Faster real root decision algorithm for symmetric polynomials

George Labahn
Cheriton School of Computer Science
University of Waterloo, Ontario, Canada

Cordian Riener
Department of Mathematics and Statistics
UiT, The Arctic University of Norway, Tromsø, Norway

Mohab Safey El Din
Sorbonne Université, CNRS, LIP6
F-75005 Paris, France

Éric Schost
Cheriton School of Computer Science
University of Waterloo, Ontario, Canada

Thi Xuan Vu
Department of Mathematics and Statistics
UiT, The Arctic University of Norway, Tromsø, Norway

ABSTRACT

In this paper, we consider the problem of deciding the existence of real solutions to a system of polynomial equations having real coefficients, and which are invariant under the action of the symmetric group. We construct and analyze a Monte Carlo probabilistic algorithm which solves this problem, under some regularity assumptions on the input, by taking advantage of the symmetry invariance property.

The complexity of our algorithm is polynomial in d^s, $\binom{n+d}{d}$, and $\binom{n}{s+1}$, where n is the number of variables and d is the maximal degree of s input polynomials defining the real algebraic set under study. In particular, this complexity is polynomial in n when d and s are fixed and is equal to $n^{O(1)}2^n$ when $d = n$.

1 INTRODUCTION

Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ be polynomials in the multivariate polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$ and let $V(\boldsymbol{f}) \subset \mathbb{C}^n$ be the algebraic set defined by $\boldsymbol{f}$. We denote by $V_{\mathbb{R}}(\boldsymbol{f}) := V(\boldsymbol{f}) \cap \mathbb{R}^n$ the set of solutions in $\mathbb{R}^n$ to the system $\boldsymbol{f}$. In addition we assume that all f_i's are invariant under the action of the symmetric group S_n, that is, are symmetric polynomials (or equivalently, S_n-invariant polynomials).

Under this invariance property, we design an algorithm which, on input $\boldsymbol{f}$, decides whether $V_{\mathbb{R}}(\boldsymbol{f})$ is empty or not. As is typical for such problems, we assume that the Jacobian matrix of $\boldsymbol{f}$ with respect to $x_1, \ldots, x_n$ has rank s at any point of $V(\boldsymbol{f})$. In this case the Jacobian criterion [23, Thm 16.19] implies that the complex algebraic set $V(\boldsymbol{f})$ is smooth and $(n-s)$-equidimensional (or empty).

Previous work. The real root decision problem for polynomial systems of equations (and more generally systems of inequalities) lies at the foundations of computational real algebraic geometry. Algorithms for solving polynomial systems over the real numbers start with Fourier [30] who provided a first algorithm for solving linear systems of inequalities (rediscovered in 1919 by Dines [22]). These algorithms are important because they make the first connection with elimination theory. Tarski's theorem [55] states that the projection of a semi-algebraic set on a coordinate subspace is a semi-algebraic set. This theorem, and its algorithmic counterpart which relies on Sturm's theorem for real root counting in the univariate case, enable recursive algorithmic patterns (eliminating variables one after another). The first algorithm with an elementary recursive complexity, *Cylindrical Algebraic Decomposition*, is due to Collins (see [20] and references in [17, 18, 25, 36, 38, 39, 52, 53] for various further improvements).

It turns out that these algorithms run in time doubly exponential in n [14, 21]. Note that some variants actually solve the quantifier elimination problem, a much more general and difficult computational problem than the real root decision problem.

Algorithms which solve the real root decision problem in time singly exponential in n and polynomial in the maximum degree of the input were pioneered by Grigoriev and Vorobjov [33] and Renegar [41], and further improved by Canny [16], Heintz, Roy and Solernó [35] and Basu, Pollack and Roy [8]. The method used in this framework is referred to as the *critical point method*. It reduces the real root decision problem to the computation of finitely many complex critical points of a polynomial map which reaches extrema at each connected component of the semi-algebraic set under study.

The algorithm proposed here for solving the real root decision problem for systems of symmetric polynomial equations also builds on the critical point method. It borrows ideas from probabilistic algorithms which have been designed to obtain sharper complexity estimates (e.g. cubic either in some Bézout bound attached to some critical point system or in some geometric intrinsic degree) and obtain practical performances that reflect the complexity gains [2–7, 46]. These algorithms make use of geometric resolution or symbolic homotopy techniques to control the complexity of the algebraic elimination step (see e.g. [32, 47] and references therein), and of regularity assumptions to easily derive critical point systems from the input polynomials.

Under the Jacobian criterion assumptions, critical points are defined as the intersection of the affine variety $V(\boldsymbol{f})$ with a determinantal variety derived from a certain Jacobian matrix. The design of dedicated algebraic elimination algorithms for this particular setting has attracted some attention already [1, 28, 34, 48, 51]. When adding the symmetry property to polynomials defining the variety

ISSAC 2023, July 24–27, 2023, Tromsø, Norway

ACM ISBN 979-8-4007-0039-2/23/07.
https://doi.org/10.1145/3597066.3597097

and the polynomial map for which one computes the critical points, significant improvements have been achieved recently in [26] by using the symbolic homotopy algorithms in [37].

These improvements, which allows one to obtain complexity gains related to the combinatorial complexity of the symmetric group, also borrow ideas from algebraic algorithms working with data which are invariant by the action of this group [29]. We emphasize that taking advantage of symmetries in data is a topical and difficult issue, which involves a variety of methodologies [15, 19, 27, 40, 54].

In [56], Timofte proves a breakthrough result which is now known as the degree principle. It states that a symmetric polynomial of degree d with real coefficients has real solutions if and only if one of these solutions has at most d distinct coordinates.

This shows that when d is fixed and n grows, the real root decision problem can be solved in polynomial time. This is far better than computing at least one sample point per connected component (see also [10–12]), and is one of the rare interesting cases where the best known algorithms for these two problems admit different complexities. This is also the starting point of several results which enhance the real root decision problem and polynomial optimization under some S_n-invariance property for classes of problems where d remains fixed and n grows (see [31, 42, 43, 45] and [44] for equivariant systems).

Main contributions. Being able to leverage S_n-invariance for critical point computations is not sufficient to solve root decision problems more efficiently using the critical point method. Additional techniques are needed.

Indeed, to solve the real root decision problem by finding the critical points of a polynomial map ϕ, one typically defines ϕ as the distance from points on the variety to a generic point. This map reaches extrema at each connected component of the semi-algebraic set under study. However, the map ϕ is not symmetric. If it was, our problem would be solved by the critical point algorithm of [26]. Unfortunately there does not appear to be an obvious symmetric map that fits the bill.

Instead, our approach is to apply the critical point method on individual S_n-orbits, with suitable ϕ found for each orbit. Thus while we cannot use the critical point algorithm of [26] directly we can make use of the various subroutines used in it to construct a fast decision procedure. Intuitively, working with S_n-orbits is the same as separately searching for real points having distinct coordinates, or real points having two or more coordinates which are the same, or groups of coordinates each of which has equal coordinates and so on. In each case an orbit can be described by points having n or fewer pairwise distinct coordinates, a key observation in constructing generic maps invariant for each orbit.

Theorem 1.1. *Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ be symmetric polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ having maximal degree d. Assume that the Jacobian matrix of $\boldsymbol{f}$ with respect to $x_1, \ldots, x_n$ has rank s at any point of $V(\boldsymbol{f})$. Then there is a Monte Carlo algorithm* Real_emptiness *which solves the real root decision problem for $\boldsymbol{f}$ with*

$$O^{\sim}\left(d^{6s+2}n^{11}\binom{n+d}{n}^6\left(\binom{n+d}{n}+\binom{n}{s+1}\right)\right) \subset \left(d^s\binom{n+d}{n}\binom{n}{s+1}\right)^{O(1)}$$

operations in $\mathbb{Q}$. Here the notion $O^{\sim}$ indicates that polylogarithmic factors are omitted.

The remainder of the paper proceeds as follows. The next section reviews known material, on invariant polynomials over products of symmetric groups, the tools we use to work with S_n-orbits, and our data structures. Section 3 discusses our smoothness requirement and shows that it is preserved by alternate representations of invariant polynomials. Section 4 shows how we construct critical point functions along with their critical point set. This is followed in Section 5 by a description of our algorithm along with a proof of correctness and complexity. The paper ends with a section on topics for future research.

2 PRELIMINARIES

2.1 Invariant Polynomials

We briefly review some properties of polynomials invariant under the action of $S_{t_1} \times \cdots \times S_{t_k}$, with S_{t_i} the symmetric group on t_i elements, for all i. In this paragraph, we work with variables $\boldsymbol{z} = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k)$, with each $\boldsymbol{z}_i = (z_{1,i}, \ldots, z_{t_i,i})$; for all i, the group S_{t_i} permutes the variables $\boldsymbol{z}_i$. For $j \geq 0$, we denote by

$$E_{j,i} = \sum_{1 \leq m_1 < m_2 < \cdots < m_j \leq t_i} z_{m_1,i} z_{m_2,i} \cdots z_{m_j,i},$$

the elementary polynomial in the variables $\boldsymbol{z}_i$, with each $E_{j,i}$ having degree j, and by

$$P_{j,i} = z_{1,i}^j + \cdots + z_{t_i,i}^j$$

the j-th Newton sum in the variables $\boldsymbol{z}_i$, for $i = 1, \ldots, k$. The following two results are well-known.

For $i = 1, \ldots, k$, let $\boldsymbol{e}_i = (e_{1,i}, \ldots, e_{t_i,i})$ be a set of t_i new variables and let $\boldsymbol{E}_i = (E_{1,i}, \ldots, E_{t_i,i})$; we write $\boldsymbol{e} = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)$ and $\boldsymbol{E} = (\boldsymbol{E}_1, \ldots, \boldsymbol{E}_k)$.

Lemma 2.1. *Let $g \in [\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k]$ be invariant under the action of $S_{t_1} \times \cdots \times S_{t_k}$. Then there exists a unique γ_g in $\mathbb{Q}[\boldsymbol{e}]$ such that $g = \zeta_g(\boldsymbol{E})$.*

Similarly, let $p_{j,i}$ be new variables, and consider the sequences $\boldsymbol{p}_i = (p_{1,i}, \ldots, p_{t_i,i})$ and $\boldsymbol{p} = (\boldsymbol{p}_1, \ldots, \boldsymbol{p}_k)$, together with their polynomial counterparts $\boldsymbol{P}_i = (P_{1,i}, \ldots, P_{t_i,i})$ and $\boldsymbol{P} = (\boldsymbol{P}_1, \ldots, \boldsymbol{P}_k)$.

Lemma 2.2. *Let $g \in [\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k]$ be invariant under the action of $S_{t_1} \times \cdots \times S_{t_k}$. Then there exists a unique ζ_g in $\mathbb{Q}[\boldsymbol{p}]$ such that $g = \gamma_g(\boldsymbol{P})$.*

Example 2.3. *Let*

$$g = 2(z_{1,1}z_{2,1} + z_{1,1}^2 + 2z_{1,1}z_{2,1} + z_{2,1}^2)(z_{1,2}^2 + z_{2,2}^2),$$

a polynomial invariant under $S_2 \times S_2$, with $\boldsymbol{z}_1 = (z_{1,1}, z_{2,1})$, $\boldsymbol{z}_2 = (z_{1,2}, z_{2,2})$, $k = 2$ and $t_1 = t_2 = 2$. In this case, we have

$$g = (3P_{1,1}^2 - P_{1,2})P_{2,2}$$

and hence $\gamma_g = (3p_{1,1}^2 - p_{1,2})p_{2,2} \in \mathbb{Q}[p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}]$.

2.2 Describing S_n-orbits via Partitions

S_n-orbits are subsets of $\mathbb{C}^n$ that play a central role in our algorithm. In this section, we review notation and description of S_n-orbits, along with the form of the output used in [26].

A simple way to parameterize S_n-orbits is through the use of partitions of n. A sequence $\lambda = (n_1^{t_1} \ \dots \ n_k^{t_k})$, where $n_1 < \cdots < n_k$ and n_i's and t_i's are positive integers, is called a partition of n if $n_1t_1 + \cdots + n_kt_k = n$. The *length* of the partition λ is defined as $\ell := t_1 + \cdots + t_k$.

For a partition $\lambda = (n_1^{t_1} \ \dots \ n_k^{t_k})$ of n, we use the notation from [26, Section 2.3] and let U_λ denote the set of all points $\boldsymbol{u}$ in $\mathbb{C}^n$ that can be written as

$$\boldsymbol{u} = (\underbrace{u_{1,1},\dots,u_{1,1}}_{n_1},\ \dots,\ \underbrace{u_{t_1,1},\dots,u_{t_1,1}}_{n_1},\ \dots,\ \underbrace{u_{1,k},\dots,u_{1,k}}_{n_k},\ \dots,\ \underbrace{u_{t_k,k},\dots,u_{t_k,k}}_{n_k}). \quad (1)$$

For any point $\boldsymbol{u}$ in $\mathbb{C}^n$, we define its *type* as the unique partition λ of n such that there exists $\sigma \in S_n$ such that $\sigma(\boldsymbol{u}) \in U_\lambda$, with the $u_{i,j}$'s in (1) pairwise distinct. Points of a given type $\lambda = (n_1^{t_1} \ \dots \ n_k^{t_k})$ are stabilized by the action of $S_\lambda := S_{t_1} \times \cdots \times S_{t_k}$, the cartesian product of symmetric groups S_{t_i}.

For a partition λ as above, we can then define a mapping $F_\lambda : U_\lambda \to \mathbb{C}^\ell$ as

$$\boldsymbol{u} \text{ as in (1)} \mapsto (E_{1,i}(u_{1,i},\dots,u_{t_i,i}),\dots,E_{t_i,i}(u_{1,i},\dots,u_{t_i,i}))_{1\le i\le k},$$

where $E_{j,i}(u_{1,i},\dots,u_{t_i,i})$ is the j-th elementary symmetric function in $u_{1,i},\dots,u_{t_i,i}$ for $i = 1,\dots,k$ and $j = 1,\dots,t_i$. One can think of the map F_λ as a compression of orbits. By applying this map, we can represent an S_n-orbit $\mathcal{O}$ of type λ by the single point $F_\lambda(\mathcal{O} \cap U_\lambda)$.

Furthermore, the map F_λ is onto: for any $\boldsymbol{c} = (c_{1,1},\dots,c_{t_k,k}) \in \mathbb{C}^\ell$, we define polynomials $\rho_1(u),\dots,\rho_k(u)$ by

$$\rho_i(T) = T^{t_i} - c_{1,i}T^{t_i-1} + \cdots + (-1)^{t_i}c_{t_i,i}.$$

We can then find a point $\boldsymbol{u} \in \mathbb{C}^n$ in the preimage $F_\lambda^{-1}(\boldsymbol{c})$ by finding the roots $u_{1,i},\dots,u_{t_i,i}$ of $\rho_i(T)$.

2.3 Zero-Dimensional Parametrizations

The subroutines we use from [26] give their output in terms of *zero-dimensional parametrizations*, which are defined as follows. Let $W \subset \mathbb{C}^n$ be a variety of dimension zero, defined over $\mathbb{Q}$. A zero-dimensional parametrization $\mathscr{R} = ((v, v_1,\dots,v_n), \mu)$ of W is

(i) a squarefree polynomial v in $\mathbb{Q}[t]$, where t is a new indeterminate, and $\deg(v) = |W|$,

(ii) polynomials $v_1,\dots,v_n$ in $\mathbb{Q}[t]$ such that $\deg(v_i) < \deg(v)$ for all i and

$$W = \left\{\left(\frac{v_1(\tau)}{v'(\tau)},\dots,\frac{v_n(\tau)}{v'(\tau)}\right) \in \mathbb{C}^n \ :\ v(\tau) = 0\right\},$$

(iii) a linear form μ in n variables such that $\mu(v_1,\dots,v_n) = tv'$ (so the roots of v are the values taken by μ on W).

When these conditions hold, we write $W = Z(\mathscr{R})$. Representing the points of W by means of rational functions with v' as denominator is not necessary, but allows for a sharp control of the bit-size of the output.

3 PRESERVING SMOOTHNESS

In our main algorithm, we assume that our input system $\boldsymbol{f} = (f_1,\dots,f_s)$ satisfies the following smoothness condition

(A) : *the Jacobian matrix of $\boldsymbol{f}$ has rank s at any point of $V(\boldsymbol{f})$.*

In this section, we discuss consequences of this assumption for symmetric polynomials.

Mapping to orbits: the map $\mathbb{T}_\lambda$. For a partition $\lambda = (n_1^{t_1} \ \dots \ n_k^{t_k})$ of n, we define the $\mathbb{Q}$-algebra homomorphism $\mathbb{T}_\lambda : \mathbb{Q}[x_1,\dots,x_n] \to \mathbb{Q}[z_1,\dots,z_k]$, with $z_i = (z_{1,i},\dots,z_{t_i,i})$ for all i, which maps the variables $x_1,\dots,x_n$ to

$$\underbrace{z_{1,1},\dots,z_{1,1}}_{n_1},\ \dots,\ \underbrace{z_{t_1,1},\dots,z_{t_1,1}}_{n_1},\ \dots,\ \underbrace{z_{1,k},\dots,z_{1,k}}_{n_k},\ \dots,\ \underbrace{z_{t_k,k},\dots,z_{t_k,k}}_{n_k}. \quad (2)$$

The operator $\mathbb{T}_\lambda$ extends to vectors of polynomials and polynomial matrices entry-wise. The key observation here is that if f is symmetric, then its image through $\mathbb{T}_\lambda$ is $S_{t_1} \times \cdots \times S_{t_k}$-invariant.

Fix a partition $\lambda = (n_1^{t_1} \ \dots \ n_k^{t_k})$ of n, and let ℓ be its length. Set

$$I_{j,i} := \{\sigma_{j,i} + 1,\dots,\sigma_{j,i} + n_i\}, 1 \le i \le k; 1 \le j \le t_i$$

with $\sigma_{j,i} := \sum_{r=1}^{i-1} t_r n_r + (j-1)n_i$. Variables x_m, for m in $I_{j,i}$, are precisely those that map to $z_{j,i}$ under $\mathbb{T}_\lambda$. Define further the matrix $Z \in \mathbb{Q}^{\ell \times n}$ with $\ell = t_1 + \cdots + t_k$, where rows are indexed by pairs (j,i) as above and columns by $m \in \{1,\dots,n\}$. For all such (j,i), the entry of row index (j,i) and column index $m \in I_{j,i}$ is set to $1/n_i$, all others are zero. In other words, $Z = \operatorname{diag}(Z_1,\dots,Z_k)$, where

$$Z_i = \begin{pmatrix} \frac{1}{n_i} & \cdots & \frac{1}{n_i} & & \mathbf{0} & & \cdots & & \mathbf{0} & \\ & \mathbf{0} & & \frac{1}{n_i} & \cdots & \frac{1}{n_i} & \cdots & & \mathbf{0} & \\ & \vdots & & & & & \ddots & & \vdots & \\ & \mathbf{0} & & & \mathbf{0} & & \cdots & \frac{1}{n_i} & \cdots & \frac{1}{n_i} \end{pmatrix}$$

is a matrix in $\mathbb{Q}^{t_i \times n_i t_i}$.

Example 3.1. *Consider the partition $\lambda = (2^2\,3^1)$ of $n = 7$. Then $n_1 = 2, t_1 = 2, n_2 = 3, t_2 = 1$ and the length of λ is 3. In this case,*

$$Z = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & & & & & \\ & & \frac{1}{2} & \frac{1}{2} & & & \\ & & & & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}.$$

Lemma 3.2. *Let $\boldsymbol{f} = (f_1,\dots,f_s) \subset \mathbb{Q}[x_1,\dots,x_n]$ be a sequence of symmetric polynomials, and let λ be a partition of n. Then*

$$\mathbb{T}_\lambda(\operatorname{Jac}_{x_1,\dots,x_n}(\boldsymbol{f})) = \operatorname{Jac}_{z_1,\dots,z_k}(\mathbb{T}_\lambda(\boldsymbol{f})) \cdot Z,$$

where Z is the matrix defined above.

Proof. For any polynomial f in $\mathbb{Q}[x_1,\dots,x_n]$, applying the operator $\mathbb{T}_\lambda$ on f evaluates f at $x_m = z_{j,i}$ for $1 \le i \le k$, $1 \le j \le t_i$

and m in $I_{j,i}$. By the multivariable chain rule,

$$\frac{\partial \mathbb{T}_\lambda(f)}{\partial z_{j,i}} = \sum_{m \in I_{j,i}} \mathbb{T}_\lambda\left(\frac{\partial f}{\partial x_m}\right).$$

If f is symmetric, for m, m' in $I_{j,i}$, we then have

$$\mathbb{T}_\lambda\left(\frac{\partial f}{\partial x_m}\right) = \mathbb{T}_\lambda\left(\frac{\partial f}{\partial x_{m'}}\right),$$

so that, for m in $I_{j,i}$,

$$\mathbb{T}_\lambda\left(\frac{\partial f}{\partial x_m}\right) = \frac{1}{n_i}\frac{\partial \mathbb{T}_\lambda(f)}{\partial z_{j,i}}.$$

This argument can be extended to a sequence of polynomials to obtain our claim. □

Example 3.3. *We continue Example 3.1 with a single S_7-invariant polynomial $f = \sum_{1\le i\le j\le 7} x_i x_j$. Then*

$$\mathbb{T}_\lambda(f) = 3z_{1,1}^2 + 3z_{2,1}^2 + 6z_{1,2}^2 + 6z_{1,1}z_{1,2} + 4z_{1,1}z_{2,1} + 6z_{1,2}z_{2,1},$$

and so

$$\mathrm{Jac}(\mathbb{T}_\lambda(f)) = (6z_{1,1}+6z_{1,2}+4z_{2,1}, 4z_{1,1}+6z_{1,2}+6z_{2,1}, 6z_{1,1}+12z_{1,2}+6z_{2,1}).$$

This implies that $\mathrm{Jac}(\mathbb{T}_\lambda(f)) \cdot Z$ *is equal to* (u, u, v, v, w, w, w), *with*

$$u = 3z_{1,1}+3z_{1,2}+2z_{2,1},\ v = 2z_{1,1}+3z_{1,2}+3z_{2,1},\ w = 2z_{1,1}+4z_{1,2}+2z_{2,1}.$$

This is precisely $\mathbb{T}_\lambda(\mathrm{Jac}(f))$.

Corollary 3.4. *Under the assumptions of the previous lemma, if $\boldsymbol{f}$ satisfies condition* (A), *then $\mathbb{T}_\lambda(\boldsymbol{f}) \subset \mathbb{Q}[z_1, \ldots, z_k]$ does as well.*

Proof. Let $\boldsymbol{\alpha} = (\alpha_{1,1}, \ldots, \alpha_{t_1,1}, \ldots, \alpha_{1,k}, \ldots, \alpha_{t_k k})$ be a zero of $\mathbb{T}_\lambda(\boldsymbol{f})$ in $\mathbb{C}^\ell$. We have to prove that $\mathrm{Jac}_{z_1,\ldots,z_k}(\mathbb{T}_\lambda(\boldsymbol{f}))(\boldsymbol{\alpha})$ has a trivial left kernel.

Consider the point

$$\boldsymbol{\varepsilon} = \big(\underbrace{\alpha_{1,1}, \ldots, \alpha_{1,1}}_{n_1}, \ldots, \underbrace{\alpha_{t_1,1}, \ldots, \alpha_{t_1,1}}_{n_1}, \ldots, \underbrace{\alpha_{1,k}, \ldots, \alpha_{1,k}}_{n_k}, \ldots, \underbrace{\alpha_{t_k,k}, \ldots, \alpha_{t_k,k}}_{n_k}\big) \in \mathbb{C}^n, \quad (3)$$

which lies in $V(\boldsymbol{f})$. In particular, for any g in $\mathbb{Q}[x_1, \ldots, x_n]$, we have $\mathbb{T}_\lambda(g)(\boldsymbol{\alpha}) = g(\boldsymbol{\varepsilon})$. Applying this to the Jacobian matrix of $\boldsymbol{f}$, we obtain $\mathbb{T}_\lambda(\mathrm{Jac}(\boldsymbol{f}))(\boldsymbol{\alpha}) = \mathrm{Jac}(\boldsymbol{f})(\boldsymbol{\varepsilon})$. Since by assumption $\boldsymbol{f}$ is symmetric, the previous lemma implies that

$$\mathrm{Jac}(\boldsymbol{f})(\boldsymbol{\varepsilon}) = \mathrm{Jac}_{z_1,\ldots,z_k}(\mathbb{T}_\lambda(\boldsymbol{f}))(\boldsymbol{\alpha}) \cdot Z.$$

Since $\mathrm{Jac}(\boldsymbol{f})(\boldsymbol{\varepsilon})$ has rank s (by condition A), the left kernel of $\mathrm{Jac}(\boldsymbol{f})(\boldsymbol{\varepsilon})$ is trivial.

It follows that the left kernel of $\mathrm{Jac}_{z_1,\ldots,z_k}(\mathbb{T}_\lambda(\boldsymbol{f}))(\boldsymbol{\alpha})$ is also trivial. □

When we represent $S_{t_1} \times \cdots \times S_{t_k}$-invariant functions in terms of Newton sums, we can show that the new representation also preserves condition (A).

Lemma 3.5. *Assume $(g_1, \ldots, g_s) \subset \mathbb{Q}[z_1, \ldots, z_k]$ is $S_{t_1} \times \cdots \times S_{t_k}$-invariant and satisfies condition* (A). *If we set $h_i = \gamma_{g_i}$ for all i, then $(h_1, \ldots, h_s)$ also satisfies condition* (A).

Proof. The Jacobian matrix $\mathrm{Jac}(\boldsymbol{g})$ of $(g_1, \ldots, g_s)$ factors as

$$\mathrm{Jac}(\boldsymbol{g}) = \mathrm{Jac}(\boldsymbol{h})(\boldsymbol{P}) \cdot \boldsymbol{V}, \text{ where } \boldsymbol{V} = \mathrm{diag}(V_1, \ldots, V_k)$$

with each V_i a row-scaled Vandermonde matrix given by

$$V_i = \begin{pmatrix} 1 & & & \\ & 2 & & \\ & & \ddots & \\ & & & t_i \end{pmatrix} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ z_{1,i} & z_{2,i} & \cdots & z_{t_i,i} \\ \vdots & & & \vdots \\ z_{1,i}^{t_i-1} & z_{2,i}^{t_i-1} & \cdots & z_{t_i,i}^{t_i-1} \end{pmatrix}. \quad (4)$$

Let $\boldsymbol{\eta}$ be a point in the vanishing set of $(h_1, \ldots, h_s)$ and let $\boldsymbol{\varepsilon}$ be in $\boldsymbol{P}^{-1}(\boldsymbol{\eta})$. If $\mathrm{Jac}(\boldsymbol{h})$ is rank deficient at $\boldsymbol{\eta}$ then $\mathrm{Jac}(\boldsymbol{h})(\boldsymbol{P})(\boldsymbol{\varepsilon})$ is also rank deficient. This implies that the rank of $\mathrm{Jac}(\boldsymbol{g})(\boldsymbol{\varepsilon})$, which is bounded above by those of $\mathrm{Jac}(\boldsymbol{h})(\boldsymbol{P})(\boldsymbol{\varepsilon})$ and $\boldsymbol{V}(\boldsymbol{\varepsilon})$, is deficient. □

Similarly, instead of using a row-scaled Vandermonde matrix V_i as in (4), we can use V_i as the Jacobian matrix of elementary symmetric functions in $\boldsymbol{z}_i$. This gives a similar result but for the polynomials $\zeta_{g_1}, \ldots, \zeta_{g_s}$.

Lemma 3.6. *Assume $(g_1, \ldots, g_s) \subset \mathbb{Q}[z_1, \ldots, z_k]$ is $S_{t_1} \times \cdots \times S_{t_k}$-invariant and satisfies condition* (A). *Then the sequence of polynomials $(\zeta_{g_1}, \ldots, \zeta_{g_s})$ also satisfies condition* (A).

4 CRITICAL LOCI

If $W \subset \mathbb{C}^\ell$ is an equidimensional algebraic set, and ϕ a polynomial function defined on W, a non-singular point $\boldsymbol{w} \in W$ is called a *critical point* of ϕ on W if the gradient of ϕ at $\boldsymbol{w}$ is normal to the tangent space $T_{\boldsymbol{w}}W$ of W at $\boldsymbol{w}$.

If $\boldsymbol{g} = (g_1, \ldots, g_s)$ are generators of the ideal associated to W, then $T_{\boldsymbol{w}}W$ is the right kernel of the Jacobian matrix $\mathrm{Jac}(\boldsymbol{g})$ of $\boldsymbol{g}$ evaluated at $\boldsymbol{w}$. In the cases we will consider, this matrix will have rank s at all points of W (that is, $\boldsymbol{g}$ satisfies condition A). The set of critical points of the restriction of ϕ to W is then defined by the vanishing of $\boldsymbol{g}$, and of the $(s+1)$-minors of the Jacobian matrix $\mathrm{Jac}(\boldsymbol{g}, \phi)$ of $\boldsymbol{g}$ and ϕ.

4.1 Finiteness through genericity

Let $\boldsymbol{g} = (g_1, \ldots, g_s)$ in $\mathbb{Q}[z_1, \ldots . z_k]$ with each g_i invariant under the action of $S_{t_1} \times \cdots \times S_{t_k}$; we write $\ell = t_1 + \cdots + t_k$. We introduce some useful $S_{t_1} \times \cdots \times S_{t_k}$-invariant mappings and discuss the properties of their critical points on $V(\boldsymbol{g}) \subset \mathbb{C}^\ell$.

For $1 \le i \le k$, let $\mathfrak{a}_i = (\mathfrak{a}_{1,i}, \ldots, \mathfrak{a}_{t_i,i})$ be new indeterminates, and recall that $P_{j,i}$ is the j-th Newton sum for the variables $\boldsymbol{z}_i$. Set

$$\phi_{\mathfrak{a}} = \sum_{i=1}^{k} c_i P_{t_i+1,i} + \sum_{i=1}^{k}\sum_{j=1}^{t_i} \mathfrak{a}_{j,i} P_{j,i} \quad (5)$$

where $c_i = 1$ if t_i is odd and $c_i = 0$ if t_i is even. So $\phi_{\mathfrak{a}}$ has even degree and is invariant under the action of $S_{t_1} \times \cdots \times S_{t_k}$. For $\boldsymbol{a} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k)$ in $\mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$, with each $\boldsymbol{a}_i$ in $\mathbb{C}^{t_i}$, we denote by $\phi_{\boldsymbol{a}}$ the polynomials in $\mathbb{C}[z_1, \ldots, z_k]$ obtained by evaluating the indeterminates $\mathfrak{a}_i$ at $\boldsymbol{a}_i$ in $\phi_{\mathfrak{a}}$, for all i.

Further, we denote by $\mathcal{U} \subset \mathbb{C}^\ell$ the open set consisting of points $\boldsymbol{w} = (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k)$ such that the coordinates of $\boldsymbol{w}_i$ are pairwise distinct for $i = 1, \ldots, k$. Note that $\mathcal{U}$ depends on the partition $\lambda = (n_1^{t_1} \ldots n_k^{t_k})$; when needed because of the use of different partitions, we will denote it by $\mathcal{U}_\lambda$.

Proposition 4.1. *Let $\boldsymbol{g} = (g_1, \ldots, g_s)$ be $S_{t_1} \times \cdots \times S_{t_k}$-invariant polynomials in $\mathbb{Q}[z_1, \ldots, z_k]$. Suppose further that $\boldsymbol{g}$ satisfies condition* (A)*. Then there exists a non-empty Zariski open set $\mathcal{A} \subset \mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$ such that for $\boldsymbol{a} \in \mathcal{A}$, the restriction of $\phi_{\boldsymbol{a}}$ to $V(\boldsymbol{g})$ has finitely many critical points in $\mathcal{U}$.*

4.2 Proof of Proposition 4.1

For new variables $L_1, \ldots, L_s$, we denote by $\mathcal{S}_{\mathfrak{a}}$ the polynomials

$$\mathcal{S}_{\mathfrak{a}} = \big(g_1, \ldots, g_s, \quad [L_1 \cdots L_s \ 1] \cdot \mathrm{Jac}(\boldsymbol{g}, \phi_{\mathfrak{a}})\big).$$

For $\boldsymbol{a} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k)$ in $\mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$, with each $\boldsymbol{a}_i$ in $\mathbb{C}^{t_i}$, we denote by $\mathcal{S}_{\boldsymbol{a}}$ the polynomials in $\mathbb{C}[L_1, \ldots, L_s, z_1, \ldots . z_k]$ obtained by evaluating $\mathfrak{a}_i$ at $\boldsymbol{a}_i$ in $\mathcal{S}_{\mathfrak{a}}$, for all i. Finally, denote by π the projection from the $(L, \boldsymbol{z})$-space $\mathbb{C}^{s+\ell}$ to the $\boldsymbol{z}$-space $\mathbb{C}^{\ell}$.

Lemma 4.2. *Suppose that $\boldsymbol{g}$ satisfies condition* (A)*. Then for $\boldsymbol{a} \in \mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$, $\pi(V(\mathcal{S}_{\boldsymbol{a}}))$ is the critical locus of the restriction of the map $\phi_{\boldsymbol{a}}$ to $V(\boldsymbol{g})$.*

Proof. For any $\boldsymbol{a} \in \mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$, we denote by $W(\phi_{\boldsymbol{a}}, \boldsymbol{g})$ the set of critical points of the restriction of $\phi_{\boldsymbol{a}}$ to $V(\boldsymbol{g})$. Since $\boldsymbol{g}$ satisfies condition (A), the set $W(\phi_{\boldsymbol{a}}, \boldsymbol{g})$ is given by

$$\{\boldsymbol{w} \mid g_1(\boldsymbol{w}) = \cdots = g_s(\boldsymbol{w}) = 0, \quad \mathrm{rank}(\mathrm{Jac}(\boldsymbol{g}, \phi_{\boldsymbol{a}})(\boldsymbol{w})) \leq s\}.$$

Consider $\boldsymbol{w}$ in $W(\phi_{\boldsymbol{a}}, \boldsymbol{g})$ and a nonzero vector $\boldsymbol{c}$ in the left kernel of $\mathrm{Jac}(\boldsymbol{g}, \phi_{\boldsymbol{a}})(\boldsymbol{w})$, of the form $\boldsymbol{c} = (c_1, \ldots, c_s, c_{s+1})$. The last coordinate c_{s+1} cannot vanish, as otherwise $(c_1, \ldots, c_s)$ would be a nonzero vector in the left kernel of $\mathrm{Jac}(\boldsymbol{g})(\boldsymbol{w})$ (which is ruled out by condition (A)). Dividing through by c_{s+1}, the point $(\boldsymbol{c}', \boldsymbol{w})$, with $c'_i = c_i / c_{s+1}$ for $i = 1, \ldots, s$, is a solution of $\mathcal{S}_{\boldsymbol{a}}$.

Conversely, take $(\boldsymbol{\ell}, \boldsymbol{w})$ in $V(\mathcal{S}_{\boldsymbol{a}})$. Thus, $\boldsymbol{w}$ cancels $\boldsymbol{g}$, and $\mathrm{Jac}(\boldsymbol{g}, \phi_{\boldsymbol{a}})$ has rank less than $s+1$ at $\boldsymbol{w}$, so that $\pi(V(\mathcal{S}_{\boldsymbol{a}}))$ is in $W(\phi_{\boldsymbol{a}}, \boldsymbol{g})$. □

Let $\phi_{\mathfrak{a}}$ and $\gamma_{\phi_{\mathfrak{a}}}$ be defined as in (5) and Lemma 2.2, respectively. For $i = 1, \ldots, k$, set $Q_i = \gamma_{P_{t_i+1,i}}$, and let $h_1, \ldots, h_s = \gamma_{g_1}, \ldots, \gamma_{g_s}$. In particular, Lemma 2.2 implies that $\gamma_{\phi_{\mathfrak{a}}}$ is given by

$$\sum_{i=1}^{k} c_i Q_i + \sum_{i=1}^{k} \sum_{j=1}^{t_i} \mathfrak{a}_{j,i} p_{j,i}.$$

The sequence $\mathcal{S}_{\mathfrak{a}}$ can be rewritten as

$$h_1 \circ \boldsymbol{P}, \ldots, h_s \circ \boldsymbol{P}, \quad [L_1 \ \ldots \ L_s \ 1] \begin{pmatrix} \frac{\partial h_1}{\partial p_{1,1}} & \cdots & \frac{\partial h_1}{\partial p_{t_k,k}} \\ \vdots & & \vdots \\ \frac{\partial h_s}{\partial p_{1,k}} & \cdots & \frac{\partial h_s}{\partial p_{t_k,k}} \\ c_1 \frac{\partial Q_1}{\partial p_{1,1}} + \mathfrak{a}_{1,1} & \cdots & c_k \frac{\partial Q_k}{\partial p_{t_k,k}} + \mathfrak{a}_{t_k,k} \end{pmatrix}_{\boldsymbol{P}(\boldsymbol{z})} \cdot \boldsymbol{V},$$

where $\boldsymbol{V}$ is a multi-row-scaled Vandermonde matrix which is the Jacobian matrix of $\boldsymbol{P}$ with respect to $\boldsymbol{z}$. This matrix has full rank at any point $\boldsymbol{w}$ in the open set $\mathcal{U}$ defined in Subsection 4.1.

In particular, for any $\boldsymbol{a} \in \mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$, the intersection of $V(\mathcal{S}_{\boldsymbol{a}})$ with $\mathbb{C}^s \times \mathcal{U}$ is contained in the preimage by the map $\mathrm{Id} \times \boldsymbol{P}$ of the vanishing set of the sequence

$$\boldsymbol{H_a}: \quad h_1, \ldots, h_s, \quad [L_1 \ \cdots \ L_s \ 1] \begin{pmatrix} \frac{\partial h_1}{\partial p_{1,1}} & \cdots & \frac{\partial h_1}{\partial p_{t_k,k}} \\ \vdots & & \vdots \\ \frac{\partial h_s}{\partial p_{1,1}} & \cdots & \frac{\partial h_s}{\partial p_{t_k,k}} \\ c_1 \frac{\partial Q_1}{\partial p_{1,1}} + a_{1,1} & \cdots & c_k \frac{\partial Q_k}{\partial p_{t_k,k}} + a_{t_k,k} \end{pmatrix}.$$

Since for all $1 \leq i \leq k$, $\boldsymbol{P}_i$ defines a map with finite fibers (by Newton identities and Vieta's formula, the preimage by $\boldsymbol{P}$ of some point is the set of roots of some polynomial of degree t_i), we deduce that $\boldsymbol{P}$ and consequently $\mathrm{Id} \times \boldsymbol{P}$ define maps with finite fibers. Thus

Lemma 4.3. *If $V(\boldsymbol{H_a})$ is finite, then $V(\mathcal{S}_{\boldsymbol{a}}) \cap (\mathbb{C}^s \times \mathcal{U})$ is finite.*

It remains to investigate finiteness properties of $V(\boldsymbol{H_a})$.

Proposition 4.4. *Suppose that $\boldsymbol{h}$ satisfies condition* (A)*. Then, there exists a non-empty Zariski open set $\mathcal{A} \subset \mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$ such that for any $\boldsymbol{a} \in \mathcal{A}$, $\langle \boldsymbol{H_a} \rangle \subset \mathbb{C}[L_1, \ldots, L_s, z_1, \ldots, z_k]$ is a radical ideal whose zero-set is finite.*

Proof. Let $W \subset \mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$ be the vanishing set of $(h_1, \ldots, h_s)$. Consider now the map

$$(\boldsymbol{\eta}, \boldsymbol{w}) \in \mathbb{C}^s \times W \to -\left(\sum_{i=1}^{s} \boldsymbol{\eta}_i \frac{\partial h_i}{\partial p_{1,1}} + c_1 \frac{\partial Q_1}{\partial p_{1,1}}\right)_{(\boldsymbol{w})}, \ldots, -\left(\sum_{i=1}^{s} \boldsymbol{\eta}_i \frac{\partial h_i}{\partial p_{t_k,k}} + c_k \frac{\partial Q_k}{\partial p_{t_k,k}}\right)_{(\boldsymbol{w})}.$$

By Sard's theorem [50, Chap. 2, Sec. 6.2, Thm 2], the set of critical values of this map is contained in a proper Zariski closed set $\mathcal{B}$ of $\mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_k}$. Since $\boldsymbol{h}$ satisfies condition (A), for $\boldsymbol{a}$ outside $\mathcal{B}$, the Jacobian matrix of $\boldsymbol{H_a}$ has full rank at any $(\boldsymbol{\eta}, \boldsymbol{w})$ with $\boldsymbol{w}$ in W. Hence, by the Jacobian criterion [23, Thm 16.19], the ideal generated by $\boldsymbol{H_a}$ in $\mathbb{C}[L_1, \ldots, L_s, z_1, \ldots, z_k]$ is radical and is of dimension at most zero. □

Proof of Prop 4.1. Let $\mathcal{A}$ be the non-empty Zariski open set defined in Prop 4.4. Since $\boldsymbol{g}$ satisfies condition (A), Lemma 4.2 implies that, for any $\boldsymbol{a} \in \mathcal{A}$, the critical locus of the map $\phi_{\boldsymbol{a}}$ restricted to $V(\boldsymbol{g})$ is equal to $\pi(V(\mathcal{S}_{\boldsymbol{a}}))$. In addition, the sequence $(\boldsymbol{h})$ also satisfies condition (A) by Lemma 3.5. Then, by Prop. 4.4, for any $\boldsymbol{a} \in \mathcal{A}$, the algebraic set defined by $\boldsymbol{H_a}$ is finite.

By Lemma 4.3, this implies that $V(\mathcal{S}_{\boldsymbol{a}})$ contains finitely many points in $\mathbb{C}^s \times \mathcal{U}$. This finishes our proof of Prop. 4.1. □

Using techniques from [24], one could give a simple exponential upper bound the degree of a hypersurface containing the complement of $\mathcal{A}$.

4.3 Finding extrema using proper maps

A real valued function $\psi : \mathbb{R}^n \to \mathbb{R}$ is *proper* at $x \in \mathbb{R}$ if there exists an $\varepsilon > 0$ such that $\psi^{-1}([x - \varepsilon, x + \varepsilon])$ is compact. Such functions are of interest because a proper polynomial restricted to a real algebraic set W reaches extrema on each connected component of W. Using [49, Thm 2.1 and Cor 2.2] one can construct proper polynomials in the following way.

Let $F = F_k(x_1, \ldots, x_n) + F_{k-1}(x_1, \ldots, x_n) + \cdots + F_0(x_1, \ldots, x_n) : \mathbb{R}^n \to \mathbb{R}$ be a real polynomial, where F_i is the homogeneous component of degree i of F. Assume further that the leading form F_k of F is positive definite; then, F is proper. In particular, the map $P_{2m} + \sum_{i=0}^{2m-1} \lambda_i P_i$, with P_i the Newton sums in $x_1, \ldots, x_n$ and all λ_i in $\mathbb{Q}$, is proper. We can extend this to blocks of variables.

Lemma 4.5. *Let $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k$ be blocks of $t_1, \ldots, t_k$ variables, respectively. If $P_{j,i} := z_{1,i}^j + \cdots + z_{t_i,i}^j$, then for any $m_1, \ldots, m_k \geq 1$ and coefficients $\lambda_{i,j}$ in $\mathbb{Q}$, the map*

$$\sum_{i=1}^{k} P_{2m_i,i} + \sum_{i=1}^{k} \sum_{j=0}^{2m_i-1} \lambda_{j,i} P_{j,i}$$

is proper.

5 MAIN RESULT

Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ be a sequence of symmetric polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ that satisfies condition (A). In this section we present an algorithm and its complexity to decide whether the real locus of $V(\boldsymbol{f})$ is empty or not.

To exploit the symmetry of $\boldsymbol{f}$ and to decide whether the set $V_{\mathbb{R}}(\boldsymbol{f})$ is empty or not, our main idea is slicing the variety $V(\boldsymbol{f})$ with hyperplanes which are encoded by a partition λ of n. This way, we obtain a new polynomial system which is invariant under the action $S_\lambda := S_{t_1} \times \cdots \times S_{t_k}$ of symmetric groups. We proved in Lemma 3.4 that this new system also satisfies condition (A). We then use the critical point method to decide whether the real locus of the algebraic variety defined by this new system is empty or not by taking a S_λ-invariant map as defined in the previous section.

5.1 Critical points along S_n-orbits

Let $\boldsymbol{g} = (g_1, \ldots, g_s)$ be a sequence of S_λ-invariant polynomials and ϕ be a S_λ-invariant map in $\mathbb{Q}[\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k]$, with $\boldsymbol{z}_i = (z_{1,i}, \ldots, z_{t_i,i})$ for all i. As before, we set $\ell = t_1 + \cdots + t_k$, and we assume that $s \leq \ell$. Assume further that the sequence $\boldsymbol{g}$ satisfies condition (A). Let ϕ be a S_λ-invariant map in $\mathbb{Q}[\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k]$.

Let ζ_ϕ and $\zeta_{\boldsymbol{g}}$ in $\mathbb{Q}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k]$, where $\boldsymbol{e}_i = (e_{1,i}, \ldots, e_{t_i,i})$ is a set of t_i new variables, be such that

$$\phi = \zeta_\phi(\boldsymbol{E}_1, \ldots, \boldsymbol{E}_k) \quad \text{and} \quad \boldsymbol{g} = \zeta_{\boldsymbol{g}}(\boldsymbol{E}_1, \ldots, \boldsymbol{E}_k).$$

Here $\boldsymbol{E}_i = (E_{1,i}, \ldots, E_{t_i,i})$ denotes the vector of elementary symmetric polynomials in variables $\boldsymbol{z}_i$, with each $E_{j,i}$ having degree j for all j, i.

Lemma 5.1. *Let $\boldsymbol{g}, \phi$, and λ as above. Assume further that ζ_ϕ has finitely many critical points on $V(\zeta_{\boldsymbol{g}})$. Then there exists a randomized algorithm* Critical_points $(\boldsymbol{g}, \phi, \lambda)$ *which returns a zero-dimensional parametrization of the critical points of ζ_ϕ restricted to $V(\zeta_{\boldsymbol{g}})$. The algorithm uses*

$$O^{\sim}\left(\delta^2 c_\lambda (e_\lambda + c_\lambda^5) n^4 \Gamma\right)$$

operations in $\mathbb{Q}$, where

$$c_\lambda = \frac{\deg(g_1) \cdots \deg(g_s) \cdot E_{\ell-s}(\delta - 1, \ldots, \delta - \ell)}{t_1! \cdots t_k!},$$

$$\Gamma = n^2 \binom{n+\delta}{\delta} + n^4 \binom{n}{s+1}, \text{ and}$$

$$e_\lambda = \frac{n(\deg(g_1)+1) \cdots (\deg(g_s)+1) \cdot E_{\ell-s}(\delta, \ldots, \delta - \ell + 1)}{t_1! \cdots t_k!},$$

with $\delta = \max(\deg(\boldsymbol{g}), \deg(\phi))$. The number of solutions is at most c_λ.

Proof. The Critical_points procedure contains two steps: first finding $\zeta_{\boldsymbol{g}}$ and ζ_ϕ from $\boldsymbol{g}$ and ϕ and then computing a representation for the set $W(\zeta_\phi, \zeta_{\boldsymbol{g}})$ of critical points of ζ_ϕ on $V(\zeta_{\boldsymbol{g}})$. The first step can be done using the algorithm Symmetric_Coordinates from [26, Lemma 9], which uses $O^{\sim}\left(\binom{\ell+\delta}{\delta}^2\right)$ operations in $\mathbb{Q}$.

Since the sequence $\boldsymbol{g}$ satisfies condition (A), Lemma 3.6 implies that $\zeta_{\boldsymbol{g}}$ also satisfies condition (A). Then, the set $W(\zeta_\phi, \zeta_{\boldsymbol{g}})$ is the zero set of $\zeta_{\boldsymbol{g}}$ and all the $(s+1)$-minors of $\mathrm{Jac}(\zeta_{\boldsymbol{g}}, \zeta_\phi)$. In particular, when $\ell = s$, $W(\zeta_\phi, \zeta_{\boldsymbol{g}}) = V(\zeta_{\boldsymbol{g}})$.

Since each $E_{j,i}$ has degree j, it is natural to assign a weight j to the variable $e_{j,i}$, so that the polynomial ring $\mathbb{Q}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k]$ is weighted of weights $(1, \ldots, t_1, \ldots, 1, \ldots, t_k)$. The weighted degrees of $\zeta_{\boldsymbol{g}}$ and ζ_ϕ are then equal to those of $\boldsymbol{g}$ and ϕ, respectively. To compute a zero-dimensional parametrization for $W(\zeta_\phi, \zeta_{\boldsymbol{g}})$ we use the symbolic homotopy method for weighted domain given in [37, Thm 5.3] (see also [26, Sec 5.2] for a detailed complexity analysis). This procedure is randomized and requires

$$O^{\sim}\left(\delta^2 c_\lambda (e_\lambda + c_\lambda^5) n^4 \Gamma\right) \text{ operations in } \mathbb{Q}.$$

Furthermore, results from [37, Thm 5.3] also imply that the number of points in the output is at most c_λ.

Thus, the total complexity of the Critical_points algorithm is then $O^{\sim}\left(\delta^2 c_\lambda (e_\lambda + c_\lambda^5) n^4 \Gamma\right)$ operations in $\mathbb{Q}$. □

5.2 The Decide procedure

Consider a partition $\lambda = (n_1^{t_1} \ \ldots \ n_k^{t_k})$ of n, and let

$$\mathscr{R}_\lambda = (v, v_{1,1}, \ldots, v_{t_1,1}, \ldots, v_{1,k}, \ldots, v_{t_k,k}, \mu)$$

be a parametrization which encodes a finite set $W_\lambda \subset \mathbb{C}^\ell$. This set lies in the target space of the algebraic map $F_\lambda : U_\lambda \to \mathbb{C}^\ell$ defined in Subsection 2.2 as

$$\boldsymbol{u} = (\underbrace{u_{1,1}, \ldots, u_{1,1}}_{n_1}, \ \ldots, \ \underbrace{u_{t_k,k}, \ldots, u_{t_k,k}}_{n_k})$$
$$\mapsto (E_{1,i}(u_{1,i}, \ldots, u_{t_i,i}), \ldots, E_{t_i,i}(u_{1,i}, \ldots, u_{t_i,i}))_{1 \leq i \leq k}, \quad (6)$$

where $E_{j,i}(u_{1,i}, \ldots, u_{t_i,i})$ is the j-th elementary symmetric function in $u_{1,i}, \ldots, u_{t_i,i}$ for $i = 1, \ldots, k$ and $j = 1, \ldots, t_i$.

Let V_λ be the preimage of W_λ by F_λ. In this subsection we present a procedure called Decide$(\mathscr{R}_\lambda)$ which takes as input $\mathscr{R}_\lambda$, and decides whether the set V_λ contains real points.

In order to do this, a straightforward strategy consists in solving the polynomial system to invert the map F_λ. Because of the group action of $S_{t_1} \times \cdots \times S_{t_k}$, we would then obtain $t_1! \cdots t_k!$ points in the preimage of a single point in W_λ: we would lose the benefit of all that had been done before.

This difficulty can be bypassed by encoding one single point per orbit in the preimage of the points in W_λ. This can be done via the following steps.

(i) Group together the variables $\boldsymbol{e}_i = (e_{1,i}, \ldots, e_{t_i,i})$ which encode the values taken by the elementary symmetric functions $E_{i,1}, \ldots, E_{i,t_i}$ (see Sec. 2.2) and denote by $v_{i,1}, \ldots, v_{i,t_i}$ the parametrizations corresponding to $e_{1,i}, \ldots, e_{t_i,i}$;

(ii) Make a reduction to a bivariate polynomial system by considering the polynomial with coefficients in $\mathbb{Q}[t]$

$$\rho_i = v' u^{t_i} - v_{1,i} u^{t_i - 1} + \cdots + (-1)^{t_i} v_{t_i,i} \in \mathbb{Q}[t][u]$$

and "solving" the system $\rho_i = v = 0$. Here we recall that $v \in \mathbb{Q}[t]$ and is square-free, so that v and v' are coprime.

(iii) It remains to decide whether, for all $1 \le i \le k$, there is a real root ϑ of v such that when replacing t by ϑ in ρ_i, the resulting polynomial has all its roots real. To do this we proceed by performing the following steps for $1 \le i \le k$:
   (1) first we compute the Sturm-Habicht sequence associated to $\left(\rho_i, \frac{\partial \rho_i}{\partial u}\right)$ in $\mathbb{Q}[t]$ (the Sturm-Habicht sequence is a signed subresultant sequence, see [9, Chap. 9, Algo. 8.21]);
   (2) next, we compute Thom-encodings of the real roots of v, which is a way to uniquely determine the roots of a univariate polynomial with real coefficients by means of the signs of its derivatives at the considered real root (see e.g. [9, Chap. 10, Algo. 10.14]);
   (3) finally, for each real root ϑ of v, evaluate the signed subresultant sequence at ϑ [9, Chap. 10, Algo. 10.15] and compute the associated Cauchy index to deduce the number of real roots of ρ_i (see [9, Cor. 9.5]).

(iv) For a given real root ϑ of v, it holds that, for all $1 \le i \le k$, the number of real roots of ρ_i equals its degree, if and only if V_λ is non-empty.

The above steps describe our Decide, which returns false if V_λ contains real points, else true.

5.3 The main algorithm

Our main algorithm Real_emptiness takes symmetric polynomials $\boldsymbol{f} = (f_1, \ldots, f_s)$ in $\mathbb{Q}[x_1, \ldots, x_n]$, with $s < n$, which satisfy condition (A), and decides whether $V_{\mathbb{R}}(f)$ is empty.

For a partition λ, we first find the polynomials $\boldsymbol{f}_\lambda := \mathbb{T}_\lambda(\boldsymbol{f})$, which are S_λ-invariant in $\mathbb{Q}[\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k]$, where $\mathbb{T}_\lambda$ is defined as in (2). By Corollary 3.4, $\boldsymbol{f}_\lambda$ satisfies condition (A), so we can apply the results of Section 4.

Let $\phi_{\mathfrak{a}}$ be the map defined in (5) and $\mathcal{A}_\lambda \subset \mathbb{C}^{t_1} \times \cdots \times \mathbb{C}^{t_1}$ be the non-zero Zariski open set defined in Proposition 4.1. Assume $\boldsymbol{a}$ is chosen in $\mathcal{A}_\lambda$ (this is one of the probabilistic aspects of our algorithm) at step 1b. By Corollary 3.4, $\boldsymbol{f}_\lambda$ satisfies condition (A). Then, the critical locus of the restriction of $\phi_{\boldsymbol{a}}$ to $V(\boldsymbol{f}_\lambda)$ is of dimension at most zero (by Proposition 4.1). In addition, the map $\phi_{\boldsymbol{a}}$ is invariant under the action of the group S_λ.

Let $\zeta_{\phi_{\boldsymbol{a}}}$ and $\zeta_{\boldsymbol{f}_\lambda}$ in $\mathbb{Q}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k]$ such that

$$\phi_{\boldsymbol{a}} = \zeta_{\phi_{\boldsymbol{a}}}(\boldsymbol{E}_1, \ldots, \boldsymbol{E}_k) \quad \text{and} \quad \boldsymbol{f}_\lambda = \zeta_{\boldsymbol{f}_\lambda}(\boldsymbol{E}_1, \ldots, \boldsymbol{E}_k).$$

Here $\boldsymbol{E}_i = (E_{1,i}, \ldots, E_{t_i,i})$ denotes the vector of elementary symmetric polynomials in variables $\boldsymbol{z}_i$. In the next step, we compute a zero-dimensional parametrization $\mathscr{R}_\lambda$ of the critical set $W_\lambda := W(\zeta_{\phi_{\boldsymbol{a}}}, \zeta_{\boldsymbol{f}_\lambda})$ of $\zeta_{\phi_{\boldsymbol{a}}}$ restricted to $V(\zeta_{\boldsymbol{f}_\lambda})$ by using the Critical_points algorithm from Lemma 5.1. The parametrization $\mathscr{R}_\lambda$ is given by a sequence of polynomials $(v, v_{1,1}, \ldots, v_{t_1,1}, \ldots, v_{1,k}, \ldots, v_{t_k,k})$ in $\mathbb{Q}[t]$ and a linear form μ.

At the final step, we run the Decide($\mathscr{R}_\lambda$) in order to determine whether the preimage of W_λ by the map F_λ contains real points.

Algorithm 1 Real_emptiness($\boldsymbol{f}$)

Input: symmetric polynomials $\boldsymbol{f} = (f_1, \ldots, f_s)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ with $s < n$ such that $\boldsymbol{f}$ satisfies (A)
Output: false if $V(\boldsymbol{f}) \cap \mathbb{R}^n$ is non-empty; true otherwise

(1) for all partitions $\lambda = (n_1^{t_1} \ \ldots \ n_k^{t_k})$ of n of length at least s, do
   (a) compute $\boldsymbol{f}_\lambda = \mathbb{T}_\lambda(\boldsymbol{f})$, where $\mathbb{T}_\lambda$ is defined in (2)
   (b) using a chosen $\boldsymbol{a} \in \mathcal{A}$, where $\mathcal{A}$ is defined as in Prop 4.1 , we construct $\phi_{\mathfrak{a}}$ as in (5) and then compute $\phi_{\boldsymbol{a}}$
   (c) compute $\mathscr{R}_\lambda$ = Critical_points($\phi_{\boldsymbol{a}}, \boldsymbol{f}_\lambda$)
   (d) run Decide($\mathscr{R}_\lambda$)
   (e) if Decide($\mathscr{R}_\lambda$) is false return false
(2) return true.

Proposition 5.2. *Assume that, on input symmetric $\boldsymbol{f}$ as above, and satisfying condition* (A)*, for all partitions λ of length at least s, $\boldsymbol{a}$ is chosen in $\mathcal{A}_\lambda$ and that all calls to the randomized algorithm* Critical_points *return the correct result. Then Algorithm* Real_emptiness *returns* true *if $V(\boldsymbol{f}) \cap \mathbb{R}^n$ is empty and otherwise it returns* false.

Proof. Since $\boldsymbol{f}$ satisfies condition (A), Lemma 3.4 implies that $\boldsymbol{f}_\lambda$ also satisfies this condition. Then, by the Jacobian criterion [23, Thm 16.19], $V(\boldsymbol{f}_\lambda)$ is smooth and equidimensional of dimension $(\ell - s)$, where ℓ is the length of λ. Therefore, if $\ell < s$, then the algebraic set $V(\boldsymbol{f}_\lambda)$ is empty. Thus, the union of $V(\boldsymbol{f}_\lambda) \cap \boldsymbol{\mathcal{U}}_\lambda$ where $\boldsymbol{\mathcal{U}}_\lambda$ is the open set defined in Subsection 4.1 and λ runs over the partitions of n of length at least s, forms a partition of $V(\boldsymbol{f})$. Hence, $V(\boldsymbol{f}) \cap \mathbb{R}^n$ is non-empty if and only if there exists at least one such partition for which $V(\boldsymbol{f}_\lambda) \cap \boldsymbol{\mathcal{U}}_\lambda \cap \mathbb{R}^n$ is non-empty.

We already observed that for all λ, $\boldsymbol{f}_\lambda$ does satisfy condition (A). Since we have assumed that each time Step 1b is performed, $\boldsymbol{a}$ is chosen in $\mathcal{A}_\lambda$, we apply Proposition 4.4 to deduce that the conditions of Lemma 5.1 are satisfied. Hence, all calls to Critical_points are valid.

Note that since we assume that all these calls return the correct result, we deduce that their output encodes points which all lie in $V(\boldsymbol{f})$. Hence, if $V(\boldsymbol{f}) \cap \mathbb{R}^n$ is empty, applying the routine Decide on these outputs will always return true and, all in all, our algorithm returns true when $V(\boldsymbol{f}) \cap \mathbb{R}^n$ is empty.

It remains to prove that it returns false when $V(\boldsymbol{f}) \cap \mathbb{R}^n$ is non-empty. Note that there is a partition λ such that $V(\boldsymbol{f}_\lambda) \cap \mathbb{R}^n$ is nonempty and has an empty intersection with the complement of $\boldsymbol{\mathcal{U}}_\lambda$. That is, all connected components of $V(\boldsymbol{f}_\lambda) \cap \mathbb{R}^n$ are in $\boldsymbol{\mathcal{U}}_\lambda$.

Let C be such a connected component. By Lemma 4.5, the map $\phi_{\boldsymbol{a}}$ is proper, and non-negative. Hence, its restriction to $V(\boldsymbol{f}_\lambda) \cap \mathbb{R}^n$ reaches its extremum at all connected components of $V(\boldsymbol{f}_\lambda) \cap \mathbb{R}^n$. This implies that the restriction of $\phi_{\boldsymbol{a}}$ to $V(\boldsymbol{f}_\lambda)$ has real critical points which are contained in C (and by Proposition 4.1 there are

finitely many). Those critical points are then encoded by the output of the call to Critical_points (Step 1c) and false is returned. □

5.4 Complexity analysis

Let $d = \max(\deg(\boldsymbol{f}))$. First for a partition λ, applying $\mathbb{T}_\lambda$ to $\boldsymbol{f}$ takes linear time in $O(n\binom{n+d}{d})$, the number of monomials of $\boldsymbol{f}$ and the cost of Step 1b is nothing. At the core of the algorithm, computing $\mathscr{R}_\lambda$ at Step 1c requires $O^\sim\left(\delta^2 c_\lambda (e_\lambda + c_\lambda^5) n^4 \Gamma\right)$ operations in $\mathbb{Q}$ by Lemma 5.1, where $\delta = \max(d, \deg(\phi_{\boldsymbol{a}}))$. Also, the degree of $\mathscr{R}_\lambda$ is at most c_λ.

In order to determine the cost of the Decide process at Step 1d, let a be the degree of v and b be the maximum of the partial degrees of ρ_i's w.r.t. u. By the complexity analysis of [9, Algo. 8.21 ; Sec. 8.3.6], Step (1) above is performed within $O\left(b^4 a\right)$ arithmetic operations in $\mathbb{Q}[t]$ using a classical evaluation interpolation scheme (there are b polynomials to interpolate, all of them being of degree $\leq 2ab$). Step (2) above requires $O\left(a^4 \log(a)\right)$ arithmetic operations in $\mathbb{Q}$ (see the complexity analysis of [9, Algo 10.14; Sec. 10.4]). Finally, in Step (3), we evaluate the signs of b polynomials of degree $\leq 2ab$ at the real roots of v (of degree a) whose Thom encodings were just computed. This is performed using $O\left(ba^3\left((\log(a)+b)\right)\right)$ arithmetic operations in $\mathbb{Q}$ following the complexity analysis of [9, Algo 10.15; Sec. 10.4]. The sum of these estimates lies in $O\left(b^4 a + ba^4\left((\log(a)+b)\right)\right)$.

Now, recall that the degree of v is the degree of $\mathscr{R}_\lambda$, so $a \leq c_\lambda$. The degree of ρ_i w.r.t. u equals t_i and $t_i \leq n$. This means $b \leq n$. All in all, we deduce that the total cost of this final step lies in $O\left(n^4 c_\lambda + n^2 c_\lambda\right)$, which is negligible compared to the previous costs.

In the worst case, one need to consider all the partitions of n of length at least s. Thus the total complexity of Real_emptiness is

$$\sum_{\lambda, \ell \geq s} O^\sim\left(\delta^2 c_\lambda (e_\lambda + c_\lambda^5) n^4 \Gamma\right)$$

operations in $\mathbb{Q}$. In addition, Lemma 34 in [26] implies that

$$\sum_{\lambda, \ell \geq s} c_\lambda \leq c \text{ and } \sum_{\lambda, \ell \geq s} e_\lambda \leq e,$$

where $c = \deg(\zeta_{f_\lambda})^s \binom{n+\delta-1}{n}$ and $e = n(\deg(\zeta_{f_\lambda})+1)^s \binom{n+\delta}{n}$. Notice further that $\binom{n+\delta}{\delta} \leq (n+1)\binom{n+\delta-1}{d}$ and $e = n(d+1)^s\binom{n+\delta}{n} \leq n(n+1)c^5$ for $\delta \geq 2$. In addition, since $\deg(\phi_{\boldsymbol{a}}) \leq \max(t_i)+1 \leq n$, the total cost of our algorithm is

$$O^\sim\left(d^2 n^6 c^6 \Gamma\right) = O^\sim\left(d^{6s+2} n^{11} \binom{n+d}{n}^6 \left(\binom{n+d}{n} + \binom{n}{s+1}\right)\right)$$

operations in $\mathbb{Q}$.

5.5 An example

Let $n = 4$ and $s = 1$ with $\boldsymbol{f} = (f)$ where

$$f = x_1^2 + x_2^2 + x_3^2 + x_4^2 - 6x_1x_2x_3x_4 - 1.$$

Consider first the partition $\lambda = (4^1)$. Then $f_\lambda := \mathbb{T}_\lambda(f) = -6z_{1,1}^4 + 4z_{1,1}^2 - 1$ which has no real solution as $f_\lambda = -2z_{1,1}^4 - (2z_{1,1}^2 - 1)^2 < 0$ for all $z_{1,1} \in \mathbb{R}$.

Next we consider $\lambda = (2^2)$. Then

$$f_{(2^2)} = 2z_{1,1}^2 + 2z_{2,1}^2 - 6z_{1,1}^2 z_{2,1}^2 - 1$$

and we take $\phi = 5(z_{1,1}^2 + z_{2,1}^2) - 9(z_{1,2} + z_{2,1}) - 3$. In this case $\zeta_{f_{(2^2)}} = 2e_{1,1}^2 - 6e_{2,1}^2 - 4e_{2,1} - 1$ and $\zeta_\phi = 5e_{1,1}^2 - 9e_{1,1} - 10e_{2,1} - 3$. The critical points of ζ_ϕ restricted to $V(\zeta_{f_{(2^2)}})$ are solutions to

$$\zeta_{f_{(2^2)}} = \det\left(\mathrm{Jac}(\zeta_{f_{(2^2)}}, \zeta_\phi)\right) = 0,$$

that is $2e_{1,1}^2 - 6e_{2,1}^2 - 4e_{2,1} - 1 = 120e_{1,1}e_{2,1} - 108e_{2,1} - 36 = 0$. A zero-dimensional parametrization of these critical points is given by $((v, v_{1,1}, v_{2,1}), \mu)$, where

$$\begin{aligned} v &= 200t^4 - 360t^3 + 62t^2 + 60t - 27, \\ v_{1,1} &= t, \text{ and} \\ v_{2,1} &= -\frac{1}{6}t^3 + \frac{9}{20}t^2 - \frac{31}{600}t - 1/20. \end{aligned}$$

At the final step, we check that the system

$$\rho_1 = v = 0, \quad \text{with} \quad \rho_1 = v'u^2 - v_{1,1}u + v_{2,1} \in \mathbb{Q}[t,u],$$

has real solutions. This implies that $V_\mathbb{R}(f)$ is non-empty.

The output of our algorithm is consistent with the fact that the point $(1, 1, 1/2, 1/2)$ is in $V_\mathbb{R}(f)$.

6 TOPICS FOR FUTURE RESEARCH

Determining topological properties of a real variety $V_\mathbb{R}(\boldsymbol{f})$ is an important algorithmic problem. Here we have presented an efficient algorithm to determine if $V_\mathbb{R}(\boldsymbol{f})$ is empty or not. More generally, we expect that the ideas presented here may lead to algorithmic improvements also in more refined questions, like computing one point per connected component or the Euler characteristic for a real symmetric variety. Furthermore, while our complexity gains are significant for symmetric input we conjecture that we can do better in certain cases. In particular, when the degree of the polynomials is at most n then we expect we that a combination with the topological properties of symmetric semi algebraic sets found in [12, Prop 9] can reduce the number of orbits considered, for example, instead of n^d we might only need $n^{d/2}$ for fixed d. Finally, a generalization to general symmetric semi algebraic sets should be possible.

REFERENCES

[1] B. Bank, M. Giusti, J. Heintz, G. Lecerf, G. Matera, and P. Solernó. Degeneracy loci and polynomial equation solving. *Foundations of Computational Mathematics*, 15(1):159–184, 2015.

[2] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

[3] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.

[4] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties and efficient real elimination procedure. *Kybernetika*, 40(5):519–550, 2004.

[5] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties: Geometry and algorithms. *Journal of complexity*, 2005.

[6] B. Bank, M. Giusti, J. Heintz, and L.M. Pardo. On the intrinsic complexity of point finding in real singular hypersurfaces. *Information Processing Letters*, 109(19):1141–1144, 2009.

[7] B. Bank, M. Giusti, J. Heintz, and M. Safey El Din. Intrinsic complexity estimates in polynomial optimization. *Journal of Complexity*, 30(4):430–443, 2014.

[8] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of ACM*, 43(6):1002–1045, 1996.

[9] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*. Algorithms and computation in Mathematics. Springer-Verlag, second edition edition, 2006. online version (2008).

[10] S. Basu and C. Riener. Bounding the equivariant Betti numbers of symmetric semi-algebraic sets. *Advances in Mathematics*, 305:803–855, 2017.

[11] S. Basu and C. Riener. Efficient algorithms for computing the euler-poincaré characteristic of symmetric semi-algebraic sets. In *Ordered Algebraic Structures and Related Topics: International Conference on Ordered Algebraic Structures and Related Topics, October 12–16, 2015, Centre International de Rencontres Mathématiques (CIRM), Luminy, France*, volume 697, pages 53–81. American Mathematical Soc. Providence, Rhode Island, 2017.

[12] S. Basu and C. Riener. Vandermonde varieties, mirrored spaces, and the cohomology of symmetric semi-algebraic sets. *Foundations of Computational Mathematics*, 22(5):1395–1462, 2022.

[13] J. Berthomieu and M. Eder, C.and Safey El Din. msolve: A Library for Solving Polynomial Systems. In *Proceedings of ISSAC 2021*, pages 51–58. ACM, 2021.

[14] C. W. Brown and J. H. Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*, pages 54–60, 2007.

[15] L. Busé and A. Karasoulou. Resultant of an equivariant polynomial system with respect to the symmetric group. *Journal of Symbolic Computation*, 76:142–157, 2016.

[16] J. Canny. *The complexity of robot motion planning*. MIT Press, 1987.

[17] C. Chen, J. H. Davenport, J. P. May, M. M. Maza, B. Xia, and R. Xiao. Triangular decomposition of semi-algebraic systems. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 187–194, 2010.

[18] C. Chen, M. M. Maza, B. Xia, and L. Yang. Computing cylindrical algebraic decomposition via triangular decomposition. In *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, pages 95–102, 2009.

[19] A. Colin. Solving a system of algebraic equations with symmetries. *Journal of Pure and Applied Algebra*, 117-118:195 – 215, 1997.

[20] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *Lecture notes in computer science*, 33:515–532, 1975.

[21] J. H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation*, 5(1-2):29–35, 1988.

[22] L. L. Dines. Systems of linear inequalities. *Annals of Mathematics*, pages 191–199, 1919.

[23] D. Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[24] J. Elliott, M. Giesbrecht, and É. Schost. On the bit complexity of finding points in connected components of a smooth real hypersurface. In *Proceedings of ISSAC 2020*, pages 170–177. ACM, 2020.

[25] M. England, R. Bradford, and J. H. Davenport. Cylindrical algebraic decomposition with equational constraints. *Journal of Symbolic Computation*, 100:38–71, 2020.

[26] J.-C. Faugère, G. Labahn, M. Safey El Din, É. Schost, and T. X. Vu. Computing critical points for invariant algebraic systems. *Journal of Symbolic Computation*, 116:365–399, 2023.

[27] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *Proceedings of ISSAC 2009*.

[28] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Critical points and Gröbner bases: The unmixed case. In *Proceedings of ISSAC 2012*, pages 162–169. ACM, 2012.

[29] J.-C. Faugère and J. Svartz. Solving polynomial systems globally invariant under an action of the symmetric group and application to the equilibria of N vortices in the plane. In *Proceedings of ISSAC 2012*, pages 170–178. ACM, 2012.

[30] J. B. J. Fourier. Solution d'une question particuliere du calcul des inégalités. *Nouveau Bulletin des Sciences par la Société philomatique de Paris*, 99:100, 1826.

[31] K. Gatermann and P. A. Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *Journal of Pure and Applied Algebra*, 192(1-3):95–128, 2004.

[32] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[33] D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.

[34] J. D. Hauenstein, M. Safey El Din, É. Schost, and T. X. Vu. Solving determinantal systems using homotopy techniques. *Journal of Symbolic Computation*, 104:754–804, 2021.

[35] J. Heintz, M.-F. Roy, and P. Solernò. On the theoretical and practical complexity of the existential theory of the reals. *The Computer Journal*, 36(5):427–431, 1993.

[36] H. Hong. Heuristic search strategies for cylindrical algebraic decomposition. In *Proceedings of Artificial Intelligence and Symbolic Mathematical Computing, Springer Lecture Notes in Computer Science 737*, pages 152–165, 1992.

[37] G. Labahn, M. Safey El Din, É. Schost, and T. X. Vu. Homotopy techniques for solving sparse column support determinantal polynomial systems. *Journal of Complexity*, 66:101557, 2021.

[38] S. McCallum. *An improved projection operator for Cylindrical Algebraic Decomposition*. PhD thesis, University of Wisconsin-Madison, 1984.

[39] S. McCallum. On projection in cad-based quantifier elimination with equational constraint. In *Proceedings of ISSAC 1999*, pages 145–149. ACM, 1999.

[40] N. Perminov and Sh. Shakirov. Discriminants of symmetric polynomials. *arXiv preprint arXiv:0910.5757*, 2009.

[41] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. *Journal of Symbolic Computation*, 13(3):255–352, 1992.

[42] C. Riener. On the degree and half-degree principle for symmetric polynomials. *Journal of Pure and Applied Algebra*, 216(4):850 – 856, 2012.

[43] C. Riener. Symmetric semi-algebraic sets and non-negativity of symmetric polynomials. *Journal of Pure and Applied Algebra*, 220(8):2809 – 2815, 2016.

[44] C. Riener and M. Safey el Din. Real root finding for equivariant semi-algebraic systems. In *Proceedings of ISSAC 2018*, page 335–342. ACM, 2018.

[45] C. Riener, T. Theobald, L. J. Andrén, and J. B. Lasserre. Exploiting symmetries in sdp-relaxations for polynomial optimization. *Mathematics of Operations Research*, 38(1):122–141, 2013.

[46] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *Proceedings of ISSAC 2003*, pages 224–231. ACM, 2003.

[47] M. Safey El Din and É. Schost. Bit complexity for multi-homogeneous polynomial system solving - Application to polynomial minimization. *Journal of Symbolic Computation*, 87:176–206, 2018.

[48] M. Safey El Din and P.-J. Spaenlehauer. Critical point computations on smooth varieties: Degree and complexity bounds. In *Proceedings of ISSAC 2016*, pages 183–190. ACM, 2016.

[49] T. Sakkalis. A note on proper polynomial maps. *Communications in Algebra*, 33(9):3359–3365, 2005.

[50] I. R. Shafarevich and M. Reid. *Basic algebraic geometry*, volume 2. Springer, 1994.

[51] P.-J. Spaenlehauer. On the complexity of computing critical points with gröbner bases. *SIAM Journal on Optimization*, 24(3):1382–1401, 2014.

[52] A. W. Strzeboński. Cylindrical algebraic decomposition using validated numerics. *Journal of Symbolic Computation*, 41(9):1021–1038, 2006.

[53] A. W. Strzeboński. Cylindrical algebraic decomposition using local projections. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, pages 389–396, 2014.

[54] B. Sturmfels. *Algorithms in Invariant Theory (Texts and Monographs in Symbolic Computation)*. Springer Publishing Company, Incorporated, 2nd ed.; vii, 197 pp.; 5 figs. edition, 2008.

[55] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. The Rand Corporation, Santa Monica, Calif., 1948.

[56] V. Timofte. On the positivity of symmetric polynomial functions.: Part I: General results. *Journal of Mathematical Analysis and Applications*, 284(1):174 – 190, 2003.

A EXPERIMENTAL RESULTS

We report on an implementation and set of experimental runs supporting the results in this paper. Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ be symmetric polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$. Assume further that f satisfies the regularity assumption (A). We compare our algrorithm with the following algorithms.

- The Distance algorithm that decides the emptiness of $V(\boldsymbol{f})$ in $\mathbb{R}^n$ by using the distance function from points on $V(\boldsymbol{f})$ to a generic point in $\mathbb{R}^n$. This procedure first generates
$$\text{dist} := (x_1 - c_1)^2 + \cdots + (x_n - c_n)^2$$
for a random point $(c_1, \ldots, c_n)$, then computes the critical points of dist restricted to $V(\boldsymbol{f})$. These critical points are zeros of $\boldsymbol{f}$ and all maximal minors of the Jacobian matrix of $\boldsymbol{f}$ and dist.
- The Safey El Din-Schost's algorithm [46] using canonical projections
$$\pi_i : \mathbb{C}^n \to \mathbb{C}^i$$
$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i),$$
for $i = 1, \ldots, (n - s)$. The algorithm first applies a randomly chosen change of variables $\mathbf{M}$, with coefficients in $\mathbb{Q}$, to the input system $\boldsymbol{f}$ to obtain a system $\boldsymbol{f}^{\mathbf{M}}$ and then chooses an arbitrary point $p_{n-s} = (c_1, \ldots, c_{n-s})$ in Q^{n-s}. At the final step, the algorithm computes zero-dimensional parametrizations of the sets $W_{n-i+1}(\boldsymbol{f}^{\mathbf{M}}) \cap \pi_{i-1}^{-1}(p_{i-1})$ for $i = 1, \ldots, n - s + 1$, where $W_{n-i+1}(\boldsymbol{f}^{\mathbf{M}})$ is the $n - i + 1$-th polar variety defined as the zero set of $\boldsymbol{f}$ and all maximal minors of $\text{Jac}(\boldsymbol{f}, \pi_i)$.

Our experiments are run using Maple computer algebra system and the msolve library [13], a library for solving multivariate polynomial systems. We run our experiments on $\boldsymbol{f} = (b(n))$ for $n \geq 2$, where $b(n)$ is the following polynomial

$$b(n) := \prod_{i=1}^{n}(x_i^2 + n - 1) - n^{n-2}\left(\sum_{i=1}^{n} x_i\right)^2 + n.$$

Here $s = 1$ and $d = 2n$. For $\boldsymbol{f} = (b(n))$, we can show that $\boldsymbol{f}$ satisfies condition (A) by proving that the system of $b(n)$ and all its patial derivatives has no solution in $\mathbb{C}^n$. We will obmit this proof since it is not our main purpose of this section.

We report in Table A the numbers N_{here}, N_{dist}, and N_{SS} of points in $\mathbb{C}^n$ that computed by using our algorithm, the Distance procedure, and Safey El Din-Schost's algorithm respectively. We also report on our timings, which are denoted by T_{here}, T_{dist}, and T_{SS}, in a detailed fashion for these three algorithms. The partition column gives a partition λ of n for which there is a real point of type λ in $V(b(n))$, where performed partitions are taken randomly among all partitions of n. In our experiments here, performing one partition is sufficient to give our final decision for each n. Experiments are stopped once the computation has gone past 20 minutes, with the corresponding time marked with a dash.

n	N_{here}	T_{here}	partition	N_{dist}	T_{dist}	N_{SS}	T_{SS}
2	4	0.002s	(1^2)	12	0.005s	8	0.003s
3	22	0.008s	$(1^1\,2^1)$	78	0.320s	48	0.119s
4	42	0.280s	$(1^2\,2^1)$	392	3.684s	192	5.892s
5	56	0.361s	$(1^1\,2^2)$	1690	277.813s	640	162.572s
6	192	2.126s	$(1^1\,2^1\,3^1)$	-	-	-	-
7	84	0.401s	$(2^2\,3^1)$	-	-	-	-

In fact, with this polynomial $b(n)$, if we consider the partition $\lambda = (n)$, then $h(n) := \mathbb{T}_\lambda(b(n)) = (x^2 + n - 1)^n - n^{n-1}n^2x^2 + n$. Since $h(n)(0) = (n-1)^n + n > 0$ and $h(n)(1) = n^n - n^{n+1} + n < 0$ for all $n \geq 2$, the Intermediate Value Theorem tells us that there is at least one real number $\alpha \in (0, 1)$ such that $h(n)(\alpha) = 0$. Thus $b(n) = 0$ has a real solution in $\mathbb{R}^n$ for all $n \in \mathbb{N}_{\geq 2}$; so the output of our algorithm is consistent with this conclusion.