the Newton-Puiseux theorem is constructive and uses the Newton polygon to show that the field of Puiseux series $\mathbb{C}\langle\langle T\rangle\rangle = \bigcup_{s=1}^{\infty} \mathbb{C}((T^{1/s}))$ is algebraically closed.

Proposition 4.2 *(Theorems 3.2 and 4.1 and Section 4.2 of Chapter IV in [47]). Let*

$$F(X,Y) = a_0 + a_1 Y + \cdots + a_d Y^d \in \mathbb{C}[X][Y], \tag{4.2}$$

where $a_d \neq 0$. There exist d (not necessarily distinct) Puiseux series $\psi_i(X) \in \mathbb{C}\langle X\rangle$ for $i = 1, \ldots, d$ such that

$$F(X,Y) = a_d \prod_{i=1}^{d} (Y - \psi_i).$$

There exist k places of the curve $F = 0$ with center at $(0,0)$ corresponding to each ψ_i with a positive order and multiplicity k. Conversely, corresponding to each place (ϕ_1, ϕ_2) of $\mathcal{C}$ with center at $(0,0)$ there exist $o(\phi_1)$ roots of $F = 0$ with identical positive orders.

If $a_d(0) = 0$ in Proposition 4.2, then $F(0,Y) = 0$ has less than d roots (including multiplicity). In that case, there exist Puiseux series ψ_i in Proposition 4.2 with negative orders, and they correspond to places with center at infinity.

4.2.3. Weierstrass polynomial

The constructive proof of the Newton-Puiseux theorem yields an iterative procedure to compute ramification indices of the Puiseux expansions in Proposition 4.2, see Section 6.1. A specialized version of Proposition 4.2 can be obtained if F is assumed to be an irreducible Weierstrass polynomial. A polynomial $W \in \mathbb{C}\{X\}[Y]$ is called a *Weierstrass polynomial* of degree d if

$$W = a_0 + a_1 Y + \cdots + a_{d-1} Y^{d-1} + Y^d,$$

where $a_j(0) = 0$ for $j = 0, \ldots, d-1$. Given an irreducible W, the local parametrization of Proposition 4.2 can be explicitly written in terms of the degree of W.

Proposition 4.3 *(Section 7.8 in [17]). Let W be irreducible over $\mathbb{C}\{X\}$. Then there exists an affine local parametrization $(T^d, \phi(T))$ with $\phi(T) \in \mathbb{C}\{T\}$, that describes the only branch of the curve $W = 0$ at $(0,0)$. Furthermore, $W = 0$ has d distinct roots near $x = 0$, and they are all described by*

$$\psi_i(X) = \sum_{j=1}^{\infty} c_j \Big(\exp\big(2\pi\sqrt{-1}(i-1)/d\big) X^{1/d} \Big)^j, \qquad i = 1, \ldots, d.$$

Example 3. The condition on the irreducibility of W is an integral part of Proposition 4.3 and cannot be dropped. For instance, the reducible Weierstrass polynomial

$$W(X,Y) = (Y^3 - X^2)(Y^2 - X^3) = Y^5 - X^3Y^3 - X^2Y^2 + X^5 \in \mathbb{C}[X,Y]$$

has roots $Y = X^{\frac{2}{3}}$ and $Y = \pm X^{\frac{3}{2}}$, while there is no local parametrization of the type $(T^5, \phi(T))$ around $x = 0$.

Let $\mathbb{C}\{X, Y\}$ denote the ring of convergent power series in X and Y. Then Proposition 4.3 can be applied to any $F \in \mathbb{C}[X,Y]$ with $F(0,Y) \neq 0$. This fact immediately follows from the *Weierstrass preparation theorem.*

Proposition 4.4 *(Section 6.7 in [17]). Suppose that $F \in \mathbb{C}\{X,Y\}$ such that*

$$F(0,Y) \neq 0 \quad \textit{and} \quad o(F(0,Y)) = d.$$

Then F can be uniquely written as $F = UW$, where $U \in \mathbb{C}\{X,Y\}$ is a unit element and $W \in \mathbb{C}\{X\}[Y]$ is a Weierstrass polynomial of degree d. In particular, if $F \in \mathbb{C}\{X\}[Y]$, then $U \in \mathbb{C}\{X\}[Y]$ holds as well.

Remark 5. Locally, a branch of $\mathcal{C}$ at a point (say $\mathbf{0} \in \mathcal{C}$) is the germ of the zero set of an irreducible factor of F over $\mathbb{C}\{X\}$, see [17, Page 123]. For instance, $F_1 = 0$ in Example 1 has one branch at $\mathbf{0}$ because F_1 is irreducible over $\mathbb{C}\{X\}$. On the other hand, F_2 has two irreducible factors in $\mathbb{C}\{X\}[Y]$ and thus $F_2 = 0$ has two branches at $\mathbf{0}$.

4.3. Analyticity of the central path

The higher-order derivatives of the central path with respect to μ are all well-defined, by the implicit function theorem. More concretely, the i^{th}-order derivatives of the central path for $i \geq 1$ can be obtained by solving

$$\begin{aligned} \langle A^i, X^{(i)} \rangle &= 0, \qquad i = 1, \ldots, m, \\ \sum_{i=1}^{m} y_i^{(i)} A^i + S^{(i)} &= 0, \\ X^{(i)} S(\mu) + X(\mu) S^{(i)} &= \begin{cases} I_n & i = 1, \\ -\sum_{j=1}^{i-1} \binom{i}{j} X^{(j)} S^{(i-j)}, & i > 1, \end{cases} \end{aligned}$$

where $(X^{(i)}, y^{(i)}, S^{(i)})$ denotes the i^{th}-order derivative, and the coefficient matrix is always non-singular. The analyticity of the central path at $\mu = 0$ follows analogously if the Jacobian is non-singular at the unique solution, as a result of strict complementarity and non-degeneracy conditions, see [2, Theorem 3.1] and [21, Theorem 3.1].

Obviously, the bounds (3.1) and (3.2) do not imply the boundedness of the derivatives as $\mu \downarrow 0$, see e.g., Example 4. In fact, derivatives of the central path converge if and only if the strict complementarity condition holds [18, Section 6] and [22, Theorem 1]. For instance, consider an orthogonal basis $Q := \big(Q_{\mathcal{B}}, Q_{\mathcal{T}}, Q_{\mathcal{N}}\big)$ for the 3-tuple of mutually orthogonal subspaces[4]

$$\Big(\operatorname{Col}(X^{**}), \operatorname{Col}(S^{**}), (\operatorname{Col}(X^{**}) + \operatorname{Col}(S^{**}))^{\perp}\Big),$$

where $\operatorname{Col}(\cdot)$ denotes the column space of a matrix. If the strict complementarity fails, then $Q_{\mathcal{T}} \neq \{\mathbf{0}\}$, and thus the first-order derivative of the central path fails to converge, because

$$Q_{\mathcal{T}}^T X^{(1)}(\mu) Q_{\mathcal{T}} Q_{\mathcal{T}}^T S(\mu) Q_{\mathcal{T}} + Q_{\mathcal{T}}^T X(\mu) Q_{\mathcal{T}} Q_{\mathcal{T}}^T S^{(1)}(\mu) Q_{\mathcal{T}} = I_{n_{\mathcal{T}}},$$

while both $Q_{\mathcal{T}}^T S(\mu) Q_{\mathcal{T}} \to 0$ and $Q_{\mathcal{T}}^T X(\mu) Q_{\mathcal{T}} \to 0$ as $\mu \downarrow 0$.

Example 4. The minimization of a linear objective function over the *3-elliptope*, see Fig. 3, can be cast into a SDO problem:

$$\min \left\{ 4x - 4y - 2z \mid \begin{pmatrix} 1 & x & y \\ x & 1 & z \\ y & z & 1 \end{pmatrix} \succeq 0 \right\}. \tag{4.3}$$

The unique solution of (4.3) is given by

[4] The subspaces $\operatorname{Col}(X^{**})$ and $\operatorname{Col}(S^{**})$ are orthogonal by the condition $XS = 0$.

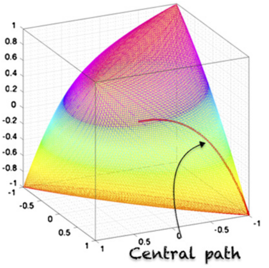


Fig. 3. The derivatives of the central path fail to exist at $\mu = 0$.

$$X^* = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, \quad y^* = (-4,\ -1,\ -1)^T, \quad S^* = \begin{pmatrix} 4 & 2 & -2 \\ 2 & 1 & -1 \\ -2 & -1 & 1 \end{pmatrix}, \tag{4.4}$$

which is not strictly complementary.

The graph of $X_{12}(\mu)$ can be described as the set of all (μ, t) with $\mu > 0$ satisfying

$$F(\mu, T) := 2T^3 + (2 - \mu/2)T^2 - (\mu + 2)T - 2 = 0, \tag{4.5}$$
$$\begin{pmatrix} 1 & T & -T \\ T & 1 & -2T^2 + \mu T/2 + 1 \\ -T & -2T^2 + \mu T/2 + 1 & 1 \end{pmatrix} \succ 0,$$
$$\begin{pmatrix} \mu - 4T & 2 & -2 \\ 2 & -2/T - 1 & -1 \\ -2 & -1 & -2/T - 1 \end{pmatrix} \succ 0.$$

By the uniqueness of (4.4), we must have $X_{12}(\mu) \to -1$ as $\mu \downarrow 0$. Then it follows from (4.5) that

$$X_{12}^{(1)}(\mu) = \frac{X_{12}^2(\mu)/2 + X_{12}(\mu)}{6X_{12}^2(\mu) + (4 - \mu)X_{12}(\mu) - (\mu + 2)} \to \infty$$

as $\mu \downarrow 0$. This explains the tangential convergence of the central path in Fig. 3.

The algebraic curve $F = 0$ in Example 4 has two branches at $(0, -1)$ and $(0, 1)$, as demonstrated by Fig. 4. By invoking the "Algcurves" package in Maple[5] we can numerically compute the Puiseux expansions of all roots of $F = 0$ near $\mu = 0$ as follows

$$\begin{aligned} T_1(\mu) &= -1 + \frac{\sqrt{8}}{8}\mu^{\frac{1}{2}} + \frac{1}{32}\mu - \frac{11\sqrt{8}}{2048}\mu^{\frac{3}{2}} - \frac{3}{512}\mu^2 - \frac{121\sqrt{8}}{1048576}\mu^{\frac{5}{2}} \\ &\quad + \frac{15}{32768}\mu^3 + \frac{19405\sqrt{8}}{268435456}\mu^{\frac{7}{2}} + \cdots, \\ T_2(\mu) &= -1 - \frac{\sqrt{8}}{8}\mu^{\frac{1}{2}} + \frac{1}{32}\mu + \frac{11\sqrt{8}}{2048}\mu^{\frac{3}{2}} - \frac{3}{512}\mu^2 + \frac{121\sqrt{8}}{1048576}\mu^{\frac{5}{2}} \end{aligned}$$

[5] Available at https://www.maplesoft.com/.

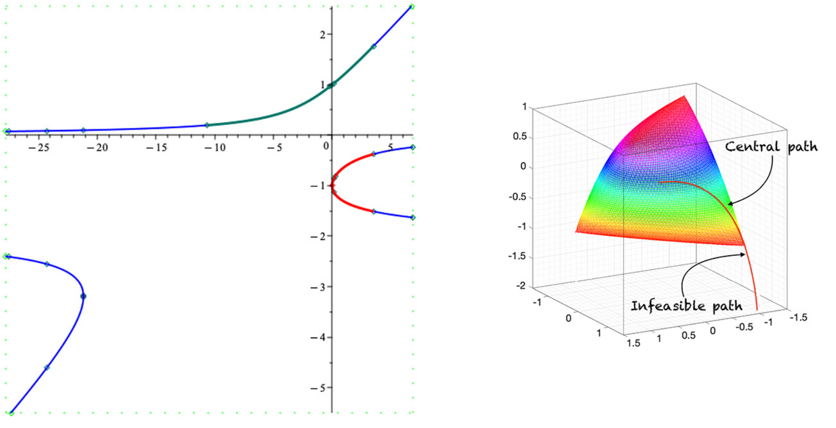


Fig. 4. $T_1(\mu)$ (the upper red segment of the branch) is the expansion of $X_{12}(\mu)$; $T_2(\mu)$ (the lower red segment of the branch) is the expansion of a semi-algebraic function converging to X_{12}^{**} from the exterior of the positive semi-definite cone; $T_3(\mu)$ (the green segment) is the expansion of a semi-algebraic function converging to an infeasible value. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

$$
\begin{aligned}
&+\frac{15}{32768}\mu^3-\frac{19405\sqrt{8}}{268435456}\mu^{\frac{7}{2}}+\cdots,\\
T_3(\mu)&=1+\frac{3}{16}\mu+\frac{3}{256}\mu^2-\frac{15}{16384}\mu^3-\frac{15}{262144}\mu^4+\frac{345}{16777216}\mu^5\\
&-\frac{21}{33554432}\mu^6-\frac{1869}{4294967296}\mu^7+\cdots,
\end{aligned}
$$

where T_1 is the Puiseux expansion of the X_{12} coordinate of the central path. The order of the Puiseux series T_1 indicates the non-Lipschitzian convergence

$$\|X(\mu)-X^{**}\|=O(\sqrt{\mu})\quad\text{and}\quad\|S(\mu)-S^{**}\|=O(\sqrt{\mu}).$$

5. Reparametrization of the central path

Although the Lipschitzian bounds (3.1) fail to exist in the absence of the strict complementarity condition, we can still exploit local information around the center point to recover the analyticity of the central path. This remedial action can be applied to Example 4, where the ramification index of T_1 suggests the local parametrization $(\mu^2,\phi(\mu))$ of the curve $F=0$ around $\mu=0$, where

$$\phi(\mu)=-1+\frac{\sqrt{8}}{8}\mu+\frac{1}{32}\mu^2-\frac{11\sqrt{8}}{2048}\mu^3-\frac{3}{512}\mu^4-\frac{121\sqrt{8}}{1048576}\mu^5+\frac{15}{32768}\mu^6+\ldots,$$

see Fig. 5. Thus, one may adopt a reparametrization $\mu\mapsto\mu^\rho$ under which the central path is analytic at $\mu=0$, where ρ is a positive integer multiple of the ramification index of the Puiseux expansion.

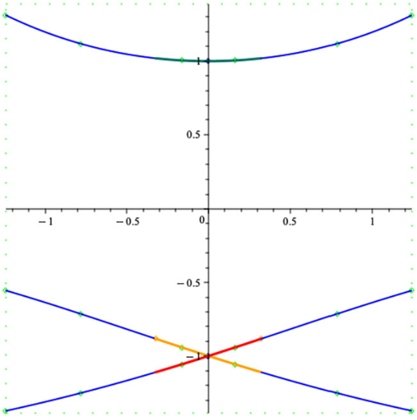


Fig. 5. The algebraic curve (4.5) after the reparametrization $\mu \to \mu^2$. The reparametrized central path (red segment) is analytic at $\mu = 0$.

In the worst-case scenario, the magnitude of the optimal ρ depends exponentially on n.

Example 5 *(Example 3.3 in [14]).* Consider the following SDO problem in dual form (D):

$$\max\left\{-y_n \mid S = \begin{pmatrix} 1 & y_1 & y_2 & \dots & y_{n-1} \\ y_1 & y_2 & 0 & \dots & 0 \\ y_2 & 0 & y_3 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ y_{n-1} & 0 & \dots & 0 & y_n \end{pmatrix} \succeq 0\right\},$$

which has a unique solution (y^{**}, S^{**}) with $y_i^{**} = 0$ for $i = 1, \dots, n$. In this case, $y_2(\mu) = O(\mu^{2^{-(n-2)}})$, which implies a reparametrization $\mu \mapsto \mu^\rho$ with optimal $\rho \geq 2^{n-2}$.

In view of Example 4, our goal is to adopt a semi-algebraic approach to identify bivariate polynomials, analogous to $F(\mu, T)$ in (4.5), that describe the tail end of the central path in a coordinate-wise manner. All we need then are the ramification indices of the Puiseux expansions corresponding to the roots of these bivariate polynomials around $\mu = 0$, which give rise to a feasible ρ for Problem 1.

The basis elements of our semi-algebraic approach are the real univariate representation of the central path for sufficiently small μ, the quantifier elimination (see Theorem 3), and the Newton-Puiseux theorem (see Proposition 4.2), which we elaborate on in Sections 5.1 and 5.2.

5.1. Real univariate representation of the central path

The central path system (1.2) can be considered as a μ-infinitesimally deformed polynomial system $\mathcal{G} \subset \mathbb{Z}[\mu][V_1, \ldots, V_{\bar{n}}]$, i.e., a μ-infinitesimal deformation of the polynomial system

$$\big\{\mathbf{A}\,\mathrm{vec}(X) = b,\ \mathbf{A}^T y + \mathrm{vec}(S - C) = 0,\ \mathrm{vec}(XS) = 0\big\},$$

whose zeros belong to $\mathbb{C}\langle\mu\rangle^{\bar{n}}$. Without loss of generality, we consider the restriction of the central path to the interval $(0, 1]$. Recall that the central path is uniformly bounded, i.e., there exists, see Lemma 5.1, a rational $\varepsilon > 0$ such that

$$\|(X(\mu), y(\mu), S(\mu))\| \leq 1/\varepsilon, \qquad \forall \mu \in (0, 1]. \tag{5.1}$$

Since we are interested in the central path, which is bounded over $(0, 1]$, we only characterize the bounded zeros of $\mathcal{G}$ in $\mathbb{R}\langle\mu\rangle^{\bar{n}}$, which are defined as

$$\mathbf{zero}_b\big(\mathcal{G}, \mathbb{R}\langle\mu\rangle^{\bar{n}}\big) := \mathbf{zero}\big(\mathcal{G}, \mathbb{R}\langle\mu\rangle^{\bar{n}}\big) \cap \mathbb{R}\langle\mu\rangle_b^{\bar{n}},$$

where $\mathbb{R}\langle\mu\rangle_b^{\bar{n}}$ denotes the subring of $\mathbb{R}\langle\mu\rangle^{\bar{n}}$ consisting of elements which are bounded over $\mathbb{R}$. The central path for sufficiently small positive μ is a bounded solution of $\mathbf{zero}\big(\mathcal{G}, \mathbb{R}\langle\mu\rangle^{\bar{n}}\big)$. Therefore, the limit point (X^{**}, y^{**}, S^{**}) is contained in $\lim_\mu \mathbf{zero}_b\big(\mathcal{G}, \mathbb{R}\langle\mu\rangle^{\bar{n}}\big)$.

5.1.1. Parameterized bounded algebraic sampling

Our approach to characterize the bounded zeros of $\mathcal{G}$ is to compute real univariate representation of the central path when μ is sufficiently small; this describes the coordinate $v_i(\mu)$ of the central path as a rational function of μ and the roots of a univariate polynomial. To that end, we define the two polynomials $Q \in \mathbb{Z}[\mu, V_1, \ldots, V_{\bar{n}}]$ and $\tilde{Q} \in \mathbb{Z}[\mu, V_1, \ldots, V_{\bar{n}+1}]$ as follows

$$\begin{aligned} Q &:= \|\mathbf{A}x - b\|^2 + \|\mathbf{A}^T y + s - c\|^2 + \|\mathrm{vec}(XS - \mu I_n)\|^2, \\ \tilde{Q} &:= Q^2 + \big(\varepsilon^2(V_1^2 + \cdots + V_{\bar{n}+1}^2) - 1\big)^2, \end{aligned} \tag{5.2}$$

where ε is defined in (5.1). Notice that for every fixed $\mu \in (0, 1]$, $\mathbf{zero}(\tilde{Q}(\mu), \mathbb{R}^{\bar{n}+1})$ is non-empty (it contains a central solution), and

$$\bigcup_{\mu \in \mathbb{R}} \mathbf{zero}(\tilde{Q}(\mu), \mathbb{R}^{\bar{n}+1})$$

is bounded, because $\mathbf{zero}(\tilde{Q}(\mu), \mathbb{R}^{\bar{n}+1})$ is the intersection of the cylinder based on $\mathbf{zero}(\mathcal{P}_\mu, \mathbb{R}^{\bar{n}})$ and an $\bar{n}$-sphere, where

Algorithm 1 Real univariate representation of the central path.

Input: The polynomial $\tilde{Q} \in \mathbb{Z}[\mu, V_1, \dots, V_{\bar{n}+1}]$.
return The set $\mathcal{U}$ of parametrized univariate representations u and Thom encodings σ of roots of $f \in \mathbb{Z}[\mu][T]$; There exists a real univariate representation (u, σ) with $u \in \mathcal{U}$ which describes the central path for sufficiently small positive μ, see Lemma 5.2.

Procedure:

(A) Generate the set $\mathcal{U}$ of parameterized univariate representations by applying [5, Algorithm 12.18] (Parameterized Bounded Algebraic Sampling) with input $\tilde{Q}$ and parameter μ.
(B) Compute the ordered list of Thom encodings of the roots of f in $\mathbb{R}\langle\mu\rangle$ by applying [5, Algorithm 10.14] (Thom Encoding) to each $f \in \mathbb{Z}[\mu][T]$ in the set $\mathcal{U}$.
(C) Decide which $((f, g), \sigma)$ describes the central path for sufficiently small positive μ by applying [5, Algorithm 14.3] (General Decision) to (5.4).

$$\mathcal{P}_\mu := \left\{ \mathbf{A}\,\mathrm{vec}(X) = b,\ \mathbf{A}^T y + \mathrm{vec}(S - C) = 0,\ \mathrm{vec}(XS - \mu I) = 0 \right\}.$$

The idea here is to utilize the parameterized bounded algebraic sampling algorithm [5, Algorithm 12.18] with input $\tilde{Q}$ to describe, for every $\mu \in \mathbb{R}$, a finite set of sample points that meets every connected component of $\mathbf{zero}\big(\tilde{Q}(\mu), \mathbb{R}^{\bar{n}+1}\big)$, see also [5, Proposition 12.42]. The description of these sample points is given by a set $\mathcal{U}$ of parameterized univariate representations

$$u := (f, g) = \big(f, (g_0, g_1, \dots, g_{\bar{n}+1})\big) \in \mathbb{Z}[\mu, T]^{\bar{n}+3}.$$

We will prove in Lemma 5.2 that for sufficiently small positive μ, there exist a univariate representation u and a real root t_σ of f with Thom encoding σ such that

$$v_i(\mu) = \frac{g_i(\mu, t_\sigma)}{g_0(\mu, t_\sigma)} \in \mathbb{R}, \qquad i = 1 \dots, \bar{n}, \tag{5.3}$$

where $g_0(\mu, t_\sigma) \neq 0$. At the end, the problem of choosing the right $\big((f, g), \sigma\big)$ is a real algebraic geometry problem and can be decided by the quantifier elimination algorithm.

To see this, let $(\hat{X}(\mu), \hat{y}(\mu), \hat{S}(\mu))$ be associated to $((f, g), \sigma)$, and let, without loss of generality, $C_x, C_s \in \mathbb{Z}[\mu][T, \Lambda]$ be the characteristic polynomials of $\hat{X}(\mu)$ and $\hat{S}(\mu)$, respectively. Then $((f, g), \sigma)$ represents the central path, when μ is sufficiently small, if the following two $\mathcal{Q}$-sentences with $\mathcal{Q} \subset \mathbb{Z}[\mu][T, \Lambda]$ are both true (see [5, Proposition 3.17]):

$$\begin{aligned} &(\exists T)(\forall \Lambda)\ \big(\mathbf{sign}(f^{(j)}) = \sigma(f^{(j)}),\ j \in \mathbb{Z}_{\geq 0}\big) \wedge \big(\neg(C_x(T, \Lambda) = 0) \vee (\Lambda > 0)\big), \\ &(\exists T)(\forall \Lambda)\ \big(\mathbf{sign}(f^{(j)}) = \sigma(f^{(j)}),\ j \in \mathbb{Z}_{\geq 0}\big) \wedge \big(\neg(C_s(T, \Lambda) = 0) \vee (\Lambda > 0)\big). \end{aligned} \tag{5.4}$$

Now we can apply [5, Algorithm 14.3] (General Decision) to (5.4).

Algorithm 1 summarizes our symbolic procedure for the real univariate representation of the central path.

5.1.2. Complexity and the proof of correctness

The correctness of Algorithm 1 follows from Theorem 4, and Lemma 5.2 below, and its complexity follows from the complexity of [5, Algorithm 12.18] and [5, Algorithm 14.3]. First, we need the following quantitative result.

Lemma 5.1. *The polynomial* $\tilde{Q}$ *in* (5.2) *has coefficients with bitsizes bounded by* $\tau 2^{O(m+n^2)}$.

Proof. All we need here is the magnitude of $1/\varepsilon$ in $\tilde{Q}$, which is also an upper bound on the norm of central solutions for all $\mu \in (0,1]$, see (5.1). From the central path equations in (1.2) it follows that $\langle X(\mu) - X(1), S(\mu) - S(1)\rangle = 0$, which results in

$$\langle X(\mu), S(1)\rangle + \langle S(\mu), X(1)\rangle = n(\mu + 1).$$

Since the central solutions are positive definite,

$$\langle X(\mu), S(1)\rangle > 0,\ \ \langle S(\mu), X(1)\rangle > 0,$$

and thus for all $\mu \in (0,1]$ we have

$$\langle X(\mu), S(1)\rangle \leq 2n \quad \text{and} \quad \langle S(\mu), X(1)\rangle \leq 2n.$$

Furthermore, the centrality condition $XS = I$ implies that

$$\begin{aligned} \|X(\mu)\| &\leq \frac{2n}{\lambda_{\min}(S(1))} \leq 2n\lambda_{\max}(X(1)), \\ \|S(\mu)\| &\leq \frac{2n}{\lambda_{\min}(X(1))} \leq 2n\lambda_{\max}(S(1)), \end{aligned} \qquad \forall \mu \in (0,1]. \tag{5.5}$$

By the integrality of the data, see Assumption 2, there exists [6, Theorem 1] a ball of radius $r = 2^{\tau 2^{O(m+n^2)}}$ containing every isolated point of $\mathbf{zero}(\mathcal{P}', \mathbb{R}^{\bar{n}})$, including $(X(1), y(1), S(1))$, where

$$\mathcal{P}' := \left\{\mathbf{A}\,\mathrm{vec}(X) = b,\ \mathbf{A}^T y + \mathrm{vec}(S - C) = 0,\ \mathrm{vec}(XS - I_n) = 0\right\}.$$

This also gives an upper bound on $\lambda_{\max}(X(1))$ and $\lambda_{\max}(S(1))$ which, by (5.5), yields

$$\|X(\mu)\|, \|S(\mu)\| = 2^{\tau 2^{O(m+n^2)}}, \qquad \forall \mu \in (0,1].$$

Now the result follows when we choose $1/\varepsilon = 2^{\tau 2^{O(m+n^2)}}$. $\square$

Lemma 5.2. *The polynomials* $(f, g) \in \mathcal{U}$ *have degree* $O(1)^{\bar{n}+1}$ *and their coefficients have bitsizes* $\tau 2^{O(m+n^2)}$, *where* τ *is an upper bound on the bitsizes of the entries in* A^i, C, *and b. Furthermore, there exist a Thom encoding σ, $u \in \mathcal{U}$, and $\gamma = 2^{\tau 2^{O(m+n^2)}}$ such that (u, σ) describes the central path for all $\mu \in (0, 1/\gamma)$.*

Proof. The output of [5, Algorithm 12.18] is a set of $(\bar{n}+3)$-tuples of polynomials (f, g) in $\mathbb{Z}[\mu, T]$ of degree $O(\deg_V(\tilde{Q}))^{\bar{n}+1}$, where $\deg_V(\tilde{Q}) = 8$ is the degree of $\tilde{Q}$ with respect to V. The bound on the bitsizes of the coefficients follows from Lemma 5.1 and [5, Algorithm 12.18].

Since a central solution is an isolated solution[6] of $\mathbf{zero}\big(Q(\mu), \mathbb{R}^{\bar{n}}\big)$, the projections of the real points associated to u to the first $\bar{n}$ coordinates contain the central path when $\mu \in (0, 1]$. Since there are finitely many $(\bar{n}+3)$-tuples of polynomials in $\mathcal{U}$, there must exist $(f, g) \in \mathcal{U}$ and $\mu_0 > 0$ such that (f, g) describes the central solutions for all $\mu \in (0, \mu_0)$.

Let $((f, g), \sigma)$ be a real univariate representation for which (5.4) is true (i.e., it describes the central path for sufficiently small μ), where $(f, g) \in \mathbb{Z}[\mu, T]^{\bar{n}+2}$ (after discarding $g_{\bar{n}+1}$), and consider the following formulas:

$$\Phi_x(\mu) = (\exists T)(\forall \Lambda)\ \big(\mathbf{sign}(f^{(j)}) = \sigma(f^{(j)}),\ j \in \mathbb{Z}_{\geq 0}\big) \wedge \big(\neg(C_x(T, \Lambda) = 0) \vee (\Lambda > 0)\big),$$

$$\Phi_s(\mu) = (\exists T)(\forall \Lambda)\ \big(\mathbf{sign}(f^{(j)}) = \sigma(f^{(j)}),\ j \in \mathbb{Z}_{\geq 0}\big) \wedge \big(\neg(C_s(T, \Lambda) = 0) \vee (\Lambda > 0)\big).$$

Notice that $\mathcal{R}(\Phi_x, \mathbb{R}) \cap \mathcal{R}(\Phi_s, \mathbb{R}) \neq \emptyset$. By Theorem 3, Φ_x and Φ_s are equivalent to quantifier-free $\mathcal{P}_x$- and $\mathcal{P}_s$-formulas, where $\mathcal{P}_x, \mathcal{P}_s \subset \mathbb{Z}[\mu]$ are of degrees $2^{O(m+n^2)}$. By [5, Lemma 10.3] and Lemma 5.1, the absolute values of all non-zero real roots of polynomials in $\mathcal{P}_x, \mathcal{P}_s$ are bigger than $1/\gamma$, where $\gamma = 2^{\tau 2^{O(m+n^2)}}$. This completes the proof. $\square$

Now, we can prove the complexity of Algorithm 1.

Theorem 5. *There exist $\gamma = 2^{\tau 2^{O(m+n^2)}}$ and an algorithm with complexity $2^{O(m+n^2)}$ to compute $((f, g), \sigma)$ which represents the central path for all $\mu \in (0, 1/\gamma)$.*

Proof. The complexity of Step A in Algorithm 1 is $2^{O(m+n^2)}$, which is determined by [5, Algorithm 12.18] and noting that $\mathrm{tdeg}_\mu(\tilde{Q}) = 6$, where $\mathrm{tdeg}_\mu(\tilde{Q})$ is the total degree of monomials in $\tilde{Q}$ containing μ. The complexity of Step B is determined by the number of parametrized univariate representations (f, g) in $\mathcal{U}$, which is $O(\deg(\tilde{Q}))^{\bar{n}+1}$ and the complexity of [5, Algorithm 10.14] applied to every $(f, g) \in \mathcal{U}$. Step C decides the truth or falsity of (5.4) for every real univariate representation $((f, g), \sigma)$. By Theorem 4, all this can be done using $2^{O(m+n^2)}$ arithmetic operations. The second part of the theorem is the direct application of Lemma 5.2. $\square$

[6] This follows from the implicit function theorem.

5.2. Puiseux expansion of the central path

Existence of the reparametrization in Problem 1 can be shown by invoking the output of Algorithm 1 and Proposition 4.2. By substituting the roots $t \in \mathbb{R}\langle\mu\rangle$ of $f(\mu, T) = 0$, it is easy to see that the i^{th} coordinate of the central path can be represented by $\sum_{j=0}^{\infty} c_{ij}\mu^{j/q_i}$ with $c_{ij} \in \mathbb{R}$, and $q_i \in \mathbb{Z}$ (see [47, Theorem 1.2 of Chapter IV]).[7] Then one can choose ρ to be (an integer multiple of) the least common multiple of q_i over $i \in \{1, \dots, \bar{n}\}$.

An alternative approach, which we will follow in Section 6, can be given in terms of a semi-algebraic description of the coordinates. More precisely, let $((f, g), \sigma)$ with $(f, g) \in \mathcal{U}$ being the real univariate representation of the central path for all sufficiently small μ, see Theorem 5. Then the graph of $v_i(\mu)$, when μ is sufficiently small, can be described by the following quantified formula

$$(\exists T)\ \big(V_i g_0 - g_i = 0\big) \wedge \big(\mathbf{sign}(f^{(j)}(\mu, T)) = \sigma(f^{(j)}),\ j = 0, 1, \dots\big). \tag{5.6}$$

By Theorem 3, (5.6) is equivalent to a quantifier-free $\mathcal{P}_i$-formula with $\mathcal{P}_i \subset \mathbb{Z}[\mu, V_i]$. Furthermore, there exists a polynomial $P_i \in \mathcal{P}_i$ such that $P_i(\mu, v_i(\mu)) = 0$ for sufficiently small μ and $P_i(0, v_i^{**}) = 0$ (because (5.6) describes the graph of a semi-algebraic function). Note that $P_i \in \mathbb{Z}[\mu, V_i]$ in Theorem 3, as the output of the quantifier elimination, is the product of a finite number of polynomials in $\mathbb{Z}[\mu, V_i]$, see e.g., the proof of Lemma 2.5.2 in [13, Page 36]. Therefore, P_i need not be irreducible over $\mathbb{C}$ (or even $\mathbb{R}$). Nevertheless, P_i has an absolutely irreducible factor with real coefficients, whose zero set contains the graph of the i^{th} coordinate of the central path when μ is sufficiently small.

Proposition 5.1. *The polynomial P_i has an absolutely irreducible factor $R_i \in \mathbb{R}[\mu, V_i]$ such that $R_i(\mu, v_i(\mu)) = 0$.*

Proof. Let $R_i \in \mathbb{C}[\mu, V_i]$ be an absolutely irreducible factor of P_i whose zero set contains the graph of the i^{th} coordinate of the central path. Then we assume that R_i can be written as

$$R_i = \mathrm{Re}(R_i) + \sqrt{-1}\,\mathrm{Im}(R_i),$$

where $\mathrm{Re}(R_i), \mathrm{Im}(R_i) \in \mathbb{R}[\mu, V_i]$ are the non-zero real and imaginary parts of R_i obtained from the real and imaginary parts of their coefficients. Then $R_i(\mu, v_i(\mu)) = 0$ indicates that

$$\mathrm{Re}(R_i)(\mu, v_i(\mu)) = \mathrm{Im}(R_i)(\mu, v_i(\mu)) = 0$$

[7] In case of the central path, j must be non-negative, since otherwise the root would be unbounded.

for all sufficiently small positive μ, which in turn implies that $\mathrm{Re}(R_i)$ and $\mathrm{Im}(R_i)$ have a common factor, see e.g., [41, Page 4]. However, this would contradict the absolute irreducibility of R_i. $\square$

Remark 6. For complexity purposes, we do not include any factorization step in Algorithm 2. Instead, we choose P_i to contain only the tail end of the central path, i.e., for sufficiently small positive μ.

Let $P_i := \sum_{j=0}^{d_i} p_{ij}(\mu)V_i^j$ from Theorem 3 applied to (5.6), where $p_{ij}(\mu) \in \mathbb{Z}[\mu]$ and $d_i := \deg_{V_i}(P_i)$. By Proposition 4.2, P_i can be factorized as

$$P_i(\mu, V_i) = p_{id_i}(\mu) \prod_{\ell=1}^{d_i} \big(V_i - \psi_{i\ell}(\mu)\big), \qquad i = 1, \dots, \bar{n}, \tag{5.7}$$

where the ramification index of $\psi_{i\ell}$ is denoted by $q_{i\ell}$. Therefore, there exists a unique (multiple) factor ℓ_i in (5.7) such that

$$v_i(\mu) = \psi_{i\ell_i}(\mu) := \sum_{j=0}^{\infty} c_{ij}\mu^{j/q_{i\ell_i}}, \quad \text{for all sufficiently small } \mu > 0, \tag{5.8}$$

where $c_{ij} \in \mathbb{R}$ and $c_{i0} = v_i^{**}$.

Remark 7. Although $\mathbf{zero}(\tilde{Q}(\mu), \mathbb{R}^{\bar{n}+1})$ is bounded over all μ, not every root of $P_i = 0$ near $\mu = 0$ is bounded, unless $p_{id_i}(0) \neq 0$.

Remark 8. Notice that $\psi_{i\ell_i} \in \mathbb{R}\langle\mu\rangle$ because $v_i(\mu)$ is semi-algebraic [5, Proposition 3.17].

Note that $P_i = 0$ may have more than one branch at $(0, v_i^{**})$, because P_i is not necessarily irreducible over $\mathbb{C}\{\mu\}$,[8] see Example 2. However, one of these branches contains the graph of the i^{th} coordinate of the central path, when μ is sufficiently small, see Proposition 4.2.

Remark 9. By Proposition 4.2, if $\psi_{i\ell_i}$ is not a multiple root of $P_i = 0$, then *exactly* one of the branches of $P_i = 0$ contains the graph of the i^{th} coordinate of the central path, when μ is sufficiently small.

This branch, in analogy with Example 4, is described by a set of $q_{i\ell_i}$ distinct Puiseux expansions, including (5.8),

$$\psi_{ik}(\mu) = \sum_{j=0}^{\infty} c_{ij}\Big(\exp\big(2\pi\sqrt{-1}(k-1)/q_{i\ell_i}\big)\mu^{1/q_{i\ell_i}}\Big)^j, \qquad k = 1, \dots, q_{i\ell_i},$$

[8] Remember that a branch of $P_i = 0$ is the germ of the zero set of an irreducible factor of P_i over $\mathbb{C}\{\mu\}$.

which they all converge to $(0, v_i^{**})$. Thus, letting q_i be the ramification index of $\psi_{i\ell_i}(\mu)$, q the least common multiple of all $q_{i\ell_i}$ over $i \in \{1, \ldots, \bar{n}\}$, and ρ be a positive integer multiple of q, then we get the series

$$\psi_{i\ell_i}(\mu^\rho) \in \mathbb{C}\{\mu\}, \quad i = 1, \ldots, \bar{n},$$

which are all convergent in a neighborhood of $\mu = 0$. This indicates that $v(\mu^\rho)$ is analytic at $\mu = 0$, providing an explicit answer to Problem 1.

Remark 10. We should note that q is well-defined and independent of the P_i and the semi-algebraic description (5.6), see [5, Theorem 3.14].

Remark 11. The authors in [24, Page 4] indicate the analyticity of $v(\mu^\rho)$ near $\mu = 0$ in terms of the cycle number of the central path, see also [24, Remark 2]. However, in contrast to [24], our algorithmic derivation of ρ is explicit in terms of the degrees and Puiseux expansions of the defining polynomials P_i.

Now, we can provide the proof of Theorem 1.

Proof of Theorem 1. By Theorem 3, the quantifier elimination applied to (5.6) returns quantifier-free formulas involving polynomials $P_i \in \mathbb{Z}[\mu, V_i]$ of degrees $2^{O(m+n^2)}$. With no loss of generality, see Section 6, we can assume that

$$P_i(0, V_i) \neq 0, \quad P_i(0, 0) = 0, \quad i = 1, \ldots, \bar{n}.$$

By Proposition 4.4, P_i is the product of a Weierstrass polynomial $W_i \in \mathbb{C}\{\mu\}[V_i]$ of degree $\deg_{V_i}(P_i)$ and a unit $U_i \in \mathbb{C}\{\mu\}[V_i]$. We may also assume that W_i is irreducible over $\mathbb{C}\{\mu\}$ (by only considering the unique component of W_i whose zero set contains the graph of the i^{th} coordinate of the central path, see Remark 5). Now, the application of Proposition 4.3 to W_i implies that

$$q_{i\ell_i} \leq \deg_{V_i}(P_i), \quad i = 1, \ldots, \bar{n}.$$

Finally, we get the result by noting that $\deg_{V_i}(P_i) = 2^{O(m+n^2)}$ and $q \leq \prod_{i=1}^{\bar{n}} q_i$. $\square$

Remark 12. In the presence of the strict complementarity condition, $q = 1$ must be exactly 1, since otherwise the analyticity of the central path would fail at $\mu = 0$ [22, Theorem 1].

Remark 13. We should note that $q_{i\ell_i}$ from two different coordinates need not be identical. For instance, the ramification indices of the coordinates of the central path in Example 5 with $n = 4$ are 1, 2, or 4:

$$X(\mu) = \begin{pmatrix} O(\mu) & 0 & O(\mu^{\frac{3}{4}}) & O(\mu^{\frac{1}{2}}) \\ 0 & O(\mu^{\frac{3}{4}}) & 0 & 0 \\ O(\mu^{\frac{3}{4}}) & 0 & O(\mu^{\frac{1}{2}}) & O(\mu^{\frac{1}{4}}) \\ O(\mu^{\frac{1}{2}}) & 0 & O(\mu^{\frac{1}{4}}) & 1 \end{pmatrix}, \quad y(\mu) = \begin{pmatrix} 0 \\ O(\mu^{\frac{1}{4}}) \\ O(\mu^{\frac{1}{2}}) \\ O(\mu) \end{pmatrix},$$

$$S(\mu) = \begin{pmatrix} 1 & 0 & O(\mu^{\frac{1}{4}}) & O(\mu^{\frac{1}{2}}) \\ 0 & O(\mu^{\frac{1}{4}}) & 0 & 0 \\ O(\mu^{\frac{1}{4}}) & 0 & O(\mu^{\frac{1}{2}}) & 0 \\ O(\mu^{\frac{1}{2}}) & 0 & 0 & O(\mu) \end{pmatrix}.$$

6. A symbolic algorithm based on the Newton-Puiseux theorem

In this section, we address the complexity of computing a feasible ρ using Algorithm 2, which applies the Newton-Puiseux theorem to P_i.

Given the real univariate representation $((f, g), \sigma)$ from Algorithm 1 (after discarding $g_{\bar{n}+1}$), we choose the semi-algebraic description (5.6) and apply the quantifier elimination algorithm to obtain a finite set $\mathcal{P}_i \subset \mathbb{Z}[\mu, V_i]$. We then identify a polynomial $P_i \in \mathcal{P}_i$ such that $P_i(\mu, v_i(\mu)) = 0$ for sufficiently small μ. This can be done by computing $\mathrm{SIGN}(\mathrm{Der}(f), \mathcal{V}_{ij})$, see Section 4.1.3, where

$$\mathcal{V}_{ij} := \mathbf{zero}\Big(g_0^{\deg_{V_i}(R_{ij})} R_{ij}(\mu, g_i/g_0), \mathbb{R}\langle\mu\rangle\Big) \tag{6.1}$$

for every $R_{ij} \in \mathcal{P}_i$ and then checking $\sigma \in \mathrm{SIGN}(\mathrm{Der}(f), \mathcal{V}_{ij})$.

6.1. Newton-Puiseux algorithm

By the proof of the Newton-Puiseux theorem, see [47, Page 98], the roots of $P_i = 0$ near $\mu = 0$ are constructed as

$$\varphi_{is}(\mu) = a_{i1}\mu^{\gamma_{i1}} + a_{i2}\mu^{\gamma_{i1}+\gamma_{i2}} + a_{i3}\mu^{\gamma_{i1}+\gamma_{i2}+\gamma_{i3}} + \cdots,$$

where φ_{is} corresponds to the segment s (described by the equation $y + \gamma_{i1}x = \beta_{i1}$) of the Newton polygon of P_i, $\gamma_{i1} \in \mathbb{Q}$ is the negative of the slope of the segment s of the Newton polygon of P_i, and $a_{i1} \in \mathbb{C}$ is a (multiple) root of a polynomial in $\mathbb{Z}[T]$ by which the terms of the lowest order of μ in the polynomial

$$P_i(\mu, \mu^{\gamma_{i1}}(V_i + T)) \tag{6.2}$$

vanish (see [47, (3.4) on Page 98]). Notice that every segment s of the Newton polygon of P_i determines the order γ_{i1} of a set of Puiseux series, as root(s) of $P_i = 0$ near $\mu = 0$. In particular, for the Puiseux series (5.8) we have $\gamma_{i1} \geq 0$, because $\psi_{i\ell_i}(\mu)$ is convergent.

This procedure continues by forming the Newton polygon for

$$P_i^{(j+1)} := \mu^{-\beta_{ij}} P_i^{(j)}(\mu, \mu^{\gamma_{ij}}(V_i + a_{ij})), \quad j = 1, 2, \dots, \tag{6.3}$$

where $P_i^{(1)} := P_i$, choosing a segment $\gamma_{i(j+1)} > 0$, and finding a (multiple) root $a_{i(j+1)}$ of a polynomial by which the terms of the lowest order of μ in the polynomial

$$P_i^{j+1}(\mu, \mu^{\gamma_{i(j+1)}}(V_i + T)) \tag{6.4}$$

vanish. The multiplicity of a_{ij} decreases monotonically, and it stabilizes at a constant integer after a finite number of iterations, say N_i. Thus, successive γ_{ij} have bounded denominators, and q_i is equal to the smallest common denominator of $\gamma_{i1}, \dots, \gamma_{iN_i}$ (see [47, Page 100]).

Remark 14. The multiplicity of a_{ij} eventually stabilizes at 1 if $P_i = 0$ has no multiple root in $\mathbb{C}\langle\mu\rangle$. By [47, Theorem IV.3.5], this can be guaranteed if

$$\deg_{V_i}(\gcd(P_i, \partial P_i/\partial V_i)) = 0.$$

6.2. Symbolic computation

We apply a symbolic version of the Newton-Puiseux algorithm in [49, Algorithm 1] to compute q_i for all bounded Puiseux expansions of $P_i(\mu, V_i) = 0$ with limit equal to v_i^{**}. The idea of [49, Algorithm 1] is to compute the exponents γ_{ij} [49, Algorithm 1, Step 1] and then carry the roots symbolically using the minimal polynomials $S_{ij} \in \mathbb{Z}[T]$ of a_{ij} [49, Algorithm 1, Step 6] and the minimal polynomials $Z_{ij} \in \mathbb{Z}[T]$ of the primitive elements α_{ij} of the extension field $\mathbb{Q}(a_{i1}, \dots, a_{ij})$, α_{ij} being an algebraic integer such that $\mathbb{Q}(\alpha_{ij}) = \mathbb{Q}(a_{i1}, \dots, a_{ij})$ [49, Algorithm 1, Step 9].

For the purpose of computing the ramification indices, the Newton-Puiseux algorithm in [49, Algorithm 1] continues until a_{ij} becomes a simple root of (6.4). To that end, we replace P_i by $P_i/\operatorname{Cont}_\mu(P_i)$, where $\operatorname{Cont}_\mu(P_i)$ is the content of $P_i \in \mathbb{Z}[\mu][V_i]$, i.e., the greatest common divisor of the coefficients of P_i in $\mathbb{Z}[\mu]$, and we set $P_i := \mu^{\alpha_i} P_i(\mu, V_i/\mu^{\theta_i})$, where α_i and θ_i are non-negative integers satisfying

$$\begin{cases} \alpha_i + o(p_{id_i}) = \theta_i d_i, \\ \alpha_i + o(p_{ij}) \geq j\theta_i, \qquad j = 1, \dots, d_i - 1, \end{cases} \tag{6.5}$$

where $d_i = \deg_{V_i}(P_i)$. This technique [28, Page 247] ensures the boundedness of the roots of $P_i = 0$. We also assume that P_i is a square-free polynomial for every $i = 1, \dots, \bar{n}$, see Remark 14. Notice that if

$$\deg_{V_i}(\gcd(P_i, \partial P_i/\partial V_i)) > 0,$$

then P_i has a multiple factor in $\mathbb{Z}(\mu)[V_i]$ [5, Propositions 4.15 and 4.24], and by [47, Theorem I.9.5] P_i has also a multiple factor in $\mathbb{Z}[\mu, V_i]$. In this case, we can compute the separable part of P_i in $\mathbb{Z}[\mu, V_i]$ (which is also square-free) by applying [5, Algorithm 10.1] to P_i and $\partial P_i/\partial V_i$, see [5, Corollary 10.15].

Proposition 6.1. *The Newton-Puiseux algorithm in [49, Algorithm 1] computes the ramification indices in $2^{O(m+n^2)}$ iterations.*

Proof. The maximum number of iterations follows from the bound

$$N_i \le 4 \deg_\mu(P_i) \deg_{V_i}(P_i)^2$$

in [49, Page 1170]. □

6.3. On computing the optimal ρ

In order to obtain the optimal ρ, one would still need to identify a factor in (5.7) which describes the graph of the i^{th} coordinate of the central path. However, this identification cannot be made by solely using the truncation of a Puiseux expansion (although we can generate as many terms as we want using the technique in [28]). More precisely, the Newton-Puiseux algorithm only computes a truncation of the Puiseux expansion of $v_i(\mu)$, which, in general, will not satisfy (5.3) exactly. On the other hand, we should also recall that $P_i = 0$ may have more than one branch at $(0, v_i^{**})$, because P_i is not necessarily irreducible over $\mathbb{C}\{\mu\}$, see Example 2. Thus, an optimal ρ may not be always obtained using this approach.

To get as smallest feasible ρ as possible, we first check the irreducibility of P_i. If it holds, then $\mathbf{zero}(P_i, \mathbb{C}^2)$ has exactly one branch at $(0, v_i^{**})$, which contains the graph of the i^{th} coordinate of the central path. Otherwise, we identify all branches of $P_i = 0$ at $(0, v_i^{**})$. We use the following technical result in Algorithm 2 to decide whether P_i is irreducible over $\mathbb{C}\{\mu\}$.

Proposition 6.2. *Suppose that all zeros of P_i are bounded and P_i is square-free. Then P_i is irreducible over $\mathbb{C}\{\mu\}$ iff $P_i = 0$ has a Puiseux expansion with a ramification index equal to $\deg_{V_i}(P_i)$.*

Proof. By the assumptions and Proposition 4.2, a Puiseux expansion with ramification index q_{is} implies a branch $(T^{q_{is}}, \phi(T))$ and q_{is} distinct roots of $P_i = 0$. Thus $q_{is} = \deg_{V_i}(P_i)$ implies that $P_i = 0$ has exactly one branch at $(0, v_i^{**})$, since otherwise $P_i = 0$ would have more than $\deg_{V_i}(P_i)$ bounded roots. Analogously, $q_{is} < \deg_{V_i}(P_i)$, implies that $P_i = 0$ must have more than one branch and thus P_i must have more than one factor in $\mathbb{C}\{\mu\}[V_i]$. □

By Proposition 6.2, if P_i is irreducible over $\mathbb{C}\{\mu\}$, then $q_i = \deg_{V_i}(P_i)$. Otherwise, we compute the product of ramification indices over all bounded Puiseux expansions of $P_i = 0$ with limit v_i^{**}, i.e., only segments with slopes $\le -\theta_i$, see (6.5), which yield a Puiseux expansion with $S_{i1}(v_i^{**}) = 0$. Let $(\bar{u}, \bar{\sigma})$ with $\bar{u} := \big(\bar{f}, \big(\bar{g}_0, \bar{g}_1, \dots, \bar{g}_{\bar{n}}\big)\big) \in \mathbb{Z}[T]^{\bar{n}+2}$ be the real univariate representation of v^{**} from [4, Algorithm 3.2], and let

$$\mathcal{V}_i^{**} := \mathbf{zero}\Big(\bar{g}_0^{\deg(S_{i1})} S_{i1}\big(\bar{g}_i/\bar{g}_0\big), \mathbb{R}\Big). \tag{6.6}$$

Then given a truncation of a Puiseux expansion of $P_i = 0$ from [49, Algorithm 1], the truth or falsity of $S_{i1}(v_i^{**}) = 0$ can be decided by computing $\mathrm{SIGN}(\mathrm{Der}(\bar{f}), \{0\})$ if $\gamma_{i1} > \theta_i$ or $\mathrm{SIGN}(\mathrm{Der}(\bar{f}), \mathcal{V}_i^{**})$ if $\gamma_{i1} = \theta_i$ and then checking the inclusion $\bar{\sigma} \in \mathrm{SIGN}(\mathrm{Der}(\bar{f}), \{0\})$ or $\bar{\sigma} \in \mathrm{SIGN}(\mathrm{Der}(\bar{f}), \mathcal{V}_i^{**})$.

Finally, we compute ρ as the least common multiple of all ρ_i, where ρ_i is the product of all distinct q_{is} corresponding to the above Puiseux expansions of $P_i = 0$. The outline of the above procedure is summarized in Algorithm 2.

Remark 15. It is clear that $\rho = \prod_{i=1}^{\bar{n}} (\deg_{V_i}(P_i)!)$ will be a feasible integer for Problem 1. However, analogous to the proof of Theorem 1, our goal is to compute the smallest possible feasible ρ.

Remark 16. It is worth noting that Algorithm 2 outputs the optimal ρ as long as the branch of $P_i = 0$ containing the graph of the i^{th} coordinate of the central path is isolated for every $i = 1, \dots, \bar{n}$. In particular, an optimal ρ is obtained if P_i is irreducible over $\mathbb{C}\{\mu\}$ for all $i = 1, \dots, \bar{n}$.

Example 6. It is easy to see from Fig. 4 that $F = 0$ is not irreducible over $\mathbb{C}\{\mu\}$, because it involves two isolated branches at $(0, -1)$ and $(0, 1)$. However, Algorithm 2 still returns the optimal $\rho = 2$ for Example 4.

6.4. Complexity and the proof of correctness

The correctness of Algorithm 2 follows from the correctness of Algorithm 1, [4, Algorithm 3.2], Theorem 3, and [49, Algorithm 1]. Step D identifies P_i for every $i = 1, \dots, \bar{n}$. Step F guarantees that the roots of $P_i = 0$ are all bounded, and Step G guarantees that the Puiseux expansions of P_i are all distinct. Step H checks the irreducibility of P_i using Proposition 6.2. Step I applies the symbolic Newton-Puiseux algorithm to every segment of the Newton polygon of P_i, if P_i is not irreducible over $\mathbb{C}\{\mu\}$. Step J decides the truth or falsity of $S_{i1}(v_i^{**}) = 0$ for all truncated Puiseux expansions obtained from Step I and thus identifies the branches at $(0, v_i^{**})$.

Now, we can prove Theorem 2. First, we need the following results.

Algorithm 2 Reparametrization based on the Newton-Puiseux theorem.

Input: The polynomial $\tilde{Q} \in \mathbb{Z}[\mu, V_1, \dots, V_{\bar{n}+1}]$; An empty set $\mathcal{L}_i$ for every $i = 1, \dots, \bar{n}$
return A feasible ρ for which $\big(X(\mu^\rho), y(\mu^\rho), S(\mu^\rho)\big)$ is analytic at $\mu = 0$

Procedure:

(A) Apply Algorithm 1 to $\tilde{Q}$ and let the output be $((f, g), \sigma)$.
(B) Apply [4, Algorithm 3.2] to $\tilde{Q}$ and let the output be $((\bar{f}, \bar{g}), \bar{\sigma})$.
(C) For every $i = 1, \dots, \bar{n}$, apply the quantifier elimination algorithm [5, Algorithm 14.5] with input (5.6). Let the output be a finite set $\mathcal{P}_i$ of polynomials in $\mathbb{Z}[\mu, V_i]$.
(D) For every $i = 1, \dots, \bar{n}$ and every $R_{ij} \in \mathcal{P}_i$ apply [5, Algorithm 10.13] (Univariate Sign Determination) with input $g_0^{\deg_{V_i}(R_{ij})} R_{ij}\big(\mu, g_i/g_0\big)$ and $\mathrm{Der}(f)$, and let $\mathrm{SIGN}(\mathrm{Der}(f), \mathcal{V}_{ij})$ be the output, see (6.1). If $\sigma \in \mathrm{SIGN}(\mathrm{Der}(f), \mathcal{V}_{ij})$, then choose R_{ij} as the polynomial whose zero set contains the graph of the i^{th} coordinate of the central path for sufficiently small μ. Set $P_i := R_{ij}$.
(E) For every $i = 1, \dots, \bar{n}$ compute $\mathrm{Cont}_\mu(P_i)$ by applying [5, Algorithm 10.1] iteratively to the coefficients of P_i (as a polynomial in V_i). Then replace P_i by $P_i/\,\mathrm{Cont}_\mu(P_i)$.
(F) For every $i = 1, \dots, \bar{n}$ apply the procedure (6.5) to P_i.
(G) For every $i = 1, \dots, \bar{n}$ apply [5, Algorithm 10.1] with inputs $P_i, \partial P_i/\partial V_i \in \mathbb{Z}[\mu][V_i]$ and replace P_i by its separable part.
(H) For every $i = 1, \dots, \bar{n}$ apply the symbolic Newton-Puiseux algorithm [49, Algorithm 1] to only one segment of the Newton polygon of P_i. If for the given segment the ramification index of the Puiseux expansion is equal to $\deg_{V_i}(P_i)$, then set $\rho_i = \deg_{V_i}(P_i)$. Otherwise, go to Step I.
(I) For every i failing the condition of Step H, apply the symbolic Newton-Puiseux algorithm [49, Algorithm 1] to P_i for the rest of segments s with negative slope of magnitude $\geq \theta_i$, see (6.5). Let the output be q_{is}, γ_{i1}, and the minimal polynomial $S_{i1} \in \mathbb{Z}[T]$.
(J) Given γ_{i1} and S_{i1} for every i from Step I, if $\gamma_{i1} > \theta_i$, then apply [5, Algorithm 10.11] (Sign Determination) with input $\{0\}$ and $\mathrm{Der}(\bar{f})$. If $\gamma_{i1} = \theta_i$, then apply [5, Algorithm 10.13] (Univariate Sign Determination) with input $\bar{g}_0^{\deg(S_{i1})} S_{i1}\big(\bar{g}_i/\bar{g}_0\big)$ and $\mathrm{Der}(\bar{f})$. Let the output be $\mathrm{SIGN}(\mathrm{Der}(\bar{f}), \{0\})$ or $\mathrm{SIGN}(\mathrm{Der}(\bar{f}), \mathcal{V}_i^{**})$, respectively, see (6.6). If $\bar{\sigma} \in \mathrm{SIGN}(\mathrm{Der}(\bar{f}), \{0\})$ or $\bar{\sigma} \in \mathrm{SIGN}(\mathrm{Der}(\bar{f}), \mathcal{V}_i^{**})$, then add s to $\mathcal{L}_i$.
(K) For every i from Step J compute $\rho_i := \prod_{s \in \mathcal{L}_i} q_{is}$. Then compute the least common multiple of ρ_i over $i = 1, \dots, \bar{n}$.

Lemma 6.1 *(Theorem 3.9 in [4]). There exists an algorithm to compute the real univariate representation $(\bar{u}, \bar{\sigma})$ using $2^{O(m+n^2)}$ arithmetic operations, where*

$$\deg(\bar{f}), \deg(\bar{g}) = 2^{O(m+n^2)}.$$

Lemma 6.2. *The ramification indices of Puiseux expansions of $P_i = 0$ can be computed using $2^{O(m+n^2)}$ arithmetic operations.*

Proof. The result is immediate from [49, Theorem 1] and Theorem 3. The total complexity of computing a ramification index [49, Theorem 1] is

$$\big(\deg_{V_i}(P_i) \cdot \deg_\mu(P_i)\big)^{O(1)},$$

where by Theorem 3 we have

$$\deg_{V_i}(P_i), \deg_\mu(P_i) = 2^{O(m+n^2)}. \quad \square$$

Proof of Theorem 2. The overall complexity of Algorithm 2 is dominated by the complexity of Algorithm 1, [4, Algorithm 3.2], and the complexity of the quantifier elimination [5, Algorithm 14.5]. By Lemmas 5.2 and 6.1, Theorem 3, and Theorem 5, Steps A to C run with complexity $2^{O(m+n^2)}$, and the quantifier elimination applied to (5.6) outputs quantifier-free formulas with polynomials of degree $2^{O(m+n^2)}$ and coefficients of bitsizes $\tau 2^{O(m+n^2)}$. The complexity of Steps D to G and Steps J and K depend on $\bar{n}$, $\mathrm{card}(\mathcal{P}_i)$, $\deg(R_{ij})$, $\deg(f)$, $\deg(\bar{f})$, $\mathrm{card}(\mathrm{Der}(\bar{f}))$, and $\mathrm{card}(\mathrm{Der}(f))$, and they are all $2^{O(m+n^2)}$. Steps H and I apply the Newton-Puiseux algorithm to segments of the Newton polygon of P_i which, by Lemma 6.2, have the total complexity $2^{O(m+n^2)}$. The doubly exponential bound on the magnitude of ρ follows from the proof of Theorem 1, $\deg_{V_i}(P_i) = 2^{O(m+n^2)}$, and the inequality

$$\prod_{s \in \mathcal{L}_i} q_{is} \leq \left\lceil e^{\frac{\deg_{V_i}(P_i)}{e}} \right\rceil. \quad \square$$

Finally, we should note that there exist procedures (e.g., based on Hensel's lemma [27, Theorem 4.2.5], Proposition 4.4, and the Newton-Puiseux algorithm) for factorization of polynomials over $\mathbb{C}\{\mu\}$, see e.g., [1,48]. However, such factorization procedures over $\mathbb{C}\{\mu\}$ would only generate a finite number of terms from each factor. Thus, even with the presence of such procedures, we would not be able to identify the branch of the central path, because only a truncation of the convergent power series, i.e., the coefficients of an irreducible factor, would be available to us.

7. Concluding remarks and future research

In this paper, we studied the analyticity of the central path of SDO in the absence of the strict complementarity condition. In essence, the superlinear convergence of primal-dual IPMs rests on the analyticity of the central path at the limit point, which is guaranteed under the stronger condition of strict complementarity. By means of the semi-algebraic description (5.6) and the Puiseux expansions of the roots of $P_i = 0$ for every $i = 1, \ldots, \bar{n}$, we developed a symbolic algorithm to compute a reparametrization $\mu \mapsto \mu^\rho$ such that $\big(X(\mu^\rho), y(\mu^\rho), S(\mu^\rho)\big)$ is analytic at $\mu = 0$, in which ρ attains its optimal value at q, i.e., the least common multiple of ramification indices of the Puiseux expansions of $v_i(\mu)$. Our semi-algebraic approach provides an upper bound $2^{O(m^2+n^2m+n^4)}$ on q and leads to Algorithm 2 for computing a feasible ρ. Algorithm 2 computes a feasible ρ, using $2^{O(m+n^2)}$ arithmetic operations, as the least common multiple of $\prod_s q_{is}$, where the product is over all distinct ramification indices corresponding to bounded Puiseux expansions with limit v_i^{**}. We proved that a feasible ρ from Algorithm 2 is bounded by $2^{2^{O(m+n^2)}}$. In case that the polynomials P_i are all irreducible over $\mathbb{C}\{\mu\}$, Algorithm 2 outputs the optimal ρ.

Real analyticity of a semi-algebraic function Broadly speaking, Algorithm 2 can be modified to guarantee the analyticity of any semi-algebraic function. In contrast to complex analyticity, which can be verified using the Cauchy-Riemann conditions, checking the real analyticity is a harder problem. Suppose that the graph of a bounded semi-algebraic function $f : \mathbb{R} \to \mathbb{R}$ is described by a quantified formula Ψ. Then, as a sufficient condition, the analyticity of f at a given $x_0 \in \mathbb{R}$ is confirmed if an analog of Algorithm 2 with input Ψ returns $\rho = 1$. However, the output would be inconclusive if $\rho > 1$. The reason lies in the fact that neither Algorithm 2 nor its analog for an arbitrary semi-algebraic function f distinguishes between different branches, and therefore ρ may not be optimal. This is the subject of our future research.

Acknowledgments

The authors are supported by NSF grants CCF-1910441 and CCF-2128702.

References

[1] S.S. Abhyankar, Irreducibility criterion for germs of analytic functions of two complex variables, Adv. Math. 74 (2) (1989) 190–257.

[2] F. Alizadeh, J.-P.A. Haeberly, M.L. Overton, Primal-dual interior-point methods for semidefinite programming: convergence rates, stability and numerical results, SIAM J. Control Optim. 8 (3) (1998) 746–768.

[3] S. Basu, Algorithms in real algebraic geometry: a survey, in: Real Algebraic Geometry, in: Panor. Synthèses, vol. 51, Soc. Math. France, Paris, 2017, pp. 107–153.

[4] S. Basu, A. Mohammad-Nezhad, On the central path of semidefinite optimization: degree and worst-case convergence rate, SIAM J. Appl. Algebra Geom. 6 (2) (2022) 299–318.

[5] S. Basu, R. Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometry, Springer, New York, NY, USA, 2006.

[6] S. Basu, M.-F. Roy, Bounding the radii of balls meeting every connected component of semi-algebraic sets, J. Symb. Comput. 45 (12) (2010) 1270–1279.

[7] D.J. Bates, A.J. Sommese, J.D. Hauenstein, C.W. Wampler, Numerically Solving Polynomial Systems with Bertini, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2013.

[8] D.A. Bayer, J.C. Lagarias, The nonlinear geometry of linear programming. I affine and projective scaling trajectories, Trans. Am. Math. Soc. 314 (2) (1989) 499–526.

[9] D.A. Bayer, J.C. Lagarias, The nonlinear geometry of linear programming. II Legendre transform coordinates and central trajectories, Trans. Am. Math. Soc. 314 (2) (1989) 527–581.

[10] C.A. Berenstein, R. Gay, Complex Variables. An Introduction, Springer-Verlag, New York, NY, USA, 1991.

[11] G. Blekherman, P.A. Parrilo, R.R. Thomas, Semidefinite Optimization and Convex Algebraic Geometry, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2013.

[12] L. Blum, F. Cucker, M. Shub, S. Smale, Complexity and Real Computation, Springer-Verlag, New York, NY, USA, 1998.

[13] J. Bochnak, M. Coste, M.-F. Roy, Real Algebraic Geometry, Springer-Verlag, Berlin, Germany, 1998.

[14] E. de Klerk, Aspects of Semidefinite Programming. Interior Point Algorithms and Selected Applications, Series of Applied Optimization, vol. 65, Springer, New York, NY, USA, 2006.

[15] J.A. De Loera, B. Sturmfels, C. Vinzant, The central curve in linear programming, Found. Comput. Math. 12 (4) (2012) 509–540.

[16] J.-P. Dedieu, G. Malajovich, M. Shub, On the curvature of the central path of linear programming theory, Found. Comput. Math. 5 (2) (2005) 145–171.

[17] G. Fischer, Plane Algebraic Curves, vol. 15, American Mathematical Society, Providence, RI, USA, 2001.

[18] D. Goldfarb, K. Scheinberg, Interior point trajectories in semidefinite programming, SIAM J. Control Optim. 8 (4) (1998) 871–886.

[19] P. Griffiths, Introduction to Algebraic Curves, American Mathematical Society, Providence, RI, USA, 1989.

[20] O. Güler, Limiting behavior of weighted central paths in linear programming, Math. Program. 65 (1) (1994) 347–363.

[21] J.-P.A. Haeberly, Remarks on nondegeneracy in mixed semidefinite-quadratic programming, Unpublished memorandum, available from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.43.7501&rep=rep1&type=pdf, 1998.
[22] M. Halická, Analyticity of the central path at the boundary point in semidefinite programming, Eur. J. Oper. Res. 143 (2) (2002) 311–324.
[23] M. Halická, E. de Klerk, C. Roos, On the convergence of the central path in semidefinite optimization, SIAM J. Control Optim. 12 (4) (2002) 1090–1099.
[24] J.D. Hauenstein, A.C. Liddell, S. McPherson, Y. Zhang, Numerical algebraic geometry and semidefinite programming, Results Appl. Math. 11 (2021) 100166.
[25] T. Illés, J. Peng, C. Roos, T. Terlaky, A strongly polynomial rounding procedure yielding a maximally complementary solution for $p^*(\kappa)$ linear complementarity problems, SIAM J. Control Optim. 11 (2) (2000) 320–340.
[26] G.A. Jones, D. Singerman, Complex Functions. An Algebraic and Geometric Viewpoint, Cambridge University Press, Cambridge, UK, 1987.
[27] S.G. Krantz, H.R. Parks, A Primer of Real Analytic Functions, Springer, New York, NY, USA, 2002.
[28] H.T. Kung, J.F. Traub, All algebraic functions can be computed fast, J. Assoc. Comput. Mach. 25 (2) (1978) 245–260.
[29] Z.-Q. Luo, J.F. Sturm, S. Zhang, Superlinear convergence of a symmetric primal-dual path following algorithm for semidefinite programming, SIAM J. Control Optim. 8 (1) (1998) 59–81.
[30] J. Milnor, Singular Points of Complex Hypersurfaces, Annals of Mathematics Studies, Princeton University Press/University of Tokyo Press, Princeton, NJ, 1968.
[31] A. Mohammad-Nezhad, T. Terlaky, On the identification of the optimal partition for semidefinite optimization, Inf. Syst. Oper. Res. 58 (2) (2020) 225–263.
[32] R. Monteiro, T. Tsuchiya, Limiting behavior of the derivatives of certain trajectories associated with a monotone horizontal linear complementarity problem, Math. Oper. Res. 21 (4) (1996) 793–814.
[33] A.P. Morgan, A.J. Sommese, C.W. Wampler, Computing singular solutions to nonlinear analytic systems, Numer. Math. 58 (1) (1990) 669–684.
[34] A.P. Morgan, A.J. Sommese, C.W. Wampler, A power series method for computing singular solutions to nonlinear analytic systems, Numer. Math. 63 (1) (1992) 391–409.
[35] Y. Nesterov, A. Nemirovskii, Interior-Point Polynomial Algorithms in Convex Programming, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1994.
[36] J. Neto, O. Ferreira, R. Monteiro, Asymptotic behavior of the central path for a special class of degenerate SDP problems, Math. Program. 103 (3) (2005) 487–514.
[37] M. Preiß, J. Stoer, Analysis of infeasible-interior-point paths arising with semidefinite linear complementarity problems, Math. Program. 99 (3) (2004) 499–520.
[38] M.V. Ramana, An exact duality theory for semidefinite programming and its complexity implications, Math. Program., Ser. B 77 (2) (1997) 129–162.
[39] M.V. Ramana, P.M. Pardalos, Semidefinite programming, in: T. Terlaky (Ed.), Interior Point Methods of Mathematical Programming, Springer US, New York, NY, USA, 1996, pp. 369–398.
[40] J.R. Sendra, F. Winkler, S. Pérez-Diaz, Rational Algebraic Curves. A Computer Algebra Approach, Algorithms and Computation in Mathematics, Springer, New York, NY, USA, 2008.
[41] I.R. Shafarevich, Basic Algebraic Geometry 1. Varieties in Projective Space, Springer-Verlag, Heidelberg, Germany, 2013.
[42] A.J. Sommese, C.W. Wampler, The Numerical Solution of Systems of Polynomials Arising in Engineering and Science, WORLD SCIENTIFIC, 2005.
[43] J. Stoer, M. Wechs, Infeasible-interior-point paths for sufficient linear complementarity problems and their analyticity, Math. Program. 83 (1) (1998) 407–423.
[44] J. Stoer, M. Wechs, On the analyticity properties of infeasible-interior-point paths for monotone linear complementarity problems, Numer. Math. 81 (4) (1999) 631–645.
[45] A. Tarski, A Decision Method for Elementary Algebra and Geometry, 2nd ed., University of California Press, Berkeley and Los Angeles, CA, USA, 1951.
[46] M.J. Todd, Semidefinite optimization, Acta Numer. 10 (2001) 515–560.
[47] R.J. Walker, Algebraic Curves, Springer, New York, NY, USA, 1978.
[48] P.G. Walsh, Irreducibility testing over local fields, Math. Comput. 69 (231) (2000) 1183–1191.
[49] P.G. Walsh, A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function, Math. Comput. 69 (231) (2000) 1167–1182.
[50] H. Wei, H. Wolkowicz, Generating and measuring instances of hard semidefinite programs, Math. Program. 125 (1) (2010) 31–45.