



ELSEVIER

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Journal of Complexity 21 (2005) 502–531

Journal of
COMPLEXITY

www.elsevier.com/locate/jco

Numeric vs. symbolic homotopy algorithms in polynomial system solving: a case study[☆]

M. De Leo^a, E. Dratman^a, G. Matera^{b, c, *}

^a*Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I (1428) Buenos Aires, Argentina*

^b*Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (1613) Los Polvorines, Buenos Aires, Argentina*

^c*Consejo Nacional de Investigaciones Científicas y Tecnológicas (CONICET), Argentina*

Received 31 January 2004; accepted 6 September 2004

Available online 2 February 2005

Abstract

We consider a family of polynomial systems which arises in the analysis of the stationary solutions of a standard discretization of certain semi-linear second-order parabolic partial differential equations. We prove that this family is well-conditioned from the numeric point of view, and ill-conditioned from the symbolic point of view. We exhibit a polynomial-time numeric algorithm solving any member of this family, which significantly contrasts the exponential behavior of all known symbolic algorithms solving a generic instance of this family of systems.

© 2005 Elsevier Inc. All rights reserved.

Keywords: Polynomial system solving; Homotopy algorithms; Conditioning; Complexity; Semi-linear parabolic problems; Stationary solutions

[☆] Research was partially supported by the following Argentinian and German grants: UBACyT X112, PIP CONICET 2461, BMBF-SETCIP AL/PA/01–EIII/02, UNGS 30/3005 and beca de posgrado interno CONICET. Some of the results presented here were first announced at the *Workshop Argentino de Informática Teórica*, WAIT'02, held in September 2002 (see [15]).

* Corresponding author. Instituto de Desarrollo Humano, Campus Universitario, Universidad Nacional de General Sarmiento, Jose. M. Gutiérrez 1150, 1613 Los Polvorines, Buenos Aires, Argentina.

E-mail addresses: amdeleo@dm.uba.ar (M. De Leo), edratman@dc.uba.ar (E. Dratman), gmatera@ungs.edu.ar (G. Matera)

URL: <http://www.medicis.polytechnique.fr/~matera> (G. Matera).

1. Introduction

Several scientific and technical problems require the solution of polynomial systems over the real or complex numbers (see e.g. [43,48]). In order to solve these problems, one is usually led to consider the following questions:

- Do there exist solutions in a given subset S of \mathbb{R}^n or \mathbb{C}^n ?
- How many solutions are there in the set S ?
- Approximate some or all the solutions in the set S .

Numeric and symbolic methods for computing all solutions of a given zero-dimensional polynomial system usually rely on deformation techniques, based on a perturbation of the original system and a subsequent (numeric or symbolic) path-following method (see e.g. [1,3,5,13,22,30,38,39,44,58]). More precisely, let V be a \mathbb{Q} -definable zero-dimensional subvariety of an affine n -dimensional space \mathbb{C}^n , and suppose that we are given an algebraic curve $W \subset \mathbb{C}^{n+1}$ such that the standard projection $\pi : W \rightarrow \mathbb{C}$ onto the first coordinate is dominant with generically finite fibers of degree D , $\pi^{-1}(1) = \{1\} \times V$ holds and $\pi^{-1}(0)$ is an unramified fiber which can be “easily” described. Then, following the D paths of W along the parameter interval $[0, 1]$, we obtain a complete description of the input variety V .

There are several variants of homotopy algorithms which profit from special features of the input system, such as sparsity patterns or the existence of suitable low-degree projections. Homotopy algorithms for sparse systems are based on so-called polyhedral homotopies (see e.g. [35,38,59,60]). Polyhedral homotopies preserve the Newton polytope (the convex hull of the set of exponents of nonzero monomials) of the input polynomials and rely on an effective version of Bernstein’s theorem (see e.g. [35,36]). Another family of symbolic homotopy algorithms is based on a flat deformation of a certain morphism of affine varieties, originally due to the papers [21,23], which was isolated and refined in [7,29,30,51,56] in order to efficiently solve particular instances of a parametric system with a finite generically unramified linear projection of “low” degree.

The complexity of symbolic homotopy methods is roughly $Ln^{O(1)}D\delta$ arithmetic operations, where n is the number of variables, L is the complexity of the evaluation of the input polynomials, δ is the degree of the variety W introduced by the deformation and D is the number of branches to be followed (see e.g. [7,29,56]). On the other hand, the complexity of numeric homotopy continuation methods is $Ln^{O(1)}D\mu^2$ floating point operations, where μ is highest condition number arising from the application of the Implicit Function Theorem to the points of the paths of $W \cap \pi^{-1}[0, 1]$ followed (cf. [5]).

Let us observe that the parameters L , n and D are somehow determined by the input variety V . In fact, D usually arises as a certain Bézout number associated to the structure of the problem (see e.g. [29,45,53]). Therefore, the complexity of an homotopy algorithm is essentially determined by the parameters δ or μ . Taking into account that the degree of V is a lower bound for δ , we shall call a given zero-dimensional system $f_1 = \dots = f_n = 0$ *ill-conditioned from the symbolic point of view* if the degree of V is close to the worst-case estimate $\prod_{i=1}^n \deg(f_i)$. Furthermore, taking into account that symbolic algorithms may profit from factorization patterns (see e.g. [7,30,51]), we shall further require an ill-conditioned variety V to be \mathbb{Q} -irreducible. On the other hand, following [5] we shall call

the input variety V ill-conditioned from the numeric point of view if the parameter μ is of kind $\prod_{i=1}^n \deg(f_i)^{\Omega(1)}$.

Our main purpose is to compare complexity and conditioning of symbolic and numeric methods on significant classes of polynomial systems. For this purpose, in this article we consider a class of polynomial systems which arise from a discretization of certain second-order parabolic semi-linear equations. More precisely, for given univariate rational polynomials f, g, h , we consider the following initial boundary value problem:

$$\begin{cases} u_t = f(u)_{xx} - g(u) & \text{in } (0, 1) \times [0, T), \\ f(u)_x(1, t) = h(u(1, t)) & \text{in } [0, T), \\ f(u)_x(0, t) = 0 & \text{in } [0, T), \\ u(x, 0) = u_0(x) \geq 0 & \text{in } [0, 1]. \end{cases}$$

This kind of problems models many physical, biological and engineering phenomena, such as heat conduction, gas filtration and liquids in porous media, growth and migration of populations, etc. (cf. [34,49]). In particular, the long-time behavior of its solutions has been intensively analyzed (see e.g. [12,37,54]). The usual numerical approach to this problem consists of considering a second-order finite difference discretization in the variable x , with a uniform mesh, keeping the variable t continuous (see [2,9]). This semi-discretization in space leads to the following initial value problem:

$$\begin{cases} u'_1 = 2(n-1)^2(f(u_2) - f(u_1)) - g(u_1), \\ u'_k = (n-1)^2(f(u_{k+1}) - 2f(u_k) + f(u_{k-1})) - g(u_k), \quad (2 \leq k \leq n-1) \\ u'_n = 2(n-1)^2(f(u_{n-1}) - f(u_n)) - g(u_n) + 2(n-1)h(u_n), \\ u_k(0) = u_0(x_k), \quad (1 \leq k \leq n), \end{cases} \tag{1}$$

where x_1, \dots, x_n define a uniform partition of the interval $[0,1]$.

In order to describe the dynamic behavior of the solutions of (1) it is usually necessary to analyze the behavior of the corresponding *stationary solutions* (see e.g. [8,17]), i.e., the *positive solutions* of the polynomial system:

$$\begin{cases} 0 = 2(n-1)^2(f(X_2) - f(X_1)) - g(X_1), \\ 0 = (n-1)^2(f(X_{k+1}) - 2f(X_k) + f(X_{k-1})) - g(X_k), \quad (2 \leq k \leq n-1), \\ 0 = 2(n-1)^2(f(X_{n-1}) - f(X_n)) - g(X_n) + 2(n-1)h(X_n). \end{cases} \tag{2}$$

A typical case study is that of the heat equation, i.e., $f(X) := X$, with nonlinear reaction and absorption terms of type $g(X) := X^d$ and $h(X) := X^e$ (see e.g. [8,12,26]). In this article we shall mainly consider the case $e = 0$, i.e., the initial boundary value problem:

$$\begin{cases} u_t = u_{xx} - u^d & \text{in } (0, 1) \times [0, T), \\ u_x(1, t) = \alpha > 0 & \text{in } [0, T), \\ u_x(0, t) = 0 & \text{in } [0, T), \\ u(x, 0) = u_0(x) \geq 0 & \text{in } [0, 1] \end{cases} \tag{3}$$

and the corresponding set of stationary solutions of its semi-discretization in space, i.e., the positive solutions of the following system:

$$\begin{cases} 0 = 2(n - 1)^2(X_2 - X_1) - X_1^d, \\ 0 = (n - 1)^2(X_{k+1} - 2X_k + X_{k-1}) - X_k^d, & (2 \leq k \leq n - 1), \\ 0 = 2(n - 1)^2(X_{n-1} - X_n) - X_n^d + 2(n - 1)\alpha. \end{cases} \quad (4)$$

In Section 3 we prove that the solutions of the semi-discrete version of (3) converge to the corresponding solutions of (3) in any interval where the latter are defined, showing thus the consistence of our semi-discretization. We further show that any solution of the semi-discrete version of (3) which is globally bounded converges to a stationary solution of (3).

Then we analyze systems (2) and (4) from the symbolic and numeric point of view. In Section 4 we show that a generic instance of (2) or (4) is likely to be ill-conditioned from the symbolic point of view. Therefore, any *universal* (in the sense of [11]) symbolic method solving such instances has a complexity which is exponential in the number n of variables (see [11,31]). Since universality is a very mild condition satisfied by all known symbolic elimination procedures, and taking into account that n may grow large in the discretization problems we are considering, we conclude that all known symbolic elimination methods are very unsuitable for this kind of problems. Let us also remark that numeric homotopy continuation methods computing *all* isolated complex solutions of the input system are also universal in the above sense, and therefore exponential in n (cf. [50]).

In Section 5 we exhibit a smooth *real homotopy* which allows us to determine the number of positive solutions of certain instances of (2), including all instances of (4), without considering the underlying set of complex solutions. More precisely, let $V_1 \subset (\mathbb{R}_{\geq 0})^n$ be the set of positive solutions of the instance of (2) under consideration. We exhibit a real algebraic curve $W_1 \subset (\mathbb{R}_{\geq 0})^{n+1}$ such that, if $\pi|_{W_1} : W_1 \rightarrow \mathbb{R}$ denotes the restriction of the standard projection onto the first coordinate, then $\pi|_{W_1}^{-1}(1) = \{1\} \times V_1$ holds, $V_0 := \pi|_{W_1}^{-1}(0)$ is easy to solve, every $t \in [0, 1]$ is regular value of $\pi|_{W_1}$ and $W_1 \cap ([0, 1] \times (\mathbb{R}_{\geq 0})^n) = W_1 \cap ([0, 1] \times (\mathbb{R}_{> 0})^n)$. Under these conditions, we conclude that V_1 and V_0 have the same cardinality, which allows us to prove that V_1 consists of one point.

Finally, in Section 6 we prove that the homotopy above is *well-conditioned* from the numeric point of view. This allows us to exhibit an algorithm approximating the only positive solution x^* of (4) by an homotopy continuation method. This algorithm computes an ε -approximation of x^* with $n^{O(1)}M \log d$ floating point operations, where $M := \log |\log(\varepsilon n^3 \alpha d)|$. The starting point for our numeric algorithm is the only positive solution of set V_0 above, and hence it does not depend on random or generic choices.

As a consequence, we see the significant contrast between the *exponential* complexity behavior of all symbolic methods solving any instance of (4) and the *polynomial* complexity behavior of our numeric method.

2. Notions and notations

We use standard notions and notations of commutative algebra and algebraic and semi-algebraic geometry, as can be found in e.g. [6,16,41,57].

2.1. Algebraic geometry, geometric solutions

For a given $n \in \mathbb{N}$, we shall denote by \mathbb{A}^n the n -dimensional affine space \mathbb{C}^n endowed with its Zariski topology over \mathbb{Q} . Let X_1, \dots, X_n be indeterminates over \mathbb{Q} and let be given polynomials $F_1, \dots, F_m \in \mathbb{Q}[X_1, \dots, X_n]$. We denote by $W := V(F_1, \dots, F_m)$ the affine subvariety of \mathbb{A}^n defined by the set of common zeros of F_1, \dots, F_m in \mathbb{A}^n . If W is equidimensional of dimension $\dim W$, we define its degree as the number of points arising when we intersect W with $\dim W$ generic affine linear hyperplanes of \mathbb{A}^n . For an arbitrary affine variety W with irreducible components C_1, \dots, C_s we define its degree as $\deg W := \deg C_1 + \dots + \deg C_s$. With this definition, the intersection of two subvarieties W_1 and W_2 of \mathbb{A}^n satisfies the following Bézout inequality (cf. [18,28]):

$$\deg(W_1 \cap W_2) \leq \deg W_1 \deg W_2. \tag{5}$$

Let W be an affine equidimensional subvariety of \mathbb{A}^n of dimension $r \geq 0$ and let $I(W) \subset \mathbb{Q}[X_1, \dots, X_n]$ be its defining ideal. The coordinate ring $\mathbb{Q}[W]$ and the ring of total fractions $\mathbb{Q}(W)$ are defined as the quotient ring $\mathbb{Q}[X_1, \dots, X_n]/I(W)$ and its total ring of fractions, respectively.

Suppose that there exist polynomials $F_1, \dots, F_{n-r} \in \mathbb{Q}[X_1, \dots, X_n]$ which form a regular sequence of $\mathbb{Q}[X_1, \dots, X_n]$ and generate the ideal $I(W)$. Let $\pi : W \rightarrow \mathbb{A}^r$ be the morphism defined by $\pi(x_1, \dots, x_n) = (x_1, \dots, x_r)$. Let $W = C_1 \cup \dots \cup C_s$ be the decomposition of W into irreducible components, and suppose that $\pi|_{C_i}$ is dominant for $1 \leq i \leq s$. We define the degree of π as the number $D := \sum_{i=1}^s [\mathbb{Q}(C_i) : \mathbb{Q}(X_1, \dots, X_r)]$, where $[\mathbb{Q}(C_i) : \mathbb{Q}(X_1, \dots, X_r)]$ denotes the degree of the finite field extension $\mathbb{Q}(X_1, \dots, X_r) \hookrightarrow \mathbb{Q}(C_i)$ for $1 \leq i \leq s$. We say that π is *generically unramified* if $\pi^{-1}(x_1, \dots, x_r)$ consists of exactly D points for a generic value $(x_1, \dots, x_r) \in \mathbb{A}^r$. This implies that the Jacobian determinant $\det(\partial F_i / \partial X_{r+j})_{1 \leq i, j \leq n-r}$ is not a zero divisor in $\mathbb{Q}[W]$.

Suppose further that π is finite and generically unramified. Then the corresponding integral ring extension $\mathbb{Q}[X_1, \dots, X_r] \hookrightarrow \mathbb{Q}[W]$ induces in $\mathbb{Q}[W]$ a structure of free $R := \mathbb{Q}[X_1, \dots, X_r]$ -module, whose rank $\text{rank}_R \mathbb{Q}[W]$ equals the cardinality D of the generic fiber of π and is upper bounded by $\deg W$ (see e.g. [24]). Following [21], a *geometric solution* of the system $F_1 = 0, \dots, F_{n-r} = 0$ (or of the variety W) with respect to π consists of the following items:

- A linear form $U \in \mathbb{Q}[X]$ which induces a primitive element of the ring extension $\mathbb{Q}[X_1, \dots, X_r] \hookrightarrow \mathbb{Q}[W]$, i.e., an element $u \in \mathbb{Q}[W]$ whose minimal polynomial $Q \in R[Y]$ over R satisfies $\deg_Y Q = D$.
- The polynomial Q .
- A generic “parametrization” of W by the zeros of Q , given by polynomials $V_{r+1}, \dots, V_n \in R[Y]$. We require the conditions $\deg_Y V_i < D$ and $(\partial Q / \partial Y)(X_1, \dots, X_r, U) X_i - V_i(X_1, \dots, X_r, U) \in I(W)$ for $r + 1 \leq i \leq n$.

In particular, for any $(x_1, \dots, x_r) \in \mathbb{Q}^r$ such that $q := Q(x_1, \dots, x_r, Y) \in \mathbb{Q}[Y]$ is square-free, the polynomials $U, q, v_i := V_i(x_1, \dots, x_r, Y)$ ($r + 1 \leq i \leq n$) define a geometric solution of the zero-dimensional variety $\pi^{-1}(x_1, \dots, x_r)$.

2.2. Semi-algebraic geometry

A subset of \mathbb{R}^n is a (\mathbb{Q} -definable) *semi-algebraic set* if it can be defined by a Boolean combination of equalities and inequalities involving polynomials of $\mathbb{Q}[X_1, \dots, X_n]$.

In what follows, we shall consider \mathbb{R}^n endowed with its standard Euclidean topology, unless otherwise stated. A real semi-algebraic set $V \subset \mathbb{R}^n$ is called *semi-algebraically connected* if for any pair of disjoint real semi-algebraic sets $C_1, C_2 \subset \mathbb{R}^n$, which are closed in V and satisfy $C_1 \cup C_2 = V$, we have $V = C_1$ or $V = C_2$. Every real semi-algebraic set $V \subset \mathbb{R}^n$ can be uniquely decomposed (up to reordering) as a disjoint union of a finite number of real semi-algebraically connected sets C_1, \dots, C_s , open and closed in V , which are called the *semi-algebraically connected components* of V (see e.g. [6]).

2.3. Computational model and complexity measures

Our computational model is based on the concept of *arithmetic-boolean circuits* (also called *arithmetic networks*) and *computation trees* (see e.g. [10,19]). An arithmetic-boolean circuit over $\mathbb{Q}[X_1, \dots, X_n]$ is a directed acyclic graph (*dag* for short) whose nodes are labeled either by an element of $\mathbb{Q} \cup \{X_1, \dots, X_n\}$, or by an arithmetic operation or a selection (pointing to other nodes) subject to a previous equal-to-zero decision. On the *dag* associated to a given arithmetic-boolean circuit β we may play a pebble game (see [55]). A pebble game is a strategy of evaluation of β which converts β into a sequential algorithm (called computation tree) and associates to β natural time and space measures. Space is defined as the maximum number arithmetic registers used at any moment of the game, and time is defined as the total number of arithmetic operations and selections performed during the game. A computation tree without selections is called a *straight-line program* (cf. [10]). In the sequel, we shall assume that our arithmetic-boolean circuits and computation trees in $\mathbb{Q}[X_1, \dots, X_n]$ contain only divisions by nonzero elements of \mathbb{Q} .

In what follows we shall use the notation $\mathcal{M}(m) := m \log^2(m) \log \log(m)$. Let us remark that the asymptotic estimate $O(\mathcal{M}(m))$ represents the number of arithmetic operations in a given domain R necessary to compute a multiplication, division, resultant, gcd and interpolation with univariate polynomials of $R[Y]$ of degree at most m (cf. [4,20]).

In order to determine the number of real roots of a given univariate polynomial with integer or rational coefficients, we shall use algorithms based on the computation of suitable Cauchy indices. For given polynomials $p, q \in \mathbb{Z}[Y]$, the *Cauchy index* $I(q/p)$ of the rational function q/p is defined as the number of jumps of q/p from $-\infty$ to $+\infty$ minus the number of jumps of q/p from $+\infty$ to $-\infty$ (see e.g. [27,40]). Let be given $p, q_1, \dots, q_s \in \mathbb{Z}[Y]$ and a set of sign conditions $\delta_1, \dots, \delta_s$ (i.e., δ_i belongs to $\{+, -, 0\}$ for $1 \leq i \leq s$). Let

$$c_{[\delta_1, \dots, \delta_s]}(p; q_1, \dots, q_s) := \#\{x \in \mathbb{R} : p(x) = 0, \text{sign}(q_i(x)) = \delta_i \ (1 \leq i \leq s)\}.$$

We have the identity $I(p'q/p) = c_{[+]}(p; q) - c_{[-]}(p; q)$ [27, Proposition 2.2]. We conclude that $I(p'/p) = c(p) := c_{[+]}(p; 1)$ holds, which relates Cauchy index computations with univariate real root counting issues (see [27]).

In [40] it is shown that computing the Cauchy index of a rational function whose numerator and denominator are integer polynomials of degree at most m requires $O(\mathcal{M}(m))$ arithmetic operations in \mathbb{Q} . This algorithm can be obviously extended to a rational function defined

by polynomials $p, q \in \mathbb{Q}[X]$, applying the algorithm to suitable integer multiples $\lambda p, \lambda q$ of p, q .

3. The initial boundary value problem under consideration

As mentioned in the introduction, we shall consider the initial boundary value problem (3) for an initial data $u_0(x)$ satisfying the “compatibility condition” $u'_0(1) = \alpha, u'_0(0) = 0$. In order to solve (3), we consider the following (semi)discrete version of (3):

$$\begin{cases} u'_1(t) = \frac{2}{h^2}(u_2(t) - u_1(t)) - u_1(t)^d, \\ u'_k(t) = \frac{1}{h^2}(u_{k+1}(t) - 2u_k(t) + u_{k-1}(t)) - u_k(t)^d, \quad (2 \leq k \leq n-1), \\ u'_n(t) = \frac{2}{h^2}(u_{n-1}(t) - u_n(t)) + \frac{2}{h}\alpha - u_n(t)^d, \\ u_k(0) = u_0(x_k), \quad (1 \leq k \leq n), \end{cases} \tag{6}$$

where x_1, \dots, x_n define a uniform partition of $[0, 1]$ and $h := (n - 1)^{-1}$.

We are going to show that the solutions of (6) converge to the corresponding solutions of (3), and we shall discuss the role of the stationary solutions of (6) in the description of the asymptotic behavior of the solutions of (6). We start with the convergence result:

Theorem 1. *Let $0 < \tau \leq T$ be a value for which there exist a positive solution $u(x, t) \in C^{4,1}([0, 1] \times [0, \tau])$ of (3) and a solution $U(t) := (u_1(t), \dots, u_n(t))$ of (6) in $[0, \tau]$. Then there exists $C > 0$, depending only on the (infinite) $C^{4,1}([0, 1] \times [0, \tau])$ -norm of u , such that for h small enough we have:*

$$\max_{t \in [0, \tau]} \max_{1 \leq k \leq n} |u(x_k, t) - u_k(t)| \leq Ch^{1/2}. \tag{7}$$

Proof. Let $v_k(t) := u(x_k, t)$ and $e_k(t) := v_k(t) - u_k(t)$ for $1 \leq k \leq n$. Let $C_0 := \max\{|v_k(t)| : 1 \leq k \leq n, 0 \leq t \leq \tau\}$ and $t_0 := \max\{t \in [0, \tau] : |e_k(s)| \leq C_0/2 \text{ for all } s \in [0, t]\}$. We shall prove that (7) is valid in the interval $[0, t_0]$, from which we shall conclude that $t_0 = \tau$ holds for h small enough.

Let $k \neq 1, n$. Then there exists a constant $C_1 > 0$ independent of h such that

$$\begin{aligned} e'_k(t) &\leq \frac{1}{h^2}(e_{k+1}(t) - 2e_k(t) + e_{k-1}(t)) - (v_k(t)^d - u_k(t)^d) + C_1h^2 \\ &\leq \frac{1}{h^2}(e_{k+1}(t) - 2e_k(t) + e_{k-1}(t)) + d|\xi_k(t)|^{d-1}|v_k(t) - u_k(t)| + C_1h^2 \end{aligned}$$

holds, where $\xi_k(t)$ is an intermediate value between $v_k(t)$ and $u_k(t)$. From the definition of t_0 we see that there exists a constant $C_2 > 0$ independent of h such that $d|\xi_k(t)|^{d-1} \leq C_2$ holds for any $1 \leq k \leq n$ and any $t \in [0, t_0]$. Furthermore, arguing in a similar way for $k = 1, n$, we obtain:

$$\begin{aligned} e'_1(t)/2 &\leq \frac{1}{h^2}(e_2(t) - e_1(t)) + C_2|e_1(t)|/2 + C_1h^2/2, \\ e'_k(t) &\leq \frac{1}{h^2}(e_{k+1}(t) - 2e_k(t) + e_{k-1}(t)) + C_2|e_k(t)| + C_1h^2, \quad (2 \leq k \leq n-1), \\ e'_n(t)/2 &\leq \frac{1}{h^2}(e_{n-1}(t) - e_n(t)) + C_2|e_n(t)|/2 + C_1h^2/2. \end{aligned} \tag{8}$$

Let $E(t) := (e_1(t), \dots, e_n(t))$ and $N(t) := e_1^2(t)/2 + \sum_{k=2}^{n-1} e_k^2(t) + e_n^2(t)/2$. Multiplying the k th inequality of (8) by $e_k(t)$ for $1 \leq k \leq n$ and adding up we have

$$N'(t) \leq 2h^{-2} E(t)^t A E(t) + 2C_2 N(t) + 2C_1 h^2 \left(e_1(t)/2 + \sum_{k=2}^{n-1} e_k(t) + e_n(t)/2 \right),$$

where $A \in \mathbb{Z}^{n \times n}$ is a suitable negative semi-definite symmetric $n \times n$ matrix (the opposite of the stiffness matrix). Therefore, taking into account the inequalities $E(t)^t A E(t) \leq 0$ and $e_k(t) \leq (e_k^2(t) + 1)/2$ ($1 \leq k \leq n$), we obtain $N'(t) \leq (2C_2 + C_1 h^2) N(t) + C_1 h$. Integrating both members of this inequality we have

$$N(t) \leq (2C_2 + C_1 h^2) \int_0^t N(s) ds + C_1 t h \leq (2C_2 + C_1 h^2) \int_0^t N(s) ds + C_1 T h$$

for any $t \in [0, t_0]$. Therefore, Gronwall's Lemma (see e.g. [34, §1.2.1]) yields:

$$N(t) \leq C_1 T h e^{2TC_2 + C_1 T h^2} \leq C_1 T e^{2TC_2 + TC_1 h}$$

for any $t \in [0, t_0]$. Hence, from the definition of $N(t)$ we easily deduce the estimate $e_k^2(t) \leq 2C_1 T e^{2TC_2 + TC_1 h}$ for any $t \in [0, t_0]$ and any $1 \leq k \leq n$.

Letting $C := (2C_1 T)^{1/2} e^{TC_2 + TC_1/2}$ we conclude that $|u(x_k, t) - u_k(t)| \leq Ch^{1/2}$ holds for any $1 \leq k \leq n$ and any $t \in [0, t_0]$. Combining this estimate with the definition of t_0 shows that $t_0 = \tau$ holds for h small enough, because otherwise the maximality of t_0 would be contradicted. This finishes the proof. \square

Let us remark that, using more technical arguments, based on a suitable comparison principle along the lines of [17, Theorem 2.1], we may improve the right-hand side of (7) to Ch^2 . Nevertheless, since we are not concerned with such convergence speed results, we shall not pursue the subject any further.

Now we analyze the asymptotic behavior of the solutions of (6). For this purpose, we are going to analyze the role of the *stationary solutions* of (6), i.e. the positive solutions of the polynomial system (4). We start with the following discrete maximum principle:

Lemma 2. *Let U be a solution of (6) with initial condition $U(0) = U_0 \in (\mathbb{R}_{\geq 0})^n$, and let $\tau \in (\mathbb{R}_{>0} \cup \{\infty\})$ be the supremum of the set of $t \in \mathbb{R}_{>0}$ for which U is well-defined in $[0, t)$. Then $U(t) \in (\mathbb{R}_{\geq 0})^n$ for any $t \in [0, \tau)$.*

Proof. By a standard approximation argument we may assume without loss of generality that $U_0 \in (\mathbb{R}_{>0})^n$ holds. Let $U := (u_1, \dots, u_n)$ and let $\mathcal{A} := \{t \in [0, \tau) : u_k(s) \geq 0 \text{ for any } s \in [0, t] \text{ and } 1 \leq k \leq n\}$. By continuity we have that there exists $\varepsilon > 0$ such that $[0, \varepsilon) \subset \mathcal{A}$ holds. We have to prove that the supremum of \mathcal{A} is equal to τ .

Let t_0 denote the supremum of \mathcal{A} , and suppose that $t_0 < \tau$ holds. If $u_k(t_0) > 0$ holds for $1 \leq k \leq n$, then by continuity there exists $\varepsilon_0 > 0$ such that $u_k(t) \geq 0$ for any $t \in [t_0, t_0 + \varepsilon_0]$ and any $k = 1, \dots, n$, contradicting thus the definition of t_0 . Hence, there exists $k_0 \in \{1, \dots, n\}$ such that $u_{k_0}(t_0) = 0$. Furthermore, a similar argument shows that there exist

semi-discrete version of several reaction–diffusion phenomena (see e.g. [8,17]). Furthermore, such kind of systems constitutes a wide generalization of the family of systems (4), the central object of study of this paper.

As mentioned in the introduction, we are going to prove that a generic instance of either (2) or (4) is likely to be ill-conditioned from the symbolic point of view, i.e., its solution set is a \mathbb{Q} -irreducible variety of degree close to d^n . Then, as an illustration of this ill-conditioning, we are going to exhibit a symbolic homotopy algorithm solving any instance of (2) with polynomial complexity in the Bézout number d^n , and thus exponential complexity with respect to n . Let us observe that [11] shows that our complexity estimate is nearly optimal for all known symbolic methods. Combining our algorithm with techniques of [27,40] we shall obtain an algorithm with time-complexity polynomial in the Bézout number d^n which determines the number of positive solutions of any instance of (2) and computes an ε -approximation of them.

4.1. Symbolic conditioning of (2)

Assuming without loss of generality that the polynomial $g \in \mathbb{Q}[T]$ of (2) is monic, let $A_{d-1}, \dots, A_0, B_{d-1}, \dots, B_0, C_{d-1}, \dots, C_0$ be new indeterminates over \mathbb{Q} , and let $f^{(A)} := A_{d-1}T^{d-1} + \dots + A_0, g^{(B)} := T^d + B_{d-1}T^{d-1} + \dots + B_0, h^{(C)} := C_{d-1}T^{d-1} + \dots + C_0$ represent the “generic” versions of the polynomials f, g, h of (2). In our subsequent arguments we are going to consider the affine variety $W^{(A,B,C)} \subset \mathbb{A}^{n+3d}$ defined by the following polynomial system:

$$\begin{cases} 0 = 2(n-1)^2(f^{(A)}(X_2) - f^{(A)}(X_1)) - g^{(B)}(X_1), \\ 0 = (n-1)^2(f^{(A)}(X_{k+1}) - 2f^{(A)}(X_k) + f^{(A)}(X_{k-1})) - g^{(B)}(X_k), \quad (2 \leq k \leq n-1), \\ 0 = 2(n-1)^2(f^{(A)}(X_{n-1}) - f^{(A)}(X_n)) - g^{(B)}(X_n) + 2(n-1)h^{(C)}(X_n). \end{cases} \quad (9)$$

Lemma 3. $W^{(A,B,C)}$ is an equidimensional variety of dimension $3d$ and the projection mapping $\Phi : W^{(A,B,C)} \rightarrow \mathbb{A}^{3d}$ defined by $\Phi(a, b, c, x) := (a, b, c)$ is a finite morphism of degree d^n .

Proof. The finiteness of Φ is equivalent to the finiteness of $\mathbb{Q}[W^{(A,B,C)}]$ as $\mathbb{Q}[A, B, C]$ -module (see e.g. [57]). In order to prove the latter, let ξ_1, \dots, ξ_n be the coordinate functions of $\mathbb{Q}[W^{(A,B,C)}]$ defined by X_1, \dots, X_n and let $\xi := (\xi_1, \dots, \xi_n)$. Then the k -th equation $F_k(A, B, C, X) = 0$ of (9) induces a relation $F_k(A, B, C, \xi) = 0$ in $\mathbb{Q}[W^{(A,B,C)}]$ for $1 \leq k \leq n$. Considering F_1, \dots, F_n as elements of the polynomial ring $\mathbb{Q}[A, B, C][X]$, we observe that the highest degree term (in the variables X) of F_k is the nonzero monomial X_k^d for $1 \leq k \leq n$. This shows that $\mathbb{Q}[W^{(A,B,C)}]$ is generated, as $\mathbb{Q}[A, B, C]$ -module, by the set of monomials $\xi_1^{j_1} \dots \xi_n^{j_n}$ with $j_k < d$ for $1 \leq k \leq n$. Hence, $\mathbb{Q}[W^{(A,B,C)}]$ is a finite $\mathbb{Q}[A, B, C]$ -module, which proves the finiteness of Φ .

We conclude that $W^{(A,B,C)}$ is an equidimensional variety of dimension $3d$. From the Bézout inequality (5) we deduce that the degree of the morphism Φ is bounded by d^n . On the other hand, taking into account that the fiber of the point of \mathbb{A}^{3d} defined by $a = c = 0$,

$b = (0, \dots, 0, 1)$ has cardinality d^n , we conclude that $\deg \Phi = d^n$ holds. This finishes the proof of the lemma. \square

Combining this lemma with e.g. [46, Proposition 3.17] we obtain our first ill-conditioning result concerning the family of systems (2):

Corollary 4. *There exists a nonempty Zariski open set $\mathcal{U} \subset \mathbb{A}^{3d}$ such that, for any $(a, b, c) \in \mathcal{U}$, the corresponding instance of (2) has d^n complex solutions.*

Now we consider the irreducibility of a given instance of (2). For this purpose, we need the following preliminary result:

Lemma 5. *Let $a^{(0)} := (0, \dots, 0, 1, 0) \in \mathbb{A}^d$, let b be an arbitrary point of \mathbb{Q}^d and let $W^{(a^{(0)}, b, 0^*, C_0)}$ denote the algebraic curve defined by $\Phi^{-1}(\{(a^{(0)}, b, 0)\} \times \mathbb{A}^1)$. Then $W^{(a^{(0)}, b, 0^*, C_0)}$ is an irreducible curve of \mathbb{A}^{n+3d} of degree d^n .*

Proof. Let us observe that the variety $W^{(a^{(0)}, b, 0^*, C_0)}$ of the statement of the lemma is determined by the following polynomial system:

$$\begin{cases} 0 = 2(n-1)^2(X_2 - X_1) - g_b(X_1), \\ 0 = (n-1)^2(X_{k+1} - 2X_k + X_{k-1}) - g_b(X_k), & (2 \leq k \leq n-1), \\ 0 = 2(n-1)^2(X_{n-1} - X_n) - g_b(X_n) + 2(n-1)C_0, \end{cases}$$

with $g_b := g^{(B)}(b, T)$. Observe that $W^{(a^{(0)}, b, 0^*, C_0)}$ may also be regarded as a subvariety of \mathbb{A}^{n+1} , by considering the polynomials defining the system above as elements of $\mathbb{Q}[C_0, X]$. In this sense, Lemma 3 implies that the mapping $\Phi^{(C_0)} : W^{(a^{(0)}, b, 0^*, C_0)} \rightarrow \mathbb{A}^1$ defined by $\Phi^{(C_0)}(c_0, x) := c_0$ is a finite morphism of degree at most d^n . This shows that $W^{(a^{(0)}, b, 0^*, C_0)}$ is an equidimensional variety of dimension 1 which, by the Bézout inequality (5), has degree at most d^n .

Let $Q_1(X_1) := X_1$, $Q_2(X_1) := X_1 + (1/2)(n-1)^{-2}g_b(X_1)$ and $Q_{k+1}(X_1) := 2Q_k - Q_{k-1} + (n-1)^{-2}g_b(Q_k)$ for $2 \leq k \leq n-1$. Then it is easy to see that the polynomial $Q \in \mathbb{Q}[C_0, X_1]$ defined by

$$Q(C_0, X_1) := 2(n-1)^2(Q_{n-1}(X_1) - Q_n(X_1)) - g_b(Q_n(X_1)) + 2(n-1)C_0$$

vanishes on the variety $W^{(a^{(0)}, b, 0^*, C_0)}$. From its definition we easily conclude that $\deg Q = \deg_{X_1} Q = d^n$ holds. Taking into account that Q is a monic element of $\mathbb{Q}[C_0][X_1]$ (up to nonzero elements of \mathbb{Q}) of degree 1 in C_0 , from the Gauss Lemma we conclude that is irreducible in $\mathbb{Q}[C_0, X_1]$ and $\mathbb{C}[C_0, X_1]$.

From the Hilbert Irreducibility Theorem (see e.g. [61]) we deduce that there exists $\alpha \in \mathbb{Q}$ such that $Q(\alpha, X_1)$ is an irreducible polynomial of $\mathbb{Q}[X_1]$. This implies that the zero-dimensional variety $W^{(a^{(0)}, b, 0^*, C_0)} \cap \{C_0 = \alpha\}$ has d^n points, which in turn shows that $W^{(a^{(0)}, b, 0^*, C_0)}$ has degree d^n .

Finally, let $\Phi^{(C_0, X_1)} : W^{(a^{(0)}, b, 0^*, C_0)} \rightarrow \mathbb{A}^2$ denote the mapping $\Phi^{(C_0, X_1)}(c_0, x) := (c_0, x_1)$. Then we have that the image of $\Phi^{(C_0, X_1)}$ is the plane curve of equation $Q(C_0, X_1) =$

0. From the irreducibility of $Q(C_0, X_1)$ we conclude that X_1 represents a primitive element of the ring extension $\mathbb{Q}[C_0] \hookrightarrow \mathbb{Q}[W^{(a^{(0)}, b, 0^*, C_0)}]$ and hence of the (finite) field extension $\mathbb{Q}(C_0) \hookrightarrow \mathbb{Q}(W^{(a^{(0)}, b, 0^*, C_0)})$. This implies that for $2 \leq i \leq n$ there exist elements $\rho_i \in \mathbb{Q}[C_0] \setminus \{0\}$, $V_i \in \mathbb{Q}[C_0, X_1]$ such that $X_i \equiv \rho_i^{-1}(C_0)V_i(C_0, X_1)$ holds in $\mathbb{Q}(W^{(a^{(0)}, b, 0^*, C_0)})$. This shows that $\Phi^{(C_0, X_1)}$ represents a birational equivalence between $W^{(a^{(0)}, b, 0^*, C_0)}$ and the curve of equation $Q(C_0, X_1) = 0$, and finishes the proof of the lemma. \square

From Lemma 5 we deduce our second ill-conditioning result concerning the family of systems (2):

Corollary 6. *There exists an infinite number of elements $\alpha \in \mathbb{Q}$ for which (4) defines a \mathbb{Q} -irreducible variety of degree d^n .*

Proof. Let $W^{(a^{(0)}, 0, 0^*, C_0)}$ be the algebraic curve defined by (4) with the value α replaced by a new indeterminate C_0 . Then the proof of Lemma 5 shows that the minimal equation of integral dependence satisfied by X_1 in the ring extension $\mathbb{Q}[C_0] \hookrightarrow \mathbb{Q}[W^{(a^{(0)}, 0, 0^*, C_0)}]$ is an irreducible polynomial $Q \in \mathbb{Q}[C_0, X_1]$ of degree d^n . Hence, Hilbert’s Irreducibility Theorem shows that there exists an infinite number of values $\alpha \in \mathbb{Q}$ for which $Q(\alpha, X_1)$ is an irreducible polynomial of $\mathbb{Q}[X_1]$. For these values of α , the corresponding instances of (4) define a \mathbb{Q} -irreducible variety of degree d^n . \square

In order to state our main result concerning the irreducibility of a given instance of (2), we first prove that a generic specialization of the variables $A, B, C_{d-1}, \dots, C_1$ yields a \mathbb{Q} -irreducible curve of degree d^n :

Proposition 7. *There exists a nonempty Zariski open set $U \subset \mathbb{A}^{3d-1}$ such that, for any $(a, b, c^*) \in U$ with $a, b \in \mathbb{A}^d$, the algebraic curve $W^{(a, b, c^*, C_0)}$ defined by $\Phi^{-1}(\{(a, b, c^*)\} \times \mathbb{A}^1)$ is (absolutely) irreducible of degree d^n .*

Proof. Let $W^{(A, B, C)} \subset \mathbb{A}^{n+3d}$ denote the equidimensional $3d$ -dimensional variety of Lemma 3, and let $\Phi : W^{(A, B, C)} \rightarrow \mathbb{A}^{3d}$ be the (finite) morphism defined by $\Phi(a, b, c, x) := (a, b, c)$. Combining Lemma 3 and [16, Corollary 18.17] we conclude that $\mathbb{Q}[W^{(A, B, C)}]$ is a free $\mathbb{Q}[A, B, C]$ -module, of rank d^n .

Let $U \in \mathbb{Q}[X]$ be a primitive element of $\mathbb{Q}[A, B, C] \hookrightarrow \mathbb{Q}[W^{(A, B, C)}]$ and let $Q \in \mathbb{Q}[A, B, C][Y]$ be its minimal polynomial over $\mathbb{Q}[A, B, C]$. Observe that Q is a monic element of $\mathbb{Q}[A, B, C][Y]$ with $\deg_Y Q = \deg Q = d^n$. We claim that Q is an irreducible polynomial of $\mathbb{C}[A, B, C, Y]$. Indeed, without loss of generality we may assume that U is also a primitive element of the ring extension $\mathbb{Q}[C_0] \hookrightarrow \mathbb{Q}[W^{(a^{(0)}, 0, 0^*, C_0)}]$, where $W^{(a^{(0)}, 0, 0^*, C_0)}$ is the algebraic curve of Corollary 6. Specializing the variables A, B and $C^* := (C_{d-1}, \dots, C_1)$ into the values $a^{(0)}, 0 \in \mathbb{A}^d$ and $0 \in \mathbb{A}^{d-1}$, respectively, from Corollary 6 we deduce that $Q(a^{(0)}, 0, 0, C_0, Y)$ is an irreducible polynomial of $\mathbb{C}[C_0, Y]$ with $\deg_Y Q(a^{(0)}, 0, 0, C_0, Y) = d^n$. Therefore, the monicity of Q in $\mathbb{C}[A, B, C][Y]$ implies that Q is an irreducible polynomial of $\mathbb{C}[A, B, C, Y]$, showing our claim.

From [57, §I.5.2] we have that there exists a nonempty Zariski open subset \mathcal{U}_0 of \mathbb{A}^N , with $N := (d^n + 2)(d^n + 1)/2$, such that any polynomial $F \in \mathbb{C}[C_0, Y]$ of degree at most d^n , whose coefficient vector $c_F \in \mathbb{A}^N$ (in dense representation) belongs to \mathcal{U}_0 , is irreducible in $\mathbb{C}[C_0, Y]$ of degree d^n . Let $g_1, \dots, g_s \in \mathbb{C}[Z_1, \dots, Z_N]$ be a system of generators of the vanishing ideal of $\mathbb{A}^N \setminus \mathcal{U}_0$. Let $Q := \sum_{i+j \leq d^n} c_{i,j}(A, B, C^*) C_0^i Y^j$. Then we have that $Q(a^{(0)}, 0, 0, C_0, Y)$ is an irreducible polynomial of $\mathbb{C}[C_0, Y]$ of degree d^n . This shows that there exists $1 \leq k \leq s$ such that $g_k(c_{i,j}(A, B, C^*); i + j \leq d^n)$ is a nonzero element of $\mathbb{C}[C_0, Y]$. Furthermore, from the definition of g_k we have that, for any $(a, b, c^*) \in \mathbb{A}^{3d-1}$ not annihilating $g_k(c_{i,j}(A, B, C^*); i + j \leq d^n)$, the polynomial $Q(a, b, c^*, C_0, Y)$ is irreducible of degree d^n .

Let $\mathcal{U} \subset \mathbb{A}^{3d-1}$ be the complement of the zero set of $g_k(c_{i,j}(A, B, C^*); i + j \leq d^n)$ and let $(a, b, c^*) \in \mathcal{U}$. Then $Q(a, b, c^*, C_0, Y)$ is irreducible of degree d^n . Hence, arguing as in the last paragraph of the proof of Lemma 5 we see that the morphism $\Phi^{(C_0, X_1)} : W^{(a, b, c^*, C_0)} \rightarrow \mathbb{A}^2$ defined by $\Phi^{(C_0, X_1)}(c_0, x) := (c_0, x_1)$ induces a birational equivalence between the curve $W^{(a, b, c^*, C_0)} := \Phi^{-1}(\{a, b, c^*\} \times \mathbb{A}^1)$ and the plane curve of equation $Q(a, b, c^*, C_0, Y) = 0$. The proposition follows from the irreducibility of the latter. \square

Combining Proposition 7 with Hilbert’s Irreducibility Theorem we obtain our third and main ill-conditioning result concerning the family of systems (2):

Corollary 8. *With notations as in Proposition 7, for any $(a, b, c^*) \in \mathcal{U} \cap \mathbb{Q}^{3d-1}$ there exist an infinite number of values $c_0 \in \mathbb{Q}$ such that the corresponding instance of (2) defines a \mathbb{Q} -irreducible variety of degree d^n .*

4.2. A symbolic homotopy algorithm solving any instance of (2).

Our results of the previous section show that a given instance of (2) is likely to be ill-conditioned from the symbolic point of view. In order to illustrate this behavior, and the kind of symbolic homotopy algorithms we are referring to, in this section we exhibit a symbolic homotopy algorithm solving any instance of (2) which slightly improves a direct application of the best (from the worst-case time–space complexity point of view) symbolic algorithm [25]. Its complexity is exponential in the number of variables n , but nevertheless nearly optimal for the family of systems under consideration (cf. [11,31]). It may be worthwhile to observe that any instance of (2) is a Pham system, which can therefore be (partially) solved by applying the *nonuniversal* symbolic homotopy algorithm of [51]. In such a case, for certain particular nonirreducible instances of (2) our time–space complexity could be significantly improved.

Our algorithm is based on the deformation of (2) defined by the polynomials:

$$\begin{aligned}
 F_1 &:= T \left(2(n-1)^2 (f(X_2) - f(X_1)) - g(X_1) \right) + (T-1)(X_1^d - X_2), \\
 F_k &:= T \left((n-1)^2 (f(X_{k+1}) - 2f(X_k) + f(X_{k-1})) - g(X_k) \right) + (T-1)(X_k^d - X_{k+1}), \\
 &\hspace{20em} (2 \leq k \leq n-1), \\
 F_n &:= T \left(2(n-1)^2 (f(X_{n-1}) - f(X_n)) - g(X_n) + 2(n-1)h(X_n) \right) + (T-1)(X_n^d - 1).
 \end{aligned}
 \tag{10}$$

This deformation satisfies the following conditions, as shall be seen below:

- (i) $F_1(1, X) = \dots = F_n(1, X) = 0$ is the input system;
- (ii) $F_1(0, X) = \dots = F_n(0, X) = 0$ is a zero-dimensional system with a geometric solution easy to compute;
- (iii) If $W := V(F_1, \dots, F_n)$ and $\pi : W \rightarrow \mathbb{A}^1$ is the projection mapping onto the first coordinate, then π is a finite generically-unramified morphism;
- (iv) $\pi^{-1}(0)$ is an unramified fiber of π .

We are going to compute a geometric solution of the variety defined by the system $F_1(T, X) = \dots = F_n(T, X) = 0$ using a global variant of a symbolic Newton–Hensel iteration originally due to [21,23] (see also [7,25,30,32,56]). Then, specializing the polynomials representing this geometric solution into the value $T = 1$, and cleaning up multiplicities, we shall obtain a geometric solution of our input system $F_1(1, X) = \dots = F_n(1, X) = 0$.

First we show that our deformation satisfies conditions (i)–(iv) above. Condition (i) follows directly from the expression of (2) and (10). Our next result proves the validity of conditions (iii) and (iv):

Lemma 9. *π is finite and generically unramified, and $\pi^{-1}(0)$ is unramified.*

Proof. Let us observe that F_i is a polynomial of degree d whose highest nonzero degree term in the variables X is the monomial X_i^d . This shows that $\mathbb{Q}[W]$ is a finite $\mathbb{Q}[T]$ -module and implies the finiteness of the morphism π .

From the Bézout inequality (5) we have that $\#(\pi^{-1}(t)) \leq d^n$ holds for any $t \in \mathbb{A}^1$. On the other hand, the fiber $\pi^{-1}(0)$ consists of the solutions of the system $X_{k+1} - X_k^d = 0$ ($1 \leq k \leq n - 1$), $1 - X_n^d = 0$, which proves that $\#(\pi^{-1}(0)) = d^n$ holds. Hence, from e.g. [28, Proposition 1] or [46, Proposition 3.17] we deduce that there exists a nonempty Zariski open subset \mathcal{U} of \mathbb{A}^n such that $\#(\pi^{-1}(t)) = d^n$ for any $t \in \mathcal{U}$.

Let $t \in \mathcal{U}$. Then $\mathbb{C}[X]/(F_1(t, X), \dots, F_n(t, X))$ is a \mathbb{C} -vector space of dimension at most d^n . Hence, applying e.g. [14, Corollary 2.6] we deduce that $F_1(t, X), \dots, F_n(t, X)$ generates a radical ideal of $\mathbb{C}[X]$. In particular, the Jacobian matrix of $F_1(t, X), \dots, F_n(t, X)$ is nonsingular in any point of $\pi^{-1}(t)$, which shows that the fiber $\pi^{-1}(t)$ is unramified for any $t \in \mathcal{U}$. Furthermore, applying this argument to $t = 0$ we conclude that $\pi^{-1}(0)$ is unramified. \square

Suppose that we are given a linear form $U \in \mathbb{Q}[X]$ which is “lucky” in the sense of [25, §5.3]. Observe that such a linear form separates the points of $\pi^{-1}(0)$, and hence represents a primitive element of the (integral) ring extension $\mathbb{Q}[T] \hookrightarrow \mathbb{Q}[T, X]/(F_1, \dots, F_n)$. Our next result shows that condition (ii) holds.

Lemma 10. *There exists a computation tree which takes as input the polynomials defining $\pi^{-1}(0)$ and the linear form U and outputs a geometric solution of $\pi^{-1}(0)$ using U as primitive element. This computation tree uses space $O(nd^n)$ and time $O(nd^n \mathcal{M}(d^n))$.*

Proof. Let us observe that $\pi^{-1}(0)$ consists of the points of \mathbb{A}^n satisfying the equations $X_{k+1} - X_k^d = 0$ ($1 \leq k \leq n - 1$), $X_n^d - 1 = 0$. By successive substitution we see that $\pi^{-1}(0)$

may be described as the set of solutions of the system $X_k = X_1^{d^{k-1}}$ ($2 \leq k \leq n$), $X_1^{d^n} = 1$. Let $\Lambda_1, \dots, \Lambda_n$ be new indeterminates, and let $U_\Lambda(X) := \Lambda_1 X_1 + \dots + \Lambda_n X_n$. Then, for $q_\Lambda := \text{Res}_{X_1}(X_1^{d^n} - 1, Y - U_\Lambda(X_1, X_1^d, \dots, X_1^{d^{n-1}}))$, it follows that $q_\Lambda(Y) = q(Y) + \sum_{i=1}^n (\Lambda_i - \lambda_i)(X_i q'(Y) - v_i(Y))$ modulo $(\Lambda_1 - \lambda_1, \dots, \Lambda_n - \lambda_n)^2$, where the polynomials $q, v_1, \dots, v_n \in \mathbb{Q}[Y]$ form a geometric solution of $\pi^{-1}(0)$ with $U := \lambda_1 X_1 + \dots + \lambda_n X_n$ as primitive element (see e.g. [25, §3.3]). The computation of q_Λ modulo $(\Lambda_1 - \lambda_1, \dots, \Lambda_n - \lambda_n)^2$ can be done by interpolation in the variable Y . For this purpose, we compute the evaluated resultant $q_\Lambda(\alpha_i)$ modulo $(\Lambda_1 - \lambda_1, \dots, \Lambda_n - \lambda_n)^2$ for $d^n + 1$ different values $\alpha_0, \dots, \alpha_{d^n+1} \in \mathbb{Q}$, using a fast algorithm for computing resultants over a field based on the Extended Euclidean Algorithm (cf. [20]). Our “lucky” choice of U guarantees that executing this algorithm over the power series $\mathbb{Q}[[\Lambda - \lambda]]$, truncating the power series arising during the execution up to order 2, will output the right results. Then, q_Λ modulo $(\Lambda_1 - \lambda_1, \dots, \Lambda_n - \lambda_n)^2$ can be recovered by interpolation (see e.g. [4]). Taking into account the time–space complexity of the algorithms for interpolation and computing resultants the lemma follows. \square

Lemmas 9 and 10 show that our deformation satisfies conditions (i)–(iv) above. Therefore, we may apply the symbolic Newton–Hensel iteration mentioned before. For this purpose, let $U := \lambda_1 X_1 + \dots + \lambda_n X_n \in \mathbb{Q}[X]$ be a “lucky” linear form (in the sense of [25, §5.3]), which also induces a primitive element of the ring extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[\pi^{-1}(1)]$. Let us fix $\rho \geq 4$. From the Zippel–Schwartz test (cf. [61]) and the estimates for the degree of the denominators arising during the execution of Extended Euclidean Algorithm of [20, Theorem 6.54], we see that the coefficients of U can be randomly chosen in the set $\{1, \dots, 16\rho d^{4n}\}$ with probability of success at least $1 - 1/\rho \geq 3/4$.

Let $q, v_1, \dots, v_n \in \mathbb{Q}[Y]$ be the polynomials obtained after applying the algorithm underlying Lemma 10. These polynomials form a geometric solution of $\pi^{-1}(0)$ using U as primitive element. Then we may apply the Algorithm “Lift Curve” of [25, §4.5], which outputs polynomials $Q, V_1, \dots, V_n \in \mathbb{Q}[T, Y]$ which form a geometric solution of $W := V(F_1, \dots, F_n)$, using U as primitive element. Taking into account the tridiagonal form of Jacobian matrix of F_1, \dots, F_n with respect to the variables X , from [7, Theorem 2; 25, Proposition 9] (see also [56, Theorem 2]) we conclude that this algorithm requires space $O(nd^{2n})$ and time $O(nd\mathcal{M}(d^n)^2)$.

Then, specializing Q, V_1, \dots, V_n into the value $T = 1$, we obtain polynomials $Q(1, Y), V_1(1, Y), \dots, V_n(1, Y) \in \mathbb{Q}[Y]$ which represent a complete description of our input system $F_1(1, X) = \dots = F_n(1, X) = 0$, eventually including multiplicities. Such multiplicities are represented by multiple factors of $Q(1, Y)$, which are also factors of $V_1(1, Y), \dots, V_n(1, Y)$ (see e.g. [25, §6.5]). Therefore, they may be removed by computing $M(Y) := \text{gcd}(Q(1, Y), (\partial Q / \partial Y)(1, Y))$, and the polynomials $Q(1, Y)/M(Y), (\partial Q / \partial Y)(1, Y)/M(Y), V_i(1, Y)/M(Y)$ ($1 \leq i \leq n$) which form a geometric solution of our input system, without changing the asymptotic complexity of our procedure. Summarizing, we have

Theorem 11. *There exists a computation tree which takes as input the polynomials F_1, \dots, F_n of (10) and a “lucky” linear form $U \in \mathbb{Q}[X]$, and outputs a geometric solution of the given instance of (2). This computation tree requires space $O(nd^{2n})$ and time*

$O(nd\mathcal{M}(d^n)^2)$, and can be probabilistically built with a probability of success of at least $3/4$.

4.3. Symbolic real root counting and approximation

In this section we briefly sketch an algorithm which, having as input a geometric solution of a given instance of (2), determines the number of positive solutions and computes ε -approximations to all of them.

Let us fix an arbitrary instance $f_1 = \dots = f_n = 0$ of (2). Suppose that we are given a geometric solution of the variety $V \subset \mathbb{A}^n$ defined by f_1, \dots, f_n , as computed by the algorithm underlying Theorem 11. Such a geometric solution consists of a linear form $U \in \mathbb{Z}[X]$ and univariate polynomials $\widehat{q}, \widehat{v}_1, \dots, \widehat{v}_n$ which, without loss of generality, we shall assume to belong to $\mathbb{Z}[Y]$. From the \mathbb{Q} -definability of this geometric solution we easily conclude that the number of real points of V equals the number of real roots of \widehat{q} . Furthermore, the number of positive solutions of $f_1 = \dots = f_n = 0$ is the number of real roots of \widehat{q} satisfying the sign conditions $\widehat{v}_i \geq 0$ ($1 \leq i \leq n$). This quantity can be determined using the algorithm [27, Recipe SI], which yields the number of real roots of a given univariate polynomial satisfying all possible sign conditions $\text{sign}(\widehat{v}_i) = \delta_i$ ($1 \leq i \leq n$). Taking into account that this algorithm requires the computation of $O(nd^n)$ Cauchy indices, and the solution of $O(n)$ linear systems of size $O(d^n)$, we obtain the following result:

Proposition 12. *There exists a computation tree which takes as input a geometric solution of our input system $f_1 = \dots = f_n = 0$ and outputs the number of positive solutions of $f_1 = \dots = f_n = 0$. This computation tree requires space $O(d^{2n})$ and time $O(nd^{3n})$.*

Let us remark that the positive solutions of any instance of (4) can be characterized as the real solutions with positive first coordinate. In such a case, algorithm [27, Recipe SI] can be significantly simplified, and requires space $O(d^n)$ and time $O(\mathcal{M}(d^n))$.

Now we consider the problem of ε -approximating the positive roots of our input system. For this purpose, we represent the real solutions of our input system by means of Thom encodings (see e.g. [27]). Let $p \in \mathbb{Z}[X]$ be a polynomial of degree e and let $p^{(i)}$ ($1 \leq i \leq e-1$) denote the i th derivative of p . For a given real root x_0 of p , its Thom encoding is the list $[p; \xi_{e-1}, \dots, \xi_1]$, where ξ_i is the sign of $p^{(i)}(x_0)$ for $1 \leq i \leq e-1$. The Thom encodings of the real roots of p also allow their ordering (see e.g. [27, Proposition 5.1]).

Let $\widehat{q}_i \in \mathbb{Z}[X]$ denote the minimal equation satisfied by X_i modulo our input system for $1 \leq i \leq n$. By an easy adaptation of [32, Lemma 3] we conclude that there exists a computation tree with space $O(nd^{n+1})$ and time $O(nd^n \mathcal{M}(d^n))$ which takes as input the geometric solution computed by the algorithm underlying Theorem 11 and outputs the polynomials $\widehat{q}_1, \dots, \widehat{q}_n$. Then the Thom encodings of each coordinate of the positive solutions of our input system may be obtained applying the algorithm [27, Recipe SI] to the polynomial \widehat{q} and the list $\widehat{v}_1, \dots, \widehat{v}_n, \widehat{q}_1^{(d^n-1)} \circ \widehat{v}_1, \dots, \widehat{q}_1' \circ \widehat{v}_1, \dots, \widehat{q}_n^{(d^n-1)} \circ \widehat{v}_n, \dots, \widehat{q}_n' \circ \widehat{v}_n$, and identifying the sign conditions $[\zeta_1^{(0)}, \dots, \zeta_n^{(0)}, \zeta_{d^n-1}^{(1)}, \dots, \zeta_1^{(1)}, \dots, \zeta_{d^n-1}^{(n)}, \dots, \zeta_1^{(n)}]$ such that $\zeta_i^{(0)} = +$ holds for $1 \leq i \leq n$.

Furthermore, let be given $\varepsilon > 0$ and an upper bound $\eta > 0$ on the absolute value of the coordinates of the real solutions of our input system. Let us observe that the positive

solutions of any instance of (4) have coordinates upper bounded by $(2(n - 1)\alpha)^{1/d}$. Then, combining the above determination of Thom encodings with a bisection strategy we obtain an algorithm which ε -approximates all the positive roots $x := (x_1, \dots, x_n)$ of our input system satisfying $x_i \leq \eta$ for $1 \leq i \leq n$. This algorithm requires determining the number of real roots of the polynomial \widehat{q} satisfying all possible combinations of sign conditions defined by a list of $O(nd^n \max\{1, \lceil \log(\eta\varepsilon^{-1}) \rceil\})$ polynomials of degree at most d^n . Therefore, we have

Theorem 13. *There exists a computation tree which takes as input a geometric solution of our input system $f_1 = \dots = f_n = 0$ and outputs an ε -approximation of all the positive solutions of $f_1 = \dots = f_n = 0$ with coordinates upper bounded by η , with space $O(nd^{2n} \max\{1, \lceil \log(\eta\varepsilon^{-1}) \rceil\})$ and time $O(nd^{4n} \max\{1, \lceil \log(\eta\varepsilon^{-1}) \rceil\})$.*

5. Real root counting

In this section we exhibit a deformation technique which allows us to determine the number of positive solutions of certain instances of (2), including in particular all the instances of (4). Such deformation technique consists in finding a smooth real homotopy which deforms the system under consideration into a system whose number of positive solutions can be easily determined.

Let X_1, \dots, X_n be indeterminates and let $X := (X_1, \dots, X_n)$. Let f_1, \dots, f_n be polynomials of $\mathbb{Q}[X]$ and let $V_{\mathbb{R}} \subset (\mathbb{R}_{\geq 0})^n$ be the semi-algebraic set consisting of the positive solutions of $f_1 = \dots = f_n = 0$. Let T be a new indeterminate, and suppose that there exist polynomials $F_1, \dots, F_n \in \mathbb{Q}[T, X]$ such that, for

$$W_{\mathbb{R}} := \{(t, x) \in [0, 1] \times (\mathbb{R}_{\geq 0})^n : F_1(t, x) = \dots = F_n(t, x) = 0\},$$

the identity $W_{\mathbb{R}} \cap \{T = 1\} = \{1\} \times V_{\mathbb{R}}$ holds. Let $\pi_{\mathbb{R}} : W_{\mathbb{R}} \rightarrow \mathbb{R}$ be the polynomial mapping defined by $\pi_{\mathbb{R}}(t, x) := t$. Our deformation technique is based on the following result:

Proposition 14. *Suppose that the following conditions hold:*

- $\pi_{\mathbb{R}}$ has no critical values in $[0, 1]$,
- $\#(\pi_{\mathbb{R}}^{-1}(t)) < \infty$ for any $t \in [0, 1]$,
- $W_{\mathbb{R}}$ is a compact subset of \mathbb{R}^{n+1} ,
- $W_{\mathbb{R}} \subset [0, 1] \times (\mathbb{R}_{> 0})^n$.

Then there exists $s \geq 0$ such that $\#(\pi_{\mathbb{R}}^{-1}(t)) = s$ holds for any $t \in [0, 1]$.

Proof. From [33, Lemma 7] we deduce that there exist $s, s' \in \mathbb{N}$ and $\varepsilon \in (0, 1)$ such that the set $\pi_{\mathbb{R}}^{-1}(t)$ has s semi-algebraically connected components for any $t \in [0, \varepsilon]$ and s' semi-algebraically connected components for any $t \in (1 - \varepsilon, 1]$. In particular, we have $\#(\pi_{\mathbb{R}}^{-1}(0)) = s$ and $\#(\pi_{\mathbb{R}}^{-1}(1)) = s'$. Applying [33, Proposition 8] in the interval $(0, 1)$ we conclude that $\#(\pi_{\mathbb{R}}^{-1}(t)) = \#(\pi_{\mathbb{R}}^{-1}(t'))$ for any $t, t' \in (0, 1)$. This shows that $s = s'$ holds and finishes the proof of the proposition. \square

We are going to apply Proposition 14 in order to determine the number of positive solutions of any instance of the following subfamily of (2):

$$\begin{cases} 0 = (n - 1)^2(f(X_2) - f(X_1)) - \frac{1}{2}g(X_1), \\ 0 = (n - 1)^2(f(X_{k+1}) - 2f(X_k) + f(X_{k-1})) - g(X_k) \quad (2 \leq k \leq n - 1), \\ 0 = (n - 1)^2(f(X_{n-1}) - f(X_n)) - \frac{1}{2}g(X_n) + (n - 1)\alpha, \end{cases} \quad (11)$$

where $\alpha > 0$ and f, g are elements of $\mathbb{Q}[X]$, with $d := \deg g > \deg f$ and $f(0) = g(0) = 0$, which define increasing functions in $\mathbb{R}_{\geq 0}$. These hypotheses are satisfied, for example, if f, g are positive monomials with $\deg g > \deg f$.

Let $V_{\mathbb{R}} \subset (\mathbb{R}_{\geq 0})^n$ be the set of positive solutions of (11). In order to apply the deformation technique underlying Proposition 14, we introduce the following polynomials $F_1, \dots, F_n \in \mathbb{Q}[T, X]$:

$$\begin{aligned} F_1 &:= (n - 1)^2(f(X_2) - f(X_1)) - \frac{1}{2}g(X_1), \\ F_k &:= (n - 1)^2(f(X_{k+1}) - (1 + T)f(X_k) + Tf(X_{k-1})) - g(X_k) \quad (2 \leq k \leq n - 1), \\ F_n &:= (n - 1)^2T(f(X_{n-1}) - f(X_n)) - \frac{1}{2}g(X_n) + (n - 1)\alpha, \end{aligned}$$

Let $W_{\mathbb{R}} := \{(t, x) \in [0, 1] \times (\mathbb{R}_{\geq 0})^n : F_1(t, x) = \dots = F_n(t, x) = 0\}$. Observe that $W_{\mathbb{R}} \cap \{T = 1\} = \{1\} \times V_{\mathbb{R}}$ holds. Let $\pi_{\mathbb{R}} : W_{\mathbb{R}} \rightarrow \mathbb{R}$ be the projection mapping onto the first coordinate. We are going to show that F_1, \dots, F_n satisfy all the hypotheses of Proposition 14.

Lemma 15. $\pi_{\mathbb{R}}$ has no critical values in $[0, 1]$.

Proof. Observe that the Jacobian matrix $(\partial F/\partial X)$ of F_1, \dots, F_n with respect to the variables X is the following tridiagonal matrix:

$$(\partial F/\partial X)_{i,j} := \begin{cases} -(n - 1)^2 f'(X_1) - \frac{1}{2}g'(X_1) & \text{for } i = j = 1, \\ -(n - 1)^2(1 + T)f'(X_i) - g'(X_i) & \text{for } 2 \leq i = j \leq n - 1, \\ -(n - 1)^2 T f'(X_n) - \frac{1}{2}(g'(X_n)) & \text{for } i = j = n, \\ (n - 1)^2 f'(X_j) & \text{for } 1 \leq i = j - 1 \leq n - 1, \\ (n - 1)^2 T f'(X_j) & \text{for } 2 \leq i = j + 1 \leq n, \\ 0 & \text{otherwise.} \end{cases}$$

By the conditions satisfied by f, g we easily conclude that $D(t) \cdot (\partial F/\partial X)(t, x)$ is a strictly column diagonally dominant square matrix for any $(t, x) \in (0, 1] \times (\mathbb{R}_{\geq 0})^n$, where $D(t)$ is the following diagonal matrix

$$D(t) := \begin{pmatrix} t^{n-1} & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$

and $(\partial F/\partial X)(0, x)$ is a triangular matrix with positive diagonal for any $x \in (\mathbb{R}_{\geq 0})^n$. Thus $(\partial F/\partial X)(t, x)$ is a nonsingular matrix for any $(t, x) \in [0, 1] \times (\mathbb{R}_{\geq 0})^n$. Therefore, from e.g. [5, §12.3, Proposition 6] we conclude that $\pi_{\mathbb{R}}$ has no critical points in $W_{\mathbb{R}}$, and hence no critical values in $[0, 1]$. \square

Lemma 16. $\pi_{\mathbb{R}}^{-1}(t)$ is a finite set for any $t \in [0, 1]$.

Proof. Let $W \subset \mathbb{A}^{n+1}$ be the affine variety defined by F_1, \dots, F_n . We observe that F_i is a polynomial of degree d whose highest nonzero degree term in the variables X is the monomial X_i^d . This shows that $\mathbb{Q}[W]$ is a finite $\mathbb{Q}[T]$ -module and hence that the projection mapping $\pi : W \rightarrow \mathbb{A}^1$ defined by $\pi(t, x) := t$ is a finite morphism, which implies that $\pi^{-1}(t)$ is a finite set for any $t \in \mathbb{A}^1$. In particular, $\pi_{\mathbb{R}}^{-1}(t)$ is a finite set for any $t \in [0, 1]$. \square

The following result, probably well-known, is included here for lack of a suitable reference.

Lemma 17. $\pi_{\mathbb{R}}$ is a proper morphism, i.e., the preimage of a compact set of $[0, 1]$ is a compact set of $W_{\mathbb{R}}$.

Proof. Let $K \subset [0, 1]$ be a compact set and let $(a_k)_{k \in \mathbb{N}} := (t^{(k)}, x^{(k)})_{k \in \mathbb{N}}$ be a sequence contained in $\pi_{\mathbb{R}}^{-1}(K)$. Then there exists a subsequence of $(t^{(k)})_{k \in \mathbb{N}}$ which converges in K . Therefore, we may assume without loss of generality that the sequence $(t^{(k)})_{k \in \mathbb{N}}$ itself converges to $t \in K$.

Let as before $W \subset \mathbb{A}^{n+1}$ denote the affine variety defined by F_1, \dots, F_n and let $\pi : W \rightarrow \mathbb{A}^1$ be the projection morphism $\pi(t, x) := t$. Since the ring extension $\mathbb{Q}[T] \hookrightarrow \mathbb{Q}[T, X]/(F_1, \dots, F_n)$ is integral (see Lemma 16), if U is a linear form of $\mathbb{Q}[X]$, the minimal polynomial $Q(T, Y)$ of the coordinate function induced by U in this extension is a monic element of $\mathbb{Q}[T][Y]$. The fact that $Q(T, U(X))$ vanishes over W implies that $Q(t^{(k)}, U(x^{(k)})) = 0$ holds for any $k \in \mathbb{N}$.

Since $(t^{(k)})_{k \in \mathbb{N}}$ converges to $t \in K$, we have that $Q(t_k, Y)$ converges, coefficient by coefficient, to $Q(t, Y)$. Taking into account the standard bounds on the absolute value of the complex roots of a univariate polynomial in terms of its coefficients (see e.g. [42]), we conclude that for $k \gg 0$ there exists a uniform bound on the absolute value of the complex roots of the polynomials $Q(t_k, Y)$ and $Q(t, Y)$. This shows that the sequence $(U(x^{(k)}))_{k \in \mathbb{N}}$ is contained in a compact subset of \mathbb{R} , which implies that $(U(x^{(k)}))_{k \in \mathbb{N}}$ has a subsequence converging to a value $u \in \mathbb{R}$ for which $Q(t, u) = 0$ holds. Let us observe that, for a generic choice of U , there exists $x \in W_{\mathbb{R}}$ such that $U(x) = u$ holds, because Q is the minimal polynomial of U in the ring extension induced by π and (t, u) does not annihilate the discriminant of Q with respect to Y .

Our previous argument is valid for any linear form of $\mathbb{Q}[X]$ which separates the points of $\pi^{-1}(t)$. Hence, let $Y_1, \dots, Y_n \in \mathbb{Q}[X]$ be \mathbb{Q} -linearly independent linear forms satisfying this condition. Then, for $U = Y_1$, we obtain a subsequence $(a_{j_k})_{k \in \mathbb{N}}$ of $(a_k)_{k \in \mathbb{N}}$ such that $(Y_1(x^{(j_k)}))_{k \in \mathbb{N}}$ converges to a value $y_1 \in \mathbb{R}$ which equals the evaluation of Y_1 in a point of $\pi_{\mathbb{R}}^{-1}(t)$. Arguing with this subsequence and $U = Y_2$, we obtain a value y_2 which also corresponds to a certain point of $\pi_{\mathbb{R}}^{-1}(t)$. Arguing inductively we conclude that there exists an accumulation point of $(a_k)_{k \in \mathbb{N}}$ in $\pi_{\mathbb{R}}^{-1}(K)$, finishing thus the proof of the lemma. \square

Lemma 17 implies that $W_{\mathbb{R}} = \pi_{\mathbb{R}}^{-1}([0, 1])$ is a compact subset of \mathbb{R}^{n+1} .

Lemma 18. $W_{\mathbb{R}} \subset [0, 1] \times (\mathbb{R}_{>0})^n$.

Proof. Let us recall that $W_{\mathbb{R}}$ is the semi-algebraic set which consists of the points of $(t, x) \in [0, 1] \times (\mathbb{R}_{\geq 0})^n$ satisfying the equations:

$$\begin{cases} 0 = (n-1)^2(f(X_2) - f(X_1)) - \frac{1}{2}g(X_1), \\ 0 = (n-1)^2(f(X_{k+1}) - (1+T)f(X_k) + Tf(X_{k-1})) - g(X_k) \quad (2 \leq k \leq n-1), \\ 0 = (n-1)^2T(f(X_{n-1}) - f(X_n)) - \frac{1}{2}g(X_n) + (n-1)\alpha. \end{cases} \quad (12)$$

Let $(t, x) \in [0, 1] \times (\mathbb{R}_{\geq 0})^n$ be an arbitrary point of $W_{\mathbb{R}}$ and suppose that $x_1 = 0$ holds. Specializing the right-hand side of the first equation of (12) into the value $X = x$ we see that $f(x_2) = 0$ holds. Since f defines a strictly increasing function in $\mathbb{R}_{\geq 0}$ with $f(0) = 0$, we conclude that $x_2 = 0$ holds. We claim that $x_k = 0$ holds for $3 \leq k \leq n$. Arguing inductively, let us fix $3 \leq k \leq n$ and assume that $x_1 = \dots = x_{k-1} = 0$ holds. Specializing the right-hand side of the $(k-1)$ th equation of (12) into the value $X = x$ we see that $f(x_k) = 0$ holds, which implies $x_k = 0$. This completes our inductive argument and shows that $x_{n-1} = x_n = 0$ holds. Then, the last equation of (12) implies $(n-1)\alpha = 0$, which contradicts our hypotheses. We conclude that $x_1 > 0$ holds.

Now we claim that $x_k > 0$ holds for $2 \leq k \leq n$. For this purpose, it suffices to show that $x_{k+1} > x_k$ holds for $1 \leq k < n$. Since $x_1 > 0$ holds and g defines an increasing function in $\mathbb{R}_{\geq 0}$, we have that $(n-1)^2(f(x_2) - f(x_1)) = \frac{1}{2}g(x_1) > 0$ holds, which implies $x_2 > x_1$. Let us fix $1 \leq m < n$ and suppose that $x_{k+1} > x_k$ holds for $1 \leq k < m$. Specializing the right-hand side of the m th equation of (12) into the value $X = x$, we deduce that $(n-1)^2(f(x_{m+1}) - f(x_m)) = (n-1)^2T(f(x_m) - f(x_{m-1})) + g(x_m) > 0$ holds, which implies $x_{m+1} > x_m$. This shows that $x_n > \dots > x_1 > 0$ holds for any $(t, x) \in W_{\mathbb{R}}$. \square

Now we are able to determine the number of positive solutions of (11).

Theorem 19. Let $\alpha > 0$ and let f, g be polynomials of $\mathbb{Q}[X]$ with $d := \deg g > \deg f$ and $f(0) = g(0) = 0$, which define increasing functions in $\mathbb{R}_{\geq 0}$. Then (11) has exactly one solution in $(\mathbb{R}_{\geq 0})^n$.

Proof. Lemmas 15–18 show that $W_{\mathbb{R}}$ and $\pi_{\mathbb{R}} : W_{\mathbb{R}} \rightarrow \mathbb{R}$ satisfy the hypotheses of Proposition 14. We conclude that $\#(\pi_{\mathbb{R}}^{-1}(1)) = \#(\pi_{\mathbb{R}}^{-1}(0))$ holds. Therefore, in order to finish the proof of the theorem there remains to prove that $\#(\pi_{\mathbb{R}}^{-1}(0)) = 1$ holds. We observe that $\pi_{\mathbb{R}}^{-1}(0) = \{0\} \times \tilde{V}_{\mathbb{R}}$ holds, where $\tilde{V}_{\mathbb{R}} \subset (\mathbb{R}_{>0})^n$ is the semi-algebraic set consisting of the points $x := (x_1, \dots, x_n) \in (\mathbb{R}_{>0})^n$ satisfying following polynomial system:

$$\begin{cases} 0 = (n-1)^2(f(X_2) - f(X_1)) - \frac{1}{2}g(X_1), \\ 0 = (n-1)^2(f(X_{k+1}) - f(X_k)) - g(X_k) \quad (2 \leq k \leq n-1), \\ 0 = (n-1)\alpha - \frac{1}{2}g(X_n). \end{cases} \quad (13)$$

Since $g(X_n)$ defines a strictly increasing function in $\mathbb{R}_{\geq 0}$ which satisfies the conditions $\lim_{x \rightarrow +\infty} g(x) = +\infty$ and $g(0) = 0$, we see that there exists a unique positive solution x_n to the equation $(n-1)\alpha - \frac{1}{2}g(X_n) = 0$. Now we show that for $2 \leq k \leq n-1$, there exist unique values $x_k, \dots, x_n \in \mathbb{R}_{\geq 0}$ satisfying the last $n-k+1$ equations of (13). Arguing by induction

on $n - k$, let $1 < k < n$ and assume our statement true for $k + 1$, i.e., there exist unique values $x_{k+1}, \dots, x_n \in \mathbb{R}_{\geq 0}$ satisfying the last $n - k$ equations of (13). Hence, the coordinate $x_k \in \mathbb{R}_{\geq 0}$ must be a solution of the equation $(n - 1)^2 f(x_{k+1}) = 2(n - 1)^2 f(X_k) + g(X_k)$. Since $p(X_k) := 2(n - 1)^2 f(X_k) + g(X_k)$ defines a strictly increasing polynomial function in $\mathbb{R}_{\geq 0}$ and satisfies $p(0) = 0$, we conclude that there exists a unique solution $x_k \in \mathbb{R}_{\geq 0}$ to the equation $(n - 1)^2 f(x_{k+1}) = p(X_k)$. This completes our inductive argument. Finally, in order to prove the uniqueness of $x_1 \in \mathbb{R}_{\geq 0}$, we apply a similar argument as above to the polynomial $\tilde{p}(X_1) := (n - 1)^2 f(X_1) + \frac{1}{2}g(X_1)$. \square

6. Numerical conditioning and complexity of our systems

In this section we are going to analyze the set of positive solutions of (4) for $d \geq 2$ and $\alpha \in \mathbb{Q}_{>0}$ from the numeric point of view. Let us recall that the positive solutions of (4) represent the stationary solutions of the initial value problem (6) of Section 3. The main result of this section asserts that (4) has only one positive solution $x^* \in (\mathbb{R}_{\geq 0})^n$, which is well-conditioned from the numeric point of view. Then, following the homotopy of Section 5 we shall be able to exhibit an algorithm which computes an ε -approximation of x^* with $n^{O(1)}M$ floating point operations, where $M := \log |\log(\varepsilon n^{3-1/d} \alpha d)|$. In particular, we see the difference of behavior between symbolic and numeric conditioning and complexity regarding the positive solution of (4).

We claim that there exists only one positive solution of (4). Indeed, following the ideas of Section 5, we consider the following deformation of (4):

$$\begin{cases} 0 = (n - 1)^2(X_1 - X_2) + \frac{1}{2}X_1^d, \\ 0 = -(n - 1)^2(X_{k+1} - X_k - T(X_k - X_{k-1})) + X_k^d \quad (2 \leq k \leq n - 1), \\ 0 = (n - 1)^2T(X_n - X_{n-1}) - (n - 1)\alpha + \frac{1}{2}X_n^d. \end{cases} \tag{14}$$

Let $W_{\mathbb{R}}$ be the set of positive solutions of (14). From Theorem 19 and Proposition 14 we conclude that $W_{\mathbb{R}} \cap (\{t\} \times (\mathbb{R}_{\geq 0})^n)$, and in particular (4), has only one positive solution for any $t \in [0, 1]$.

6.1. An estimate on the condition number of the positive solution of (14).

Let T, X_1, \dots, X_n be indeterminates over \mathbb{Q} , let $X := (X_1, \dots, X_n)$ and let $F : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n$ denote the polynomial mapping defined by the right-hand side members of (14). Then $F(t, X) = 0$ has exactly one positive solution $(x_1(t), \dots, x_n(t))$ for any $t \in [0, 1]$, which in fact belongs to $(\mathbb{R}_{>0})^n$. Thus, we have defined an analytic function $g : [0, 1] \rightarrow \mathbb{R}^n$ by $g(t) := (x_1(t), \dots, x_n(t))$.

Our intention is to analyze the conditioning of approximating the value $g(1)$ by a continuation homotopy method. Following, e.g. [5], the condition number of approximating $g(t)$ is given by

$$\begin{aligned} \|g'(t)\|_{\infty} &= \|(\partial F / \partial X)(t, g(t))^{-1} \cdot (\partial F / \partial T)(t, g(t))^t\|_{\infty} \\ &\leq \|(\partial F / \partial X)(t, g(t))^{-1}\|_{\infty} \|(\partial F / \partial T)(t, g(t))\|_{\infty}, \end{aligned}$$

where $\|\cdot\|_{\infty}$ denotes the standard infinite norm and $\{\}^t$ denotes transposition.

Let us fix $t \in [0, 1]$. In order to estimate $\|(\partial F/\partial X)(t, g(t))^{-1}\|_\infty$ and $\|(\partial F/\partial T)(t, g(t))\|_\infty$, we are going to find a suitable lower bound for $x_1(t)$ and a suitable upper bound for $x_n(t)$.

From the first $n - 1$ equations of (14) we easily see that $x_2(t), \dots, x_n(t)$ are uniquely determined by t and $x_1(t)$. Therefore, letting x_1 vary, we may consider X_2, \dots, X_n as functions of x_1 , which are indeed recursively defined as follows:

$$\begin{aligned} X_1(x_1) &:= x_1, & X_2(x_1) &:= x_1 + (1/2)(n - 1)^{-2}x_1^d, \\ X_3(x_1) &:= X_2(x_1) + t(X_2(x_1) - x_1) + (n - 1)^{-2}X_2^d(x_1), \\ X_{k+1}(x_1) &:= X_k(x_1) + t(X_k - X_{k-1})(x_1) + (n - 1)^{-2}X_k^d(x_1) \quad \text{for } k \geq 3. \end{aligned} \tag{15}$$

Remark 20. For any $x_1 > 0$ we have:

- (i) $(X_k - X_{k-1})(x_1) > 0$ and $X_k(x_1) > 0$ for $2 \leq k \leq n$.
- (ii) $(X'_k - X'_{k-1})(x_1) > 0$ and $X'_k(x_1) > 0$ for $2 \leq k \leq n$.

Proof. Let $k = 2$. Then, from (15) we have the identities

$$X_2(x_1) - x_1 = (1/2)(n - 1)^{-2}x_1^d, \quad X'_2(x_1) = 1 + (d/2)(n - 1)^{-2}x_1^{d-1}$$

from which we immediately deduce (i) and (ii) for $k = 2$. Now, arguing inductively, suppose our statement true for a given $k \geq 2$. From (15) we have

$$\begin{aligned} (X_{k+1} - X_k)(x_1) &= t(X_k - X_{k-1})(x_1) + (n - 1)^{-2}X_k^d(x_1), \\ (X'_{k+1} - X'_k)(x_1) &= t(X'_k - X'_{k-1})(x_1) + d(n - 1)^{-2}X_k^{d-1}(x_1)X'_k(x_1). \end{aligned}$$

Combining these identities with the inductive hypotheses, we easily conclude that (i) and (ii) hold for $k + 1$. \square

Our next technical result is a critical point in our estimate on the lower bound of $x_1(t)$ for any $t \in [0, 1]$.

Lemma 21. Assume that $d \geq 2$ and $n \geq 3d/2 + 1$ hold, and let $\lambda := 1/d$. For $x_{1,0} := (n - 1)^{-\lambda(2+\lambda)}$ and $t \in [0, 1]$, we have the following estimates for $2 \leq k \leq n$:

$$\begin{aligned} X_k(x_{1,0}) - X_{k-1}(x_{1,0}) &\leq (1/2 + 3(k - 2))(n - 1)^{-(4+\lambda)}, \\ X_k(x_{1,0}) &\leq (n - 1)^{-\lambda(2+\lambda)} + \left(\frac{k-1}{2} + \frac{3}{2}(k - 1)(k - 2)\right)(n - 1)^{-(4+\lambda)}. \end{aligned}$$

Proof. Let $x_{k,0} := X_k(x_{1,0})$ for $2 \leq k \leq n$. By hypothesis, we have

$$\begin{aligned} x_{2,0} &= x_{1,0} + \frac{1}{2}(n - 1)^{-2}x_{1,0}^d = (n - 1)^{-\lambda(2+\lambda)} + \frac{1}{2}(n - 1)^{-(4+\lambda)}, \\ x_{2,0} - x_{1,0} &= \frac{1}{2}(n - 1)^{-(4+\lambda)}. \end{aligned}$$

Arguing inductively, assume the statement true for a given $1 < k < n$. From (15) we have

$$\begin{aligned} x_{k+1,0} - x_{k,0} &= t(x_{k,0} - x_{k-1,0}) + (n - 1)^{-2}x_{k,0}^d \leq x_{k,0} - x_{k-1,0} + (n - 1)^{-2}x_{k,0}^d \\ &\leq \left(\frac{1}{2} + 3(k - 2)\right)(n - 1)^{-(4+\lambda)} + (n - 1)^{-2} \left((n - 1)^{-\lambda(2+\lambda)}\right) \end{aligned}$$

$$+ \left(\frac{k-1}{2} + \frac{3}{2}(k-1)(k-2) \right) (n-1)^{-(4+\lambda)} \Big)^d .$$

We first estimate the second term in the right-hand side of the last expression

$$\begin{aligned} & (n-1)^{-2} \left((n-1)^{-\lambda(2+\lambda)} + \left(\frac{k-1}{2} + \frac{3}{2}(k-1)(k-2) \right) (n-1)^{-(4+\lambda)} \right)^d \\ & \leq (n-1)^{-\lambda d(2+\lambda)-2} \left(1 + \frac{3k^2}{2} (n-1)^{-(4+\lambda)+\lambda(2+\lambda)} \right)^d \\ & \leq (n-1)^{-(4+\lambda)} \left(1 + \frac{3}{2} (n-1)^{-(2+\lambda)(1-\lambda)} \right)^d \\ & \leq (n-1)^{-(4+\lambda)} \left(1 + \frac{3}{2} (n-1)^{-1} \right)^d \quad (\text{for } n \geq 3d/2 + 1) \\ & \leq (n-1)^{-(4+\lambda)} (1 + 1/d)^d \leq 3(n-1)^{-(4+\lambda)}. \end{aligned}$$

Hence, combining this estimate with the previous one we obtain:

$$\begin{aligned} x_{k+1,0} - x_{k,0} & \leq (1/2 + 3(k-2))(n-1)^{-(4+\lambda)} + 3(n-1)^{-(4+\lambda)} \\ & \leq (1/2 + 3(k-1))(n-1)^{-(4+\lambda)}, \end{aligned}$$

which shows our first assertion for $k + 1$. In order to prove our second assertion for $k + 1$, we have

$$\begin{aligned} x_{k+1,0} & \leq x_{k,0} + \left(\frac{1}{2} + 3(k-1) \right) (n-1)^{-(4+\lambda)} \\ & \leq (n-1)^{-\lambda(2+\lambda)} + \left(\frac{k-1}{2} + \frac{3}{2}(k-1)(k-2) \right) (n-1)^{-(4+\lambda)} \\ & \quad + \left(\frac{1}{2} + 3(k-1) \right) (n-1)^{-(4+\lambda)} \\ & \leq (n-1)^{-\lambda(2+\lambda)} + \left(\frac{k}{2} + \frac{3}{2}k(k-1) \right) (n-1)^{-(4+\lambda)}. \end{aligned}$$

This finishes the proof of the lemma. \square

From Lemma 21 we easily deduce the following estimates:

$$\begin{aligned} x_{n,0} - x_{n-1,0} & \leq \left(\frac{1}{2} + 3(n-2) \right) (n-1)^{-(4+\lambda)} \leq 3(n-1)^{-(3+\lambda)} \\ x_{n,0} & \leq (n-1)^{-\lambda(2+\lambda)} + \left(\frac{n-1}{2} + \frac{3}{2}(n-1)(n-2) \right) (n-1)^{-(4+\lambda)} \quad (16) \\ & \leq (n-1)^{-\lambda(2+\lambda)} + 2(n-1)^{-(2+\lambda)}. \end{aligned}$$

6.1.1. A lower bound for $x_1(t)$

Let $Q : [0, 1] \times \mathbb{R} \rightarrow \mathbb{R}$ be the polynomial mapping defined by

$$Q(t, x_1) := t(n-1)^2(X_n(t, x_1) - X_{n-1}(t, x_1)) - (n-1)\alpha + \frac{1}{2}X_n^d(t, x_1). \quad (17)$$

Observe that Q represents the minimal polynomial of the coordinate function defined by X_1 in the integral ring extension $\mathbb{Q}[T] \hookrightarrow \mathbb{Q}[W]$, where W is the affine subvariety of \mathbb{A}^{n+1}

defined by the polynomial system $F(T, X) = 0$ of (14). Therefore, for fixed $t \in [0, 1]$, the (only) positive root of $Q(t, X_1)$ is the value $x_1(t)$ we want to estimate.

From Remark 20 we see that $Q(t, X_1)$ is a strictly increasing function in $\mathbb{R}_{\geq 0}$ for any $t \in [0, 1]$. In particular, taking into account that $Q(t, 0) < 0$ holds, we obtain a new proof of the uniqueness of the positive solution of the system $F(t, X) = 0$ for any $t \in [0, 1]$. Let us assume, as in Lemma 21, that $d \geq 2$ and $n \geq 3d/2 + 1$ hold, and let $x_{1,0} := (n - 1)^{-\lambda(2+\lambda)}$, $x_{2,0} := X_2(x_{1,0}), \dots, x_{n,0} := X_n(x_{1,0})$. From (16) we have

$$\begin{aligned} t(n - 1)^2(x_{n,0} - x_{n-1,0}) &\leq 3t(n - 1)^{-(1+\lambda)} \leq 3(n - 1)^{-1} \\ \frac{1}{2}x_{n,0}^d &\leq \frac{1}{2}((n - 1)^{-\lambda(2+\lambda)} + 2(n - 1)^{-(2+\lambda)})^d \\ &\leq \frac{1}{2}(n - 1)^{-2}(1 + 2(n - 1)^{-1})^d \leq \frac{3}{2}(n - 1)^{-2} \end{aligned}$$

for $n \geq 2d + 1$. We conclude that

$$Q(t, (n - 1)^{-\lambda(2+\lambda)}) \leq 3(n - 1)^{-1} - (n - 1)\alpha + \frac{3}{2}(n - 1)^{-2} < 0$$

holds, provided that $n > 2\alpha^{-1/2} + 1$ holds. Combining this estimate with the fact that $Q(t, X_1)$ is a strictly increasing function in $\mathbb{R}_{\geq 0}$ for any $t \in [0, 1]$, we deduce the following result:

Lemma 22. *Assume that $d \geq 2$ and $n \geq \max\{2d + 1, 2\alpha^{-1/2} + 1\}$ hold. Then, for any $t \in [0, 1]$ we have the following estimate:*

$$(n - 1)^{-\lambda(2+\lambda)} \leq x_1(t). \tag{18}$$

6.1.2. An upper bound for $x_n(t)$

We adapt an idea of [8]. Let $Q : [0, 1] \times \mathbb{R} \rightarrow \mathbb{R}$ be the function defined in (17), and let $x_{1,1}(t) \in \mathbb{R}_{>0}$ be the only positive solution of the equation $X_n(t, X_1) = (2\alpha(n - 1))^\lambda$. Then we have

$$Q(t, x_{1,1}(t)) = (n - 1)^2 t (X_n(t, x_{1,1}) - X_{n-1}(t, x_{1,1})).$$

If $t = 0$, from the above expression we conclude that $x_n(0) = (2\alpha(n - 1))^\lambda$ holds. On the other hand, for $t \in (0, 1]$ we have $Q(t, x_{1,1}(t)) > 0 = Q(t, x_1(t))$, which implies $x_{1,1}(t) > x_1(t)$. Therefore, taking into account that $X_n(t, X_1)$ is a strictly increasing function in $\mathbb{R}_{\geq 0}$ for any $t \in [0, 1]$, we have

Lemma 23. *For any $t \in [0, 1]$ we have the estimate $x_n(t) \leq (2(n - 1)\alpha)^\lambda$.*

6.1.3. An estimate on the condition number of approximating $g(t)$

Let us fix $t \in [0, 1]$. In order to estimate the condition number of approximating $g(t)$, we observe that the Jacobian matrix $\partial F(t, X)/\partial X$ of $F(t, X)$ is tridiagonal with the following

6.2. A numerical algorithm computing the positive solution of (4)

As an illustration of the numerical well-conditioning of the positive solution of the system $F(t, X) = 0$ of (14) for any $t \in [0, 1]$, we shall exhibit a *polynomial* algorithm which computes the only positive solution $g(1)$ of (4). This algorithm is a Newton–Euler continuation method (see e.g. [48]). For this purpose, let us fix $0 < \widehat{\varepsilon} < \alpha$ and let us introduce for any $\eta \in \mathbb{R}$ the polynomial mapping $F_\eta : [0, 1] \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ defined in the following way:

$$F_\eta(T, X) := F(T, X) - (0, \dots, 0, \eta)^t.$$

With the same arguments as in Section 6.1.1 we conclude that $F_\eta(t, X) = 0$ has only one positive solution for any $t \in [0, 1]$ and any $\eta \in \mathbb{R}$ with $|\eta| \leq \widehat{\varepsilon}$.

Let $f(T) := -2T^3 + 3T^2$. Observe that $f(0) = 0$, $f(1) = 1$ and $f([-1/4, 5/4]) = [0, 1]$ hold. Then we have that the semi-algebraic subset of $\mathbb{R} \times (\mathbb{R}_{\geq 0})^n$ defined by the following system of equalities and inequalities:

$$(0, \dots, 0, -\widehat{\varepsilon})^t \leq F(f(T), X) \leq (0, \dots, 0, \widehat{\varepsilon})^t, \quad -1/4 \leq T \leq 5/4,$$

is a compact neighborhood of the real algebraic curve $F(T, X) = 0$, $0 \leq T \leq 1$. Observe that this semi-algebraic set may also be defined as the set of points $(t, g(t, \eta))$ with $t \in [-1/4, 5/4]$ and $|\eta| \leq \widehat{\varepsilon}$, where $g(\eta, t) := (x_{1,\eta}(t), \dots, x_{n,\eta}(t))$ denotes the positive solution of $F_\eta(f(T), X) = 0$.

In order to estimate the complexity of the Newton–Euler method which computes the positive solution of (14), we need an upper bound for $x_{n,\eta}(t)$ and a lower bound for $x_{1,\eta}(t)$, for any $t \in [-1/4, 5/4]$ and any $\eta \in [-\widehat{\varepsilon}, \widehat{\varepsilon}]$. For this purpose, we follow the approach of Section 6.1. More precisely, analogously to (17), we introduce for any $\eta \in \mathbb{R}$ the polynomial mapping $Q_\eta : [0, 1] \times \mathbb{R} \rightarrow \mathbb{R}$ defined in the following way:

$$Q_\eta(t, x_1) := f(t)(n - 1)^2(X_n - X_{n-1})(f(t), x_1) - (n - 1)\alpha - \eta + \frac{1}{2}X_n^d(f(t), x_1).$$

Observe that $Q_\eta(t, X_1)$ is a strictly increasing function in $\mathbb{R}_{>0}$ with $Q_\eta(t, 0) < 0$ for any $t \in [-1/4, 5/4]$. As in the proof of Lemma 23, for any $t \in [-1/4, 5/4]$ we denote by $x_{1,1,\eta}(t)$ the only positive solution of the equation $X_n(f(t), X_1) = (2\alpha(n - 1) + 2\eta)^\lambda$. Then we have

$$Q_\eta(t, x_{1,1,\eta}) = (n - 1)^2 f(t)(X_n - X_{n-1})(f(t), x_{1,1,\eta}(t)) \geq 0 = Q_\eta(t, x_{1,\eta}(t)).$$

We conclude that $x_{1,1,\eta}(t) \geq x_{1,\eta}(t)$, which implies

$$\begin{aligned} (4(n - 1)\alpha)^\lambda &> (2(n - 1)\alpha + 2\eta)^\lambda \\ &= X_n(f(t), x_{1,1,\eta}(t)) > X_n(f(t), x_{1,\eta}(t)) = x_{n,\eta}(t). \end{aligned}$$

On the other hand, assuming that $d \geq 2$ and $n \geq \max\{2d + 1, 2\alpha^{-1/2} + 2\}$ hold, applying Lemma 22 *mutatis mutandis* we deduce that $(n - 1)^{-\lambda(2+\lambda)} \leq x_{1,\eta}(t)$ holds for any $t \in [-1/4, 5/4]$. Therefore, using the estimates of Section 6.1.3 we conclude that the following estimate holds:

$$\|(\partial F_\eta(f(T), X)/\partial X)^{-1}(t, g(\eta, t))\|_\infty \leq 2d^{-1}(n - 1)^{2-\lambda} =: \beta.$$

We also need an upper bound on $\|(\partial^2 F_\eta(f(T), X)/\partial X^2)(t, g(\eta, t))\|_\infty$. For this purpose, we have to estimate the norm of the Hessian matrix of each coordinate of F_η , which is in turn reduced to estimate the quantity $\max_{1 \leq k \leq n} \{d(d-1)X_k(f(t), x_{1,\eta}(t))^{d-2}\}$ for any $t \in [-1/4, 5/4]$ and any $\eta \in [-\widehat{\varepsilon}, \widehat{\varepsilon}]$. We have

$$\begin{aligned} \|(\partial^2 F_\eta(f(T), X)/\partial X^2)(t, g(\eta, t))\|_\infty &\leq d(d-1)x_{n,\eta}(t)^{d-2} \\ &\leq 4d(d-1)(n-1)\alpha =: \gamma. \end{aligned}$$

Finally, we have $\|(\partial F_\eta(f(T), X)/\partial T)(t, g(\eta, t))\|_\infty \leq 4(n-1)^2\alpha =: \delta$.

Then, applying e.g. [48, 10.4.3], we see that there exists $N \leq 4\beta^2\gamma\delta \leq \leq 2^8(n-1)^{7-2\lambda}\alpha^2 = O(n^7)$ such that the following holds:

If $x^{(0)} := g(0)$ denotes the positive solution of $F(0, X) = 0$, and $0 = t_0 < t_1 < \dots < t_N = 1$ is a uniform partition of the interval $[0, 1]$, then the iteration

$$x^{(k+1)} = x^{(k)} - (\partial F(T, X)/\partial X)^{-1}(t_k, x^{(k)})F(t_k, x^{(k)}) \quad (0 \leq k \leq N-1),$$

yields an attraction point of the standard Newton iteration associated to the system $F(1, X) = 0$. Let us remark that, taking into account that the Jacobian matrix $(\partial F(T, X)/\partial X)(t_k, x^{(k)})$ is tridiagonal, we conclude that each step of this iteration requires $O(n^2 \log d)$ floating point operations, keeping $O(n \log d)$ arithmetic registers.

From [48, 10.4.2–3] we conclude that the vector $x^{(N+k)}$, obtained from the vector $x^{(N)}$ above after k steps of the iteration

$$x^{(k+1)} = x^{(k)} - \left((\partial F(1, X)/\partial X)(x^{(k)}) \right)^{-1} F(1, x^{(k)}) \quad (k \geq N),$$

satisfies the estimate $\|x^{(N+k)} - g(1)\|_\infty \leq 2^{-k}(2\beta\gamma)^{-1}$. Furthermore, combining this estimate with [48, 10.2.2] we see that $\|x^{(N+k)} - g(1)\|_\infty \leq 2^{-2k-2}(4\beta\gamma)^{-1} \leq 2^{-2k-2-5}(d-1)^{-1}\alpha^{-1}(n-1)^{\lambda-3}$ holds for $k \geq 2$. Therefore, in order to obtain an ε -approximation of $g(1)$, we have to perform $O(M)$ steps of the second iteration, with $M := \log |\log(\varepsilon n^{3-\lambda}\alpha d)|$. Summarizing, we have

Theorem 25. *There exists a computation tree computing an ε -approximation of the positive solution of (4) with space $O(n \log d)$ and time $O(n^2 \log d(n^7 + M))$, where $M := \log |\log(\varepsilon n^{3-\lambda}\alpha d)|$.*

Acknowledgments

The authors wish to thank Diego Rial, Julio Rossi and Pablo Solernó for their helpful remarks. They are also grateful to the anonymous referees for several suggestions which helped to improve the presentation of the results of this paper.

References

[1] E. Allgower, K. Georg, Numerical continuation methods: an introduction, Springer Series in Computational Mathematics, vol. 13, Springer, New York, 1990.

- [2] C. Bandle, H. Brunner, Blow-up in diffusion equations: a survey, *J. Comput. Appl. Math.* 97 (1–2) (1998) 3–22.
- [3] D. Bayer, D. Mumford, What can be computed in algebraic geometry?, in: D. Eisenbud, L. Robbiano (Eds.), *Computational Algebraic Geometry and Commutative Algebra, Symposia Mathematica*, vol. 34, Cambridge University Press, Cambridge, 1993, pp. 1–49.
- [4] D. Bini, V. Pan, *Polynomial and matrix computations*, Progress in Theoretical Computer Science, Birkhäuser, Boston, 1994.
- [5] L. Blum, F. Cucker, M. Shub, S. Smale, *Complexity and Real Computation*, Springer, New York, Berlin, Heidelberg, 1998.
- [6] J. Bochnack, M. Coste, M.-F. Roy, *Real Algebraic Geometry, Ergebnisse der Mathematik und ihrer Grenzgebiete, Folge 3*, vol. 36, Springer, Berlin, 1998.
- [7] A. Bompadre, G. Matera, R. Wachenchauer, A. Weissbein, Polynomial equation solving by lifting procedures for ramified fibers, *Theoret. Comput. Sci.* 315 (2–3) (2004) 335–369.
- [8] J.F. Bonder, J. Rossi, Blow-up vs. spurious steady solutions, *Proc. Amer. Math. Soc.* 129 (1) (2001) 139–144.
- [9] C. Budd, W. Huang, R. Russell, Moving mesh methods for problems with blow-up, *SIAM J. Sci. Comput.* 17 (2) (1996) 305–327.
- [10] P. Bürgisser, M. Clausen, M. Shokrollahi, *Algebraic Complexity Theory, Grundlehren der mathematischen Wissenschaften*, vol. 315, Springer, Berlin, 1997.
- [11] D. Castro, M. Giusti, J. Heintz, G. Matera, L. Pardo, The hardness of polynomial equation solving, *Found. Comput. Math.* 3 (4) (2003) 347–420.
- [12] M. Chipot, M. Fila, P. Quittner, Stationary solutions, blow up and convergence to stationary solutions for semilinear parabolic equations with nonlinear boundary conditions, *Acta Math. Univ. Comenian.* 60 (1) (1991) 35–103.
- [13] A. Chistov, D. Grigoriev, Subexponential time solving systems of algebraic equations. I, II, LOMI preprints E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.
- [14] D. Cox, J. Little, D. O’Shea, *Using algebraic geometry*, Graduate Texts in Mathematics, vol. 185, Springer, New York, 1998.
- [15] E. Dratman, G. Matera, Deformation techniques for counting the real solutions of specific polynomial equation systems, in: *Proceedings Workshop Argentino de Informática Teórica, WAIT’02*, Santa Fe, Argentina, September 2002, *Anales JAIIO*, vol. 31, SADIO, Buenos Aires, 2002, pp. 42–52.
- [16] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, vol. 150, Springer, New York, 1995.
- [17] R. Ferreira, P. Groisman, J. Rossi, Numerical blow-up for a nonlinear problem with a nonlinear boundary condition, *Math. Models Methods Appl. Sci.* 12 (4) (2002) 461–484.
- [18] W. Fulton, *Intersection theory*, Springer, Berlin, Heidelberg, New York, 1984.
- [19] J. von zur Gathen, Parallel arithmetic computations: a survey, in: J. Gruska, B. Rován, J. Wiedermann (Eds.), *Proceedings of the 12th International Symposium on Mathematics Foundations in Computer Science*, Bratislava, Czechoslovakia, August 25–29, 1986, *Lecture Notes in Computer Science*, vol. 233, Springer, Berlin, 1986, pp. 93–112.
- [20] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge, 1999.
- [21] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, L.M. Pardo, Lower bounds for Diophantine approximation, *J. Pure Appl. Algebra* 117,118 (1997) 277–317.
- [22] M. Giusti, J. Heintz, La détermination des points isolés et de la dimension d’une variété algébrique peut se faire en temps polynomial, in: D. Eisenbud, L. Robbiano (Eds.), *Computational Algebraic Geometry and Commutative Algebra, Symposia Mathematica*, vol. 34, Cambridge University Press, 1993, pp. 216–256.
- [23] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, Straight-line programs in geometric elimination theory, *J. Pure Appl. Algebra* 124 (1998) 101–146.
- [24] M. Giusti, J. Heintz, J. Sabia, On the efficiency of effective Nullstellensätze, *Comput. Complexity* 3 (1993) 56–95.
- [25] M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, *J. Complexity* 17 (1) (2001) 154–211.
- [26] J.L. Gomez, V. Marquez, N. Wolanski, Dynamic behavior of positive solutions to reaction–diffusion problems with nonlinear absorption through the boundary, *Rev. Un. Mat. Argentina* 38 (1993) 196–209.

- [27] L. Gonzalez-Vega, F. Rouillier, M.-F. Roy, G. Trujillo, Symbolic recipes for real solutions, in: A. Cohen et al. (Ed.), *Some tapas in computer algebra*, Algorithms in Computational Mathematics, vol. 4, Springer, Berlin, 1999, pp. 121–167.
- [28] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, *Theoret. Comput. Sci.* 24 (3) (1983) 239–277.
- [29] J. Heintz, G. Jerónimo, J. Sabia, J. San Martín, P. Solernó, *Intersection Theory and Deformation Algorithms: The Multihomogeneous Case*, Manuscript, University of Buenos Aires, 2002.
- [30] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, Deformation techniques for efficient polynomial equation solving, *J. Complexity* 16 (1) (2000) 70–109.
- [31] J. Heintz, G. Matera, L. Pardo, R. Wachenchauser, The intrinsic complexity of parametric elimination methods, *Electron. J. SADIO* 1 (1) (1998) 37–51.
- [32] J. Heintz, G. Matera, A. Waissbein, On the time–space complexity of geometric elimination procedures, *Appl. Algebra Eng. Comm. Comput.* 11 (4) (2001) 239–296.
- [33] J. Heintz, M.-F. Roy, P. Solernó, Description des composantes connexes d’un ensemble semialgébrique en temps simplement exponentiel, *C. R. Math. Acad. Sci.* 313 (1991) 167–170.
- [34] D. Henry, *Geometric theory of semilinear parabolic equations*, Lecture Notes in Mathematics, vol. 840, Springer, New York, 1981.
- [35] B. Huber, B. Sturmfels, A polyhedral method for solving sparse polynomial systems, *Math. Comp.* 64 (112) (1995) 1541–1555.
- [36] B. Huber, B. Sturmfels, Bernstein’s Theorem in affine space, *Discrete Comput. Geom.* 17 (1997) 137–141.
- [37] H. Levine, The role of critical exponents in blow up theorems, *SIAM Rev.* 32 (1990) 262–288.
- [38] T. Li, Numerical solution of multivariate polynomial systems by homotopy continuation methods, *Acta Numer.* 6 (1997) 399–436.
- [39] T. Li, X. Wang, Solving real polynomial systems with real homotopies, *Math. Comp.* 60 (202) (1993) 669–680.
- [40] T. Lickteig, M.-F. Roy, Sylvester–Habicht sequences and fast Cauchy index computation, *J. Symbolic Comput.* 31 (3) (2001) 315–341.
- [41] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, Cambridge, 1986.
- [42] M. Mignotte, *Mathematics for Computer Algebra*, Springer, New York, 1992.
- [43] J. Moré, A collection of nonlinear model problems, in: E. Allgower, K. Georg (Eds.), *Computational solution of nonlinear systems of equations*, American Mathematical Society, Providence, RI, 1990, pp. 723–762.
- [44] A. Morgan, *Solving polynomial systems using continuation for engineering and scientific problems*, Prentice-Hall, Englewood Cliffs, NJ, 1987.
- [45] A. Morgan, A. Sommese, C. Wampler, A generic product-decomposition formula for Bézout numbers, *SIAM J. Numer. Anal.* 32 (1995) 1308–1325.
- [46] D. Mumford, *Algebraic Geometry I. Complex Projective Varieties*, 2nd ed., Classics in Mathematics, Springer, Berlin, 1995.
- [47] R. Nabben, Two-side bounds on the inverses of diagonally dominant tridiagonal matrices, *Linear Algebra Appl.* 287 (1–3) (1998) 289–305.
- [48] J. Ortega, W. Rheinboldt, *Iterative solutions of nonlinear equations in several variables*, Academic Press, New York, 1970.
- [49] C. Pao, *Nonlinear Parabolic and Elliptic Equations*, Plenum Press, New York, 1992.
- [50] L. Pardo, Universal elimination requires exponential running time, in: A. Montes (Ed.), *Computer Algebra and Applications*, Proceedings of EACA–2000, Barcelona, Spain, September 2000, pp. 25–51.
- [51] L. Pardo, J. San Martín, Deformation techniques to solve generalized Pham systems, *Theoret. Comput. Sci.* 315 (2–3) (2004) 593–625.
- [52] L. Perko, *Differential equations and dynamical systems*, 2nd ed., Texts in Applied Mathematics, vol. 7, Springer, Berlin, 1996.
- [53] M. Rojas, Why polyhedra matter in non-linear equation solving, in: Proceedings Conference on Algebraic Geometry and Geometric Modelling, (Vilnius, Lithuania, July 29–August 2, 2002), Contemporary Mathematics, vol. 334, American Mathematical Society, Providence, RI, 2003, pp. 293–320.
- [54] A. Samarskii, V. Galaktionov, S. Kurdyumov, A. Mikhailov, Blow-up in quasilinear parabolic equations, de Gruyter Experimental Mathematics, vol. 19, de Gruyter, Berlin, 1995.

- [55] J. Savage, *Models of Computation. Exploring the Power of Computing*, Addison-Wesley, Reading, MA, 1998.
- [56] E. Schost, Computing parametric geometric resolutions, *Appl. Algebra Eng. Comm. Comput.* 13 (2003) 349–393.
- [57] I. Shafarevich, *Basic Algebraic Geometry: Varieties in Projective Space*, Springer, Berlin, Heidelberg, New York, 1994.
- [58] A. Sommese, J. Verschelde, C. Wampler, Numerical decomposition of the solution sets of polynomial systems into irreducible components, *SIAM J. Numer. Anal.* 38 (6) (2001) 2022–2046.
- [59] J. Verschelde, K. Gatermann, R. Cools, Mixed volume computation by dynamic lifting applied to polynomial system solving, *Discrete Comput. Geom.* 16 (1) (1996) 69–112.
- [60] J. Verschelde, P. Verlinden, R. Cools, Homotopies exploiting Newton polytopes for solving sparse polynomial systems, *SIAM J. Numer. Anal.* 31 (3) (1994) 915–930.
- [61] R. Zippel, *Effective Polynomial Computation*, Kluwer International Series in Engineering and Computer Science, Kluwer Academic Publishers, Dordrecht, 1993.