



Sorbonne Université
Université de cotutelle

École Doctorale Informatique, Télécommunications et Électronique (Paris)

Homotopy algorithms for solving structured determinantal systems

Sous-titre de la thèse

par **Thi Xuan VU**

Thèse de doctorat de Informatique

Dirigée par Mohab Safey El Din, George Labahn, Éric Schost

Présentée et soutenue publiquement le 9 décembre 2020

devant le jury composé de:

M. Laurent Busé	INRIA Sophia Antipolis	Rapporteur
M. Stef Graillat	Sorbonne Université	Examinateur
M. George Labahn	University of Waterloo	Directeur de thèse
M. Cordian Riener	Arctic University of Norway	Rapporteur
M. Mohab Safey El Din	Sorbonne Université	Directeur de thèse
M. Éric Schost	University of Waterloo	Directeur de thèse
M. Pierre-Jean Spaenlehauer	INRIA Nancy	Examinateur
Mme. Lihong Zhi	University of Chinese Academy of Sciences	Examinateur

après avis des rapporteurs:

M. Laurent Busé	INRIA Sophia Antipolis
M. Cordian Riener	Arctic University of Norway

Abstract

Multivariate polynomial systems arising in numerous applications have special structures. In particular, determinantal structures and invariant systems appear in a wide range of applications such as in polynomial optimization and related questions in real algebraic geometry. The goal of this thesis is to provide efficient algorithms to solve such structured systems.

In order to solve the first kind of systems, we design efficient algorithms by using the symbolic homotopy continuation techniques. While the homotopy methods, in both numeric and symbolic, are well-understood and widely used in polynomial system solving for square systems, the use of these methods to solve over-detemined systems is not so clear. Meanwhile, determinantal systems are over-determined with more equations than unknowns. We provide probabilistic homotopy algorithms which take advantage of the determinantal structure to compute isolated points in the zero-sets of determinantal systems. The runtimes of our algorithms are polynomial in the sum of the multiplicities of isolated points and the degree of the homotopy curve. We also give the bounds on the number of isolated points that we have to compute in three contexts: all entries of the input are in classical polynomial rings, all these polynomials are sparse, and they are weighted polynomials.

In the second half of the thesis, we deal with the problem of finding critical points of a symmetric polynomial map on an invariant algebraic set. We exploit the invariance properties of the input to split the solution space according to the orbits of the symmetric group. This allows us to design an algorithm which gives a triangular description of the solution space and which runs in time polynomial in the number of points that we have to compute. Our results are illustrated by applications in studying real algebraic sets defined by invariant polynomial systems by the means of the critical point method.

Résumé

Les systèmes polynomiaux multivariés apparaissant dans de nombreuses applications ont des structures spéciales et les systèmes invariants apparaissent dans un large éventail d'applications telles que dans l'optimisation polynomiale et des questions connexes en géométrie algébrique réelle. Le but de cette thèse est de fournir des algorithmes efficaces pour résoudre de tels systèmes structurés.

Afin de résoudre le premier type de systèmes, nous concevons des algorithmes efficaces en utilisant les techniques d'homotopie symbolique. Alors que les méthodes d'homotopie, à la fois numériques et symboliques, sont bien comprises et largement utilisées dans la résolution de systèmes polynomiaux pour les systèmes carrés, l'utilisation de ces méthodes pour résoudre des systèmes surdéterminés n'est pas si claire. Hors, les systèmes déterminants sont surdéterminés avec plus d'équations que d'inconnues. Nous fournissons des algorithmes d'homotopie probabilistes qui tirent parti de la structure déterminantielle pour calculer des points isolés dans les ensembles des zéros de tels systèmes. Les temps d'exécution de nos algorithmes sont polynomiaux dans la somme des multiplicités des points isolés et du degré de la courbe d'homotopie. Nous donnons également des bornes sur le nombre de points isolés que nous devons calculer dans trois contextes: toutes les termes de l'entrée sont dans des anneaux polynomiaux classiques, tous ces polynômes sont creux, et ce sont des polynômes à degrés pondérés.

Dans la seconde moitié de la thèse, nous abordons le problème de la recherche de points critiques d'une application polynomiale symétrique sur un ensemble algébrique invariant. Nous exploitons les propriétés d'invariance de l'entrée pour diviser l'espace de solution en fonction des orbites du groupe symétrique. Cela nous permet de concevoir un algorithme qui donne une description triangulaire de l'espace des solutions et qui s'exécute en temps polynomial dans le nombre de points que nous devons calculer. Nos résultats sont illustrés par des applications à l'étude d'ensembles algébriques réels définis par des systèmes polynomiaux invariants au moyen de la méthode des points critiques.

Acknowledgements

First I would like to thank my advisors, George Labahn, Mohab Safey El Din, and Éric Schost, for all their supervision of my research and their support and encouragement during the three years of the PhD. Their doors were always open for me whenever needed. I would also like to thank Jean-Charles Faugére who was one of my original supervisors at Sorbonne Université.

I would like to thank Laurent Busé and Cordian Riener for their roles as external examiners and rapporteurs of this thesis and for spending their time to read and review this manuscript. In addition, I would like to give thanks to Stef Graillat, Pierre-Jean Spaenlehauer, Arne Storjohann, Stephen Vavasis, and Lihong Zhi for accepting to be part of the jury of my thesis.

A special thanks should go to Claude-Pierre Jeannerod and Vincent Neiger, my advisors in Lyon where I did my master degree, and who brought me to the area of symbolic computation. I thank them for always believing in me, for their support and encouragement.

To all of my teachers in Vietnam, Lyon, Paris, and Waterloo I give my thanks. Without them, I could not be at this stage of my study.

I thank all the members of both the PolSys team at Sorbonne Université and of the Symbolic Computation Group at the University of Waterloo for their companionship and enjoyable coffee time with good coffee. Special thanks to Jérémy for his unconditional help and my office-mates for our shared time together.

I give special thanks to all of my friends in Vietnam, Lyon, Paris, and Waterloo for our friendships, especially to French friends who have tried to teach and encourage me to speak french even though they already knew the final result.

Finally I thank my parents, my brother Thuyết and my sister-in-law Hậu for their unconditional love. I thank them for always standing by my side through all of the ups and downs of life. I thank my mother for teaching me how to compare $2 + 2 + 2$ and 5 when I was at age 3, for how she raised me, and for all the lessons she has taught me. I thank my father for teaching me that being a good and happy person is more important than anything else, and my brother for everything he did for me.

To my grandmother who is celebrating her ninetieth birthday.

To my parents for their unconditional love and support.

To my brother for our beautiful and unforgettable childhood.

Tặng bà ngoại, bố mẹ, và anh trai.

Table of Contents

List of Algorithms 11

List of Figures 12

List of Tables 13

Glossary 14

Abbreviations 15

Nomenclature 16

List of Symbols 17

1 Introduction 1

1.1 Motivation and problem statements . . . 2
1.2 Complexity model and data structure . . . 4
1.3 Methods for polynomial system solving . . . 4
1.4 Our Contributions . . . 8
1.5 Related work . . . 14
1.6 Organization of the thesis . . . 17

2 Résumé en Français 19

2.1 Motivations et problématiques . . . 19
2.2 Méthodes pour la résolution de systèmes polynomiaux . . . 21
2.3 Contributions . . . 23
2.4 Organisation de la thèse . . . 26

3 Preliminaries **28**

3.1 Commutative algebra and algebraic geometry . . . 28
3.1.1 Ideals . . . 28
3.1.2 Algebraic sets and Zariski topology . . . 30
3.1.3 Generic properties of varieties . . . 31
3.1.4 Irredudant decomposition . . . 31
3.1.5 Regular, singular, and critical points . . . 33
3.1.6 Primary decomposition of ideals . . . 35
3.1.7 Localization . . . 35
3.1.8 Cohen-Macaulay rings . . . 37
3.2 Determinantal varieties . . . 37
3.2.1 Determinantal ideals . . . 37
3.2.2 Left-hand diagonal block matrices . . . 38
3.3 Sparse polynomial systems . . . 39
3.3.1 Initial forms . . . 40
3.3.2 The BKK Theorem . . . 41
3.4 Weighted polynomial domains . . . 42
3.4.1 Weighted Bézout Theorem . . . 43
3.4.2 Combinatorics of monomials . . . 43
3.5 The ring of symmetric polynomials . . . 44
3.6 Computational model and complexity estimates . . . 45
3.6.1 Straight-line programs . . . 45
3.6.2 The probabilistic aspects . . . 46
3.6.3 Basic complexity estimates . . . 47
3.7 Symbolic homotopy continuation methods . . . 47
3.7.1 The homotopy curve $\mathcal{W}$ . . . 48
3.7.2 Newton-Hensel Lifting . . . 50
3.7.3 Recover a zero-dimensional parametrization $\mathscr{R}$ of $\mathcal{W}$ . . . 53
3.7.4 Rational reconstruction . . . 53
3.7.5 Specializing at $t = 1$ . . . 54
3.7.6 Cleaning non-isolated points . . . 55
3.7.7 Degree bounds and start systems . . . 56

I Determinantal systems **58**

4 An overview **59**

4.1 Problem statements . . . 59

4.2 Main results . . . 60

4.3 Roadmap of algorithms . . . 65

5 Determinantal homotopy algorithm **68**

5.1 A local dimension test . . . 68

5.2 Symbolic homotopy algorithms . . . 74

5.2.1 Bounds on the number of isolated points . . . 74

5.2.2 Properties of the start system . . . 77

5.2.3 Homotopy algorithms . . . 80

5.3 Properties of determinantal ideals . . . 85

6 Determinantal ideals in classical polynomial rings **89**

6.1 A property of start systems . . . 89

6.2 The column-degree homotopy . . . 90

6.2.1 Setting up systems . . . 91

6.2.2 Degrees of the start and deformed systems . . . 93

6.2.3 Solutions of the homogenization of the start system . . . 93

6.2.4 Radical and zero-dimensional properties of $\langle \boldsymbol{A} \rangle$ . . . 94

6.2.5 Setting up parameters . . . 96

6.2.6 Completing the cost analysis . . . 97

6.3 The row-degree homotopy . . . 99

6.3.1 Preliminaries for the row-degree homotopy . . . 101

6.3.2 Setting up the systems . . . 112

6.3.3 A subroutine to solve the start systems . . . 115

6.3.4 Solving the start systems . . . 120

6.3.5 The row-degree homotopy algorithms . . . 122

7 Determinantal ideals in sparse domains and application in weighted polynomial rings **129**

7.1 The column-support homotopy . . . 129

7.1.1 Generic sparse polynomials . . . 130

7.1.2 Setting up the systems . . . 131

7.1.3 Radical and zero-dimensional properties of $\langle \boldsymbol{A} \rangle$ . . . 132

7.1.4 The associated Lagrange system . . . 133

7.1.5 The boundedness property . . . 137

7.1.6 Setting up parameters . . . 138

7.1.7 Completing the cost analysis . . . 141

7.2 The weighted column-degree homotopy . . . 141

7.2.1 Setting up the systems . . . 142

7.2.2 Setting up parameters . . . 143

7.2.3 Completing the weighted column-degree homotopy . . . 146

7.2.4 Example . . . 147

II Invariant algebraic systems **150**

8 An overview **151**

8.1 Problem statement and main results . . . 151

8.2 Organization of part II . . . 155

9 Invariant algebraic representations **156**

9.1 Partitions . . . 156

9.2 Symmetric representations . . . 158

9.3 Some useful algorithms . . . 162

9.3.1 $\mathcal{S}_\lambda$-invariant polynomials: the Symmetric_Coordinates algorithm . . . 162

9.3.2 $\mathcal{S}_\lambda$-equivariant polynomials: the Symmetrize algorithm . . . 165

10 Computing critical points for invariant algebraic systems **175**
10.1 Description of the algebraic set $W(\phi, \boldsymbol{G})$ 175
10.2 Algorithms for computing critical points 179
10.2.1 Some subroutines 179
10.2.2 The main algorithm 180
10.3 Cost of the main algorithm 181
10.3.1 The Prepare procedure 181
10.3.2 The complexity of the WeightedColumnDegree procedure 182
10.3.3 Finishing the proof of Theorem 8.1.1 185
10.4 Experimental results 188

11 Conclusions and Topics for Future Research **191**
11.1 Conclusions 191
11.2 Topics for future work 192

References **194**

List of Algorithms

1 Newton-HenselLifting($\boldsymbol{h}, \boldsymbol{\alpha}, \delta$) . . . 52
2 HomotopySquare($\boldsymbol{h}, \mathscr{R}_0, \delta$) . . . 55
3 Homotopy($\Gamma, \mathscr{R}_0, e$) . . . 84
4 Homotopy_simple($\Gamma, \mathscr{R}_0, e$) . . . 85
5 ColumnDegree(Γ) . . . 99
6 ColumnDegree_simple(Γ) . . . 100
7 RowDegreeDiagonal($(\lambda_{i,j,k})_{i,j,k}$) . . . 117
8 RowDegreeStart(Δ) . . . 121
9 RowDegree_simple(Γ) . . . 124
10 RowDegree(Γ) . . . 128
11 ColumnSupport($\boldsymbol{F}, \boldsymbol{G}$) . . . 142
12 WeightedColumnDegree($\boldsymbol{F}, \boldsymbol{G}$) . . . 147
13 Symmetric_Coordinates(λ, f) . . . 164
14 Symmetrize($\lambda, \boldsymbol{q}$) . . . 174
15 Critical_Points_Per_Orbit($\boldsymbol{G}, \phi$) . . . 180
16 Prepare_G($\boldsymbol{G}, \lambda$) . . . 181
17 Prepare_G_H($\boldsymbol{G}, \phi, \lambda$) . . . 182

List of Figures

1.1 Varieties of polynomial systems 2

3.1 Irreducible components of $V(x_1^2x_2 + x_2^3 + x_1^2 + x_2^2 - 4x_2 - 4)$ 32
3.2 Singularities 34
3.3 Minkowski sum of polytopes 41

8.1 Critical points of $x_1x_2x_3 - 3x_1 - 3x_2 - 3x_3$ over the sphere $x_1^2 + x_2^2 + x_3^2 - 6$ 152
8.2 The zero set of $(x_1^2 + 2x_2^2 - 6, x_2^2 + x_1x_2 - 3, x_2 - x_3)$ 153

List of Tables

10.1 Degrees and bounds 189
10.2 Algorithm timings 190

Chapter 1

Introduction

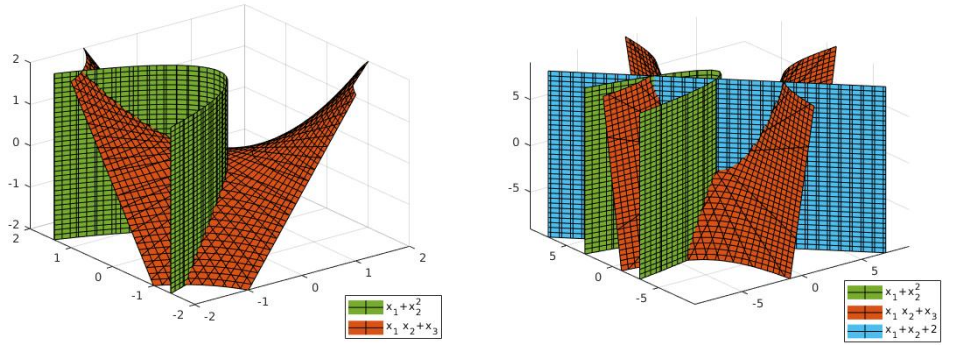
Solving systems of polynomial equations over a given field is a classical and fundamental problem in the fields of algebraic geometry and symbolic computation. Algebraic systems arise in a number of symbolic and scientific applications in computer algebra [20, 45, 46], robotics [147], geometric modeling [2], signal processing [89], chromatology [134] and structural molecular biology to name just a few.

A polynomial system is a set of equations $f_1 = \cdots = f_m = 0$ with the f_i multivariate polynomials in a ring $\mathbb{K}[x_1, \ldots, x_n]$ in n variables with coefficients in a field $\mathbb{K}$. In this thesis, $\mathbb{K}$ will always be a field of characteristic zero. A system is called zero dimensional if it has finitely many solutions, otherwise it is said to be of positive dimension. If we denote the algebraic closure of $\mathbb{K}$ by $\overline{\mathbb{K}}$, then solving a zero-dimensional system then consists of finding all solutions in the field $\overline{\mathbb{K}}$ or in the field of real numbers. When the system is positive dimensional, then solving consists of producing a description of the solutions set which allows one to get desired information easily. In general, polynomial system solving is difficult, and it is known as an NP-hard problem (see e.g. [71, 79]). The zero set in $\overline{\mathbb{K}}^n$ of a polynomial system $\boldsymbol{f} = (f_1, \ldots, f_m)$, denoted by $V(\boldsymbol{f})$, is called the variety or algebraic set defined by $\boldsymbol{f}$.

Example 1.0.1. Consider $n = 3$ and $\mathbb{K} = \mathbb{Q}$, the field of rational numbers. The set $\boldsymbol{f} = (x_1x_2 + x_3, x_1 + x_2^2)$ is a polynomial system in $\mathbb{Q}[x_1, x_2, x_3]$ with its associated algebraic set being a curve in $\mathbb{C}$ (Figure 1.1(a)), so that the system $\boldsymbol{f}$ in $\mathbb{Q}[x_1, x_2, x_3]$ has positive dimension.

However, if we add the equation $x_1 + x_2 + 2$ into the system $\boldsymbol{f}$, we obtain a zero-dimensional polynomial system $\boldsymbol{g} = (x_1x_2 + x_3, x_1 + x_2^2, x_1 + x_2 + 2)$ in $\mathbb{Q}[x_1, x_2, x_3]$ with the solution set of $\boldsymbol{g}$ in $\mathbb{C}^3$ being $\{(-1, -1, -1), (-4, 2, 8)\}$ (Figure 1.1(b)).

Several polynomial systems which come from practical applications have special structures. In this case one hopes to obtain algorithms for polynomial systems solving which can take advantage of the added structure for more efficient computation. In this thesis, we focus on a family of systems modelling rank defects in matrices with polynomial entries.



(a) $V(x_1x_2 + x_3, x_1 + x_2^2)$ (b) $V(x_1x_2 + x_3, x_1 + x_2^2, x_1 + x_2 + 2)$

Figure 1.1: Varieties of polynomial systems

1.1 Motivation and problem statements

Consider a sequence of polynomials $\boldsymbol{G}$ and a polynomial matrix $\boldsymbol{F}$, with entries coming from the ring $\mathbb{K}[x_1, \ldots, x_n]$. The problem of computing the points in $\overline{\mathbb{K}}^n$ at which all polynomials $\boldsymbol{G}$ vanish and $\boldsymbol{F}$ is not full-rank appears naturally in polynomial optimization [92, 111, 13, 90, 143], and related questions in real algebraic geometry [7, 10, 12, 14, 21, 22, 28, 35, 95, 156, 157, 158]. In these cases $\boldsymbol{F}$ consists of the Jacobian matrix of $\boldsymbol{G}$, together with one extra row, corresponding to the gradient of a function ϕ with the problem being to optimize ϕ on the zero set of $\boldsymbol{G}$. We denote this Jacobian matrix by $\mathrm{Jac}(\boldsymbol{G}, \phi)$.

A second interesting application is the problem of deciding whether an algebraic set defined over $\mathbb{Q}$, the field of rationals, is empty over a real field. This problem is tackled by the critical point method (see e.g. [91, 99, 148, 97, 19, 18, 11, 10] and references therein), and its principle is the following: choose a polynomial map reaching its extrema and having a zero-dimensional critical locus. This method has been used to answer several problems in real geometry, including for example quantifier elimination [103] and answering connectivity queries [161, 157] to name just a few.

Problem. *Given polynomials $\boldsymbol{G}$ and a polynomial matrix $\boldsymbol{F}$, all entries are in $\mathbb{K}[x_1, \ldots, x_n]$. Compute points $\boldsymbol{x}$ in $\overline{\mathbb{K}}^n$ such that $\boldsymbol{G}(\boldsymbol{x}) = 0$ and $\boldsymbol{F}(\boldsymbol{x})$ is not full rank.*

When there are no extra polynomials $\boldsymbol{G}$, then the above problem is a particular case of the more general MinRank problem, which arises naturally in numerous applications such as cryptography and coding theory. Consider a matrix $\boldsymbol{F}$, and a positive integer r. Then the MinRank problem is to find points in $\overline{\mathbb{K}}^n$ at which the matrix $\boldsymbol{F}$ has rank at most r. This problem plays an essential role in the cryptanalysis of several systems, including, for instance the TTM cryptosystem [88], the ABC cryptosystem [137, 138], and the HFE cryptosystem [118, 29, 173, 50].

For the systems coming from optimization, we also study the important case where the input polynomials $\boldsymbol{G}$ and ϕ are all invariant under the action of the symmetric group $\mathcal{S}_n$,

that is, when $\boldsymbol{G}$ and ϕ are *symmetric* in $(x_1, \ldots, x_n)$. In this case we wish to exploit the symmetric structure of $\boldsymbol{G}$ and ϕ to reduce the complexity of the solving problem.

Problem. *Given symmetric polynomials $\boldsymbol{G}$ and ϕ, compute points $\boldsymbol{x}$ in $\overline{\mathbb{K}}^n$ such that $\boldsymbol{G}(\boldsymbol{x}) = 0$ and $\mathrm{Jac}(\boldsymbol{G}, \phi)(\boldsymbol{x})$ is not full rank, taking advantage of symmetric structures.*

Symmetric polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ form a subring $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$ of $\mathbb{K}[x_1, \ldots, x_n]$. For each integer $k \geq 0$, let η_k be the k-th elementary symmetric function in $(x_1, \ldots, x_n)$. The fundamental theorem of symmetric polynomials [49, Theorem 3.10.1] implies that $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$ is isomorphic (as a $\mathbb{K}$-algebra) to the polynomial ring $\mathbb{K}[e_1, \ldots, e_n]$, where $(e_1, \ldots, e_n)$ are new variables. Note that, for $1 \leq k \leq n$, $\deg(\eta_k) = k$, so in the domain $\mathbb{K}[e_1, \ldots, e_n]$, the variables $(e_1, \ldots, e_n)$ can be viewed to have weighted degrees. This can be studied using the concept of weighted polynomial domains. These are multivariate polynomial rings $\mathbb{K}[x_1, \ldots, x_n]$ where each variable x_i has a weighted degree $w_i \geq 1$ (denoted by $\mathrm{wdeg}(x_i) = w_i$). When the weights are $(1, \ldots, 1)$, we have the classical polynomial ring.

Note that the weighted structure also exists when considering bounds for solutions of polynomial systems when comparing classical to weighted domains. With polynomial systems lying in a weighted polynomial domain, the weighted Bézout's theorem (see e.g. [108]) states that the number of isolated solutions to polynomial systems of equations is decreased by a factor of the product of the weights of the variables of the polynomial ring, when compared to the classical Bézout's theorem. Therefore, it is natural to study the following problem.

Problem. *Given polynomials $\boldsymbol{G}$ and a polynomial matrix $\boldsymbol{F}$, with entries in a weighted polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$. Compute points $\boldsymbol{x}$ in $\overline{\mathbb{K}}^n$ such that $\boldsymbol{G}(\boldsymbol{x}) = 0$ and $\boldsymbol{F}(\boldsymbol{x})$ is not full rank, taking advantage of the special structure of weighted domains.*

Notice further that polynomials in weighted domains have a natural sparse structure when compared to polynomials in classical domains; a polynomial is *sparse* if there are few monomials with nonzero coefficients. For example, a polynomial in $\mathbb{K}[x_1, x_2, x_3]$ having total degree bounded by 10 has 286 possible terms in a classical domain. However in a weighted domain with weights $w = (5, 3, 2)$ there are only 19 possible terms. Furthermore, when the system consists of sparse polynomials, instead of using the classical Bézout's theorem to bound the number of isolated points in the zero set, one should use the Bernstein-Khovanskii-Kushnirenko (BKK) theorem. The BKK theorem bounds the number of isolated solutions of a system of sparse polynomials by the mixed volume of the Newton polytopes of the equations. Thus, the final problem we study in the thesis is the following.

Problem. *Given polynomials $\boldsymbol{G}$ and a polynomial matrix $\boldsymbol{F}$, with entries being sparse polynomials. Compute points $\boldsymbol{x}$ in $\overline{\mathbb{K}}^n$ such that $\boldsymbol{G}(\boldsymbol{x}) = 0$ and $\boldsymbol{F}(\boldsymbol{x})$ is not full rank with a cost depending on the sparse structure of the input polynomials.*

1.2 Complexity model and data structure

In this thesis, we use the *straight-line program* encoding, that is, a sequence of elementary operations $+, -, \times$, to compute polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ (see Definition 3.6.1 for a detailed description). Note that the straight-line program coding for the input of our algorithms is not restrictive as we can see in Subsection 3.6.1 that this covers other encodings. The reason we use straight-line program as the encoding is because some algorithms that we use as subroutines use this encoding for their inputs.

We will represent the output of our algorithms using univariate polynomials. Let $V \subset \overline{\mathbb{K}}^n$ be a zero-dimensional variety defined by polynomials over $\mathbb{K}$. A *zero-dimensional parametrization* $\mathscr{R} = ((q, v_1, \ldots, v_n), \lambda)$ of V consists of

- a square-free polynomial q in $\mathbb{K}[y]$, where y is a new indeterminate, such that q is square-free and with $\deg(q) = |V|$,
- polynomials $(v_1, \ldots, v_n)$ in $\mathbb{K}[y]$ with each $\deg(v_i) < \deg(q)$ and satisfying

$$V = \left\{ \left(\frac{v_1(\tau)}{q'(\tau)}, \ldots, \frac{v_n(\tau)}{q'(\tau)} \right) \in \overline{\mathbb{K}}^n \mid q(\tau) = 0 \right\}, \text{ where } q' = \frac{\partial q}{\partial y},$$

- a linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ with coefficients in $\mathbb{K}$, such that $\lambda(v_1, \ldots, v_n) = yq' \mod q$ (so the roots of q are the values taken by λ on V).

When this holds, we write $V = Z(\mathscr{R})$. This representation was introduced in early work of Kronecker and Macaulay [119, 131] and has been widely used as a data structure in computer algebra, see for instance [83, 5, 85, 86, 154, 87]. One of the reasons why we use this representation is that using a rational parametrization, with q' as a denominator, allows one to control the bit-size of the coefficients when $\mathbb{K} = \mathbb{Q}$ or the degree in t when $\mathbb{K}$ is a field of fractions $k(t)$, where k is a field [5, 154, 87].

1.3 Methods for polynomial system solving

There are several procedures for finding the solution set of a polynomial system. Below we give a brief overview of some of these methods. In this thesis, we mainly focus on homotopy methods, which are given in more detail in Section 3.7.

Homotopy methods

The idea behind homotopy methods is to deform a system with known roots into a target system that we wish to solve. There are two kinds of homotopy algorithms: numeric and symbolic homotopy algorithms. In this thesis, we focus on the latter algorithms.

Symbolic and numeric homotopy methods rely on deformation techniques which are based on the perturbation of the target system and a subsequent symbolic or numeric path following methods (see e.g. [4, 25, 33, 96, 129, 126, 165, 139]). More precisely, let $V \subset \overline{\mathbb{K}}^n$ be a zero-dimensional variety and $W \subset \overline{\mathbb{K}}^{n+1}$ be an algebraic curve such that $\pi : W \to \overline{\mathbb{K}}$ onto the first coordinate is dominant (i.e. the Zariski closure of $\pi(W)$ is $\overline{\mathbb{K}}$) with generically finite fibers of degree c, $\pi^{-1}(1) = \{1\} \times V$ holds, $\pi^{-1}(0)$ is an unramified fiber, and it is easy to describe $\pi^{-1}(0)$. Then, following c paths of W along the parameter interval $[0, 1]$, one can find a zero-dimensional parametrization for V. Section 3.7 gives a more detailed description.

The complexity of symbolic homotopy continuation methods is $Ln^{O(1)}c\delta$ arithmetic operations (see e.g. [34, 109, 162]), where

- L is the complexity to evaluate the input system,
- c is the number of paths to be followed, and
- δ is the degree of the curve W.

In comparison, the complexity of numeric homotopy continuation methods is $Ln^{O(1)}c\nu^2$ floating point operations (see e.g. [33]), where

- ν is the highest condition number arising from the application of the Implicit Function Theorem to the points of the following paths of $\pi^{-1}[0, 1] \cap W$.

There are several improvements which exploit the structure of the input system, for example, taking advantage of sparsity patterns, to reduce the complexity of finding the zero set of a given polynomial system by using homotopy methods. Homotopy algorithms for sparse systems are so-called polyhedral homotopies (see e.g. [175, 104, 174, 110], [100, 101, 102] and references therein). Polyhedral homotopies preserve the Newton polytopes of the input polynomials and rely on the BKK bound of the system.

We remark that most previously mentioned homotopy algorithms solve square systems, that is, systems with as many equations as unknowns, although extensions can deal with systems of positive dimension by using variants of algorithms for square systems. Note that using slack variables as in [164], polyhedral homotopies apply to over-determined systems but the control of their complexities is not known. Some dedicated homotopies have been designed for special over-determined systems as in [106, 166]. As far as we know, they cannot be used to solve the determinantal systems which we tackle in this thesis.

Finally, homotopy continuation techniques for multi-homogeneous polynomial systems can be found in [109] and [159].

Geometric resolution

The geometric resolution algorithm has been more recently studied [123, 87, 124] but goes back to [86, 84, 85]. Let V be a variety of dimension zero consisting of D points. A *geometric resolution* of V consists of a linear form $\ell(\boldsymbol{X}) = u_0 + u_1 x_1 + \cdots + u_n x_n$ in $\mathbb{K}[x_1, \ldots, x_n]$ and polynomials $(q, w_1, \ldots, w_n)$ in $\mathbb{K}[y]$, with y is a new variable, such that

- the linear form ℓ is a *primitive element* of V, i.e., $\ell(\boldsymbol{x}) \neq \ell(\boldsymbol{x}')$, for all $\boldsymbol{x} \neq \boldsymbol{x}'$ in V.
- the polynomial q is monic of degree D and $q(\ell(\boldsymbol{x})) = 0$ for all $\boldsymbol{x} \in V$; that is, $q = \prod_{\boldsymbol{x} \in V} y - \ell(\boldsymbol{x})$ is the *minimal polynomial* of ℓ over V.
- for $i = 1, \ldots, n$, $\deg(w_i) < \deg(q)$ and

$$V = \left\{ (w_1(\tau), \ldots, w_n(\tau)) \ : \ \tau \in \overline{\mathbb{K}}^n \text{ and } q(\tau) = 0 \right\};$$

  that is, w_i's polynomials parametrize V by the zeroes of q.

It is shown, for example in [87], that any generic enough hyperplane $\ell(\boldsymbol{X})$ will separate the points in V.

We remark that, given a zero-dimensional parametrization $\mathscr{R} = ((q, v_1, \ldots, v_n), \lambda)$ of a variety, we can obtain a geometric resolution of V as the following. Since q is square-free, then q' is invertible in $\mathbb{K}[y]/\langle q(y) \rangle$. Then, setting $w_i(y) := (q')^{-1}(y)\, v_i(y) \mod q(y)$, for $1 \leq i \leq n$, gives a geometric resolution $((q, w_1, \ldots, w_n), \lambda)$ of V.

Consider a system of polynomials $\boldsymbol{f} = (f_1, \ldots, f_n)$ in $\mathbb{K}[x_1, \ldots, x_n]$. For any $1 \leq i \leq n$, suppose that the algebraic set $\mathcal{V}_i$ defined by $(f_1, \ldots, f_i)$ is equidimensional of codimension i (see Section 3.1 for precise definitions) and the Jacobian matrix of $(f_1, \ldots, f_i)$ has full rank at the generic points of $\mathcal{V}_i$ (a system $\boldsymbol{f}$ satisfying all these conditions is called a *reduced regular* sequence). The *geometric degree* δ of the polynomial system $\boldsymbol{f}$ is defined as

$$\delta = \max_{1 \leq i \leq n} \deg(\mathcal{V}_i).$$

The geometric degree of a polynomial system measures the largest degree attained by adding the equations successively. If $\boldsymbol{f}$ is encoded by a straight-line program of length L, then, there exists a randomized algorithm [84, Theorem 19] that computes a geometric resolution of $V(\boldsymbol{f})$ within complexity $(nD\delta L)^{O(1)}$, where D is the numbers of points in $\overline{\mathbb{K}}^n \cap V(\boldsymbol{f})$.

Later on, Giusti et al. [87] introduced an algorithm to compute a geometric resolution of $V(\boldsymbol{f})$ using $\tilde{O}(n(nL + n^\omega)d^2\delta^2)$ operations in $\mathbb{K}$, where $d = \max_{1 \leq i \leq n}(\deg(f_i))$ and ω is the exponent in the complexity of the multiplication of two matrices with coefficients in $\mathbb{Q}$. As we will use this algorithm in Section 7.2, we restate the result in [87].

Theorem 1.3.1. [87, Theorem 1] *Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ of degree at most d and given by a straight-line program Γ of length at most L, such that $(f_1, \ldots, f_n)$ defines a reduced regular sequence.*

Then there exists a randomized algorithm called GeometricResolution *that takes Γ as the input and computes a geometric resolution of the variety $V(f_1, \ldots, f_n)$ by using*

$$O^{\sim}(n(nL + n^{\omega})d^2\delta^2)$$

operations in $\mathbb{K}$, where δ is the geometric degree of $(f_1, \ldots, f_n)$.

Gröbner basis computations

Gröbner bases which transform an input polynomial system into a triangular system was originated by Bruno Buchberger in his PhD thesis [36]. The Gaussian elimination algorithm applied to non-linear systems and the euclidean algorithm for multivariate polynomials are performed in order to obtain Gröbner bases. We will use Gröbner basis computations to perform our experiment in Section 10.4; for this latter purpuse, we give here a brief overview of Gröbner basis computations.

Monomial orderings on multivariate polynomial rings play an essential role in Gröbner basis computations. The most important example is the *lexicographic* (*lex*) *ordering* on $\mathbb{K}[x_1, \ldots, x_n]$, which are defined as $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \succ_{\text{lex}} x_1^{\beta_1} \cdots x_n^{\beta_n}$ if and only if the first non-zero entry of the vector $(\alpha_1, \ldots, \alpha_n) - (\beta_1, \ldots, \beta_n)$ in $\mathbb{Z}^n$ is positive. An ideal in $\mathbb{K}[x_1, \ldots, x_n]$ is called zero-dimensional if the variety defined by this ideal is of dimension zero. Performing Gröbner basis computations in the lex ordering $x_1 > x_2 > \cdots > x_n$ on a zero-dimensional ideal leads to an upper triangular structure such as the following

$$\begin{aligned} &g_1(x_1, \ldots, x_n), \ldots, g_{k_1}(x_1, \ldots, x_n), \\ &\qquad g_{k_1+1}(x_2, \ldots, x_n), \ldots, g_{k_2}(x_2, \ldots, x_n), \ldots, \\ &\qquad\qquad g_{k_{n-1}+1}(x_n), \ldots, g_{k_n}(x_n). \end{aligned}$$

A system with such a structure can be solved by using a backward solve strategy. That is, we first solve the variable x_n by using univariate equations $g_{k_{n-1}+1}(x_n) = \cdots = g_{k_n}(x_n) = 0$, then we solve for the variable x_{n-1} by using values of x_n and equations $g_{k_{n-2}+1}(x_{n-1}, x_n) = \cdots = g_{k_{n-1}}(x_{n-1}, x_n) = 0$, and so on, until all the solutions $x_n, \ldots, x_1$ of the original system are found. This procedure is convenient since we only need to solve univariate polynomial systems. However, the cost to compute the Gröbner basis in lex ordering by using Buchberger's algorithm is expensive as the degrees of polynomials occurring during the computation can become very large (see e.g. [112] and references therein).

In a Gröbner basis computation, pairs of polynomials (critical pairs) are chosen, the leading terms of polynomials are eliminated and the difference, which is known as the S-polynomial, is reduced by the current basis with respect to the fixed monomial ordering.

Many S-polynomials reduce to zero. However, if a new non-zero polynomial is found, then it is added to the basis and new critical pairs appear.

In recent decades, there have been many improvements made to Buchberger's algorithm. In the F_4 algorithm [58], Faugère reduces a numerous number of critical pairs at the same time by first constructing a matrix whose columns are indexed by the monomials and the rows are indexed by polynomials appearing in the polynomial division process, and then using linear algebra techniques to reduce this sparse matrix to a reduced row echelon form. The result of this process is all S-polynomials of all pairs considered. However, many rows reduce to zero in F_4, even when we also use the Buchberger's criterion [36]. Latter on, in the F_5 algorithm [59], Faugère builds a new criterion to detect useless critical pairs, and then to avoid unneeded computations. A variant of the algorithm in [59] which is suitable for the complexity analysis can be found in [17, 16, 15].

Another important algorithm which is used for zero-dimensional systems is the FGLM algorithm [61, 63, 107]. It takes as input a Gröbner basis for some monomial ordering, for example, the graded reverse lexicographical ordering, and outputs a Gröbner basis for a second monomial ordering, for instance, the lex ordering. The graded reverse lexicographical ordering (grevlex) on $\mathbb{K}[x_1, \ldots, x_n]$ is defined by $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \succ_{\text{grevlex}} x_1^{\beta_1} \cdots x_n^{\beta_n}$ if and only if either $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ or $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ and the last non-zero entry of the vector $(\alpha_1, \ldots, \alpha_n) - (\beta_1, \ldots, \beta_n)$ in $\mathbb{Z}^n$ is negative.

The FGLM algorithm is central for solving zero-dimensional systems since it is more efficient to compute first a Gröbner basis in grevlex ordering by using algorithms from [58, 59] and then to convert into a Gröbner basis for lex ordering by using FGLM algorithm. Indeed the degrees of polynomials occurred in the grevlex Gröbner basis are much smaller than those in the lex basis. Then computing grevlex Gröbner bases is more efficient than computing lex Gröbner bases directly. Furthermore, the complexity of the FGLM algorithm is well understood and is polynomial in the number of solutions of the input system.

We refer the reader to the articles [61, 58, 59, 17, 16, 15, 63] and to references therein for the state of art algorithms for computing Gröbner bases. Also, the books of Cox et. al. [45, 46] are good references for the reader to obtain a good overview of Gröbner bases and their applications.

1.4 Our Contributions

Consider a sequence of s polynomials $\boldsymbol{G}$ in $\mathbb{K}[x_1, \ldots, x_n]$ and a polynomial matrix $\boldsymbol{F}$ in $\mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with $p \leq q$ and $n = q - p + s + 1$. The set of points in $\overline{\mathbb{K}}^n$, denoted by $V_p(\boldsymbol{F}, \boldsymbol{G})$, at which the polynomials $\boldsymbol{G}$ vanish and the matrix $\boldsymbol{F}$ has rank defect is an algebraic set.

In this thesis, our goal is to compute the isolated or simple points in $V_p(\boldsymbol{F}, \boldsymbol{G})$. *Isolated points* in $V_p(\boldsymbol{F}, \boldsymbol{G})$ are points in the zero-dimensional irreducible components of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

Equivalently, these are all points $\boldsymbol{x}$ in $V_p(\boldsymbol{F},\boldsymbol{G})$ such that there exists a neighborhood of $\boldsymbol{x}$ in which the system defining $V_p(\boldsymbol{F},\boldsymbol{G})$ has no other solutions. *Simple points* in $V_p(\boldsymbol{F},\boldsymbol{G})$ are the points in $V_p(\boldsymbol{F},\boldsymbol{G})$ at which the associated Jacobian matrix of the system defining $V_p(\boldsymbol{F},\boldsymbol{G})$ has full rank. Note that the set of simple points is finite and is always a subset of the set of isolated points of $V_p(\boldsymbol{F},\boldsymbol{G})$ [53, Theorem 16.19].

It is natural to assume that $n = q-p+s+1$. Indeed results due to Macaulay [131] and Eagon and Northcott [52] imply that all irreducible components of the variety defined by maximal minors of $\boldsymbol{F}$ have codimension at most $q-p+1$. Then by Krull's theorem [120, 53] the irreducible components of $V_p(\boldsymbol{F},\boldsymbol{G})$ have codimension at most $q-p+s+1$. This implies that the irreducible components of $V_p(\boldsymbol{F},\boldsymbol{G})$ in $\overline{\mathbb{K}}^n$ have dimension at least $n-(q-p+s+1)$, which is positive when $n > q-p+s+1$. Furthermore, in the case $n = q-p+1$ (when $s=0$), it is proved, for instance, in [167], that $V_p(\boldsymbol{F},\boldsymbol{G})$ has dimension zero for a generic choice of polynomials $\boldsymbol{G}$ and entries of $\boldsymbol{F}$. Therefore, in this thesis, we restrict to the case when $n = q-p+s+1$. Note that for the systems coming from optimization, this condition is satisfied since in these cases $p = s+1$ and $q = n$.

Note also that, even when $n = q-p+s+1$, the algebraic set $V_p(\boldsymbol{F},\boldsymbol{G})$ may have components of positive dimension. In this case, we will be interested in computing the isolated points in $V_p(\boldsymbol{F},\boldsymbol{G})$, while in some situations, we are only interested in computing the simple points in $V_p(\boldsymbol{F},\boldsymbol{G})$.

We recall the notion of multiplicity of a point $\boldsymbol{x}$ with respect to an ideal I in $\overline{\mathbb{K}}[x_1,\ldots,x_n]$. This notion extends to ideals in $\mathbb{K}[x_1,\ldots,x_n]$ by considering their extension in $\overline{\mathbb{K}}[x_1,\ldots,x_n]$. We refer the readers to Section 3.1 for more details of the following notions. The ideal I can be written as $I = Q_1\cap\cdots\cap Q_r$, for some primary ideals $Q_1,\ldots,Q_r$; this decomposition is said to be minimal if $V(Q_i)\neq V(Q_j)$ for $i\neq j$. For any isolated point $\boldsymbol{x}$ in $V(I)$, there exists a unique primary component Q_i, for $1\leq i\leq r$, which has dimension zero, such that $\boldsymbol{x}$ is in Q_i. Since we take a primary decomposition over $\overline{\mathbb{K}}$, one can has $Q_i = \{\boldsymbol{x}\}$. Although minimal primary decompositions are not unique, the fact that $\boldsymbol{x}$ is isolated in $V(I)$ implies that Q_i does not depend on the primary decomposition that we are considering. Then, the *multiplicity* of $\boldsymbol{x}$ is defined as the dimension of the $\overline{\mathbb{K}}$-vector space $\overline{\mathbb{K}}[x_1,\ldots,x_n]/Q_i$. When $\boldsymbol{x}=0$ in $\overline{\mathbb{K}}^n$, by [46, Theorem 4.2.2], the dimension of $\overline{\mathbb{K}}[x_1,\ldots,x_n]/Q_i$ equals the dimension of $\overline{\mathbb{K}}[[x_1,\ldots,x_n]]/Q_i$, where $\overline{\mathbb{K}}[[x_1,\ldots,x_n]]$ is the ring of the formal power series in $(x_1,\ldots,x_n)$, with coefficients in $\overline{\mathbb{K}}^n$.

A local dimension test

Note that the set $V_p(\boldsymbol{F},\boldsymbol{G})$ is the same as $V(\boldsymbol{C})$ where $\boldsymbol{C} = (c_1,\ldots,c_s,c_{s+1},\ldots,c_m)$ in $\mathbb{K}[x_1,\ldots,x_n]$, with $m = s+\binom{q}{p}$, $(c_1,\ldots,c_s) = \boldsymbol{G}$ and $(c_{s+1},\ldots,c_m)$ the p-minors of $\boldsymbol{F}$. We use this representation when it is convenient for us.

Our first contribution is an algorithm which takes as input a polynomial system $\boldsymbol{C} = (c_1,\ldots,c_m)$ and a point $\boldsymbol{x}\in\overline{\mathbb{K}}^n$ in the zero set $V(\boldsymbol{C})$ of $\boldsymbol{C}$, and decides whether $\boldsymbol{x}$ is an isolated point of $V(\boldsymbol{C})$.

Without any other information, this problem is difficult to solve efficiently. However, when a bound μ on the multiplicity of $\boldsymbol{x}$ as a root of $\boldsymbol{C}$ is known, it is possible to get an algorithm with a good complexity for this decision problem. Given a bound μ, we establish an algorithm which solves this decision problem in time polynomial in the bound μ, the number of equations m, the number of variables n, and the complexity of evaluation of $\boldsymbol{C}$. This result is given in Section 5.1, Chapter 5.

We remark that testing that a point $\boldsymbol{x}$ in $V(\boldsymbol{C})$ is a simple point in $V(\boldsymbol{C})$ is much easier than deciding whether it is an isolated point. Indeed we only need to compute the Jacobian matrix associated to $\boldsymbol{C}$ and then find the rank of this matrix at $\boldsymbol{x}$.

Determinantal homotopy algorithms

Assuming there exists a suitable homotopy deformation, we give an algorithm which takes as input the system $\boldsymbol{C} = (c_1, \ldots, c_m)$ and computes a zero-dimensional parametrization of the isolated points of $V(\boldsymbol{C})$. More precisely, let t be a new variable, and suppose that we know a family of polynomials $\boldsymbol{B} = (b_1, \ldots, b_m)$ in $\mathbb{K}[t, \boldsymbol{X}]$, where $\boldsymbol{X} = (x_1, \ldots, x_n)$ such that $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$. Let $\boldsymbol{A}$ be the polynomials $\boldsymbol{B}(0, \boldsymbol{X})$ in $\mathbb{K}[\boldsymbol{X}]$, and suppose $V(\boldsymbol{A})$ is finite, and that we are able to find a zero-dimensional parametrization of $V(\boldsymbol{A})$ efficiently. We then give symbolic homotopy algorithms which take as inputs the polynomials $\boldsymbol{B}$, together with a zero-dimensional parametrization of $V(\boldsymbol{A})$, under certain regularity assumptions, and which computes a zero-dimensional parametrization of either the isolated solutions or the simple solutions of $\boldsymbol{C}$. This is where we use the local dimension testing algorithms mentioned earlier.

The complexity we obtain depends linearly on the evaluation of $\boldsymbol{C}$ and polynomially on the sum of the multiplicities of isolated points (or simple points) in $V(\boldsymbol{C})$ and the degree of the homotopy curve. These algorithms are given in Section 5.2, Chapter 5. Note that our algorithms work for any systems which satisfy certain regularity assumptions.

To apply these results to our determinantal problems, given polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[\boldsymbol{X}]$ and $\boldsymbol{F}$ in $\mathbb{K}[\boldsymbol{X}]^{p \times q}$, we will build a matrix

$$\boldsymbol{U} = (1 - t) \cdot \boldsymbol{L} + t \cdot \boldsymbol{F} \in \mathbb{K}[t, \boldsymbol{X}]^{p \times q}$$

that connects a suitable *start matrix* $\boldsymbol{L}$ to the target matrix $\boldsymbol{F}$, together with a sequence $\boldsymbol{V} = (v_1, \ldots, v_s)$ in $\mathbb{K}[t, \boldsymbol{X}]$ of the form

$$\boldsymbol{V} = (1 - t) \cdot \boldsymbol{M} + t \cdot \boldsymbol{G} \in \mathbb{K}[t, \boldsymbol{X}]^s$$

that connects a *start sequence* $\boldsymbol{M} = (m_1, \ldots, m_s)$ in $\mathbb{K}[\boldsymbol{X}]$ to the polynomials $\boldsymbol{G}$. The *start system* $\boldsymbol{A} = (a_1, \ldots, a_s, a_{s+1}, \ldots, a_m)$ in $\mathbb{K}[\boldsymbol{X}]$ is given by $(a_1, \ldots, a_s) = (m_1, \ldots, m_s)$ and $(a_{s+1}, \ldots, a_m)$ are the p-minors of $\boldsymbol{L}$, the *deformed system* $\boldsymbol{B} = (b_1, \ldots, b_s, b_{s+1}, \ldots, b_m)$ in $\mathbb{K}[t, \boldsymbol{X}]$ is defined as $(b_1, \ldots, b_s) = (v_1, \ldots, v_s)$ and $(b_{s+1}, \ldots, b_m)$ are the p-minors of $\boldsymbol{U}$; all the p-minors of $\boldsymbol{L}$ and $\boldsymbol{U}$ are followed the same order as those of $\boldsymbol{F}$. By this construction, it is clear that $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$ and $\boldsymbol{B}(0, \boldsymbol{X}) = \boldsymbol{A}$. We show in Section 5.3 that these systems satisfy all regularity assumptions for the determinantal homotopy algorithms above.

Determinantal varieties

Bounds on the number of isolated solutions of $V_p(\boldsymbol{F}, \boldsymbol{G})$**.** As we have seen so far, the number of solutions of a given system plays an important role in the polynomial system solving. Our next contribution is to give bounds on the number of isolated points in $V_p(\boldsymbol{F}, \boldsymbol{G})$.

In order to state this, we will consider two degree measures for the matrix $\boldsymbol{F}$ which have been previously used in [144, 136]. For $i = 1, \ldots, p$, we will write $\mathrm{rdeg}(\boldsymbol{F}, i)$ for the degree of the ith row of $\boldsymbol{F} = [f_{i,j}]_{1 \leq i \leq p, 1 \leq j \boldsymbol{q}}$, that is, $\mathrm{rdeg}(\boldsymbol{F}, i) = \max_{1 \leq j \leq q}(\deg(f_{i,j}))$. Similarly, for $j = 1, \ldots, q$, we write $\mathrm{cdeg}(\boldsymbol{F}, j)$ for the degree of the j-th column of $\boldsymbol{F}$, that is, $\mathrm{cdeg}(\boldsymbol{F}, j) = \max_{1 \leq i \leq p}(\deg(f_{i,j}))$.

We prove that the sum of multiplicities of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$ is at most $\min(c, c')$, with

$$c = \deg(g_1) \cdots \deg(g_s) \cdot \eta_{n-s}(\mathrm{cdeg}(\boldsymbol{F}, 1), \ldots, \mathrm{cdeg}(\boldsymbol{F}, q))$$

and

$$c' = \deg(g_1) \cdots \deg(g_s) \cdot h_{n-s}(\mathrm{rdeg}(\boldsymbol{F}, 1), \ldots, \mathrm{rdeg}(\boldsymbol{F}, p)),$$

where $\eta_k(\cdot)$ is the k-th elementary symmetric function and $h_k(\cdot)$ is the k-th complete symmetric function. This result is presented as a part of Chapter 6.

Computing zero-dimensional parametrizations of the isolated/simple points of $V_p(\boldsymbol{F}, \boldsymbol{G})$**.** Our algorithms take as input a straight-line program that computes $\boldsymbol{G}$ and all entries of $\boldsymbol{F}$ from the input variables $\boldsymbol{X}$. The runtimes of our algorithms are linear in the length of a straight-line program that evaluates $\boldsymbol{G}$ and all entries of $\boldsymbol{F}$ and polynomial in the sum of multiplicities of isolated solutions of $V_p(\boldsymbol{F}, \boldsymbol{G})$ (which is bounded by $\min(c, c')$) and the degree of the homotopy curve which is at most $\min(e, e')$, where

$$e = (\deg(g_1) + 1) \cdots (\deg(g_s) + 1) \cdot \eta_{n-s}(\mathrm{cdeg}(\boldsymbol{F}, 1) + 1, \ldots, \mathrm{cdeg}(\boldsymbol{F}, q) + 1)$$

and

$$e' = (\deg(g_1) + 1) \cdots (\deg(g_s) + 1) \cdot \eta_{n-s}(\mathrm{rdeg}(\boldsymbol{F}, 1) + 1, \ldots, \mathrm{rdeg}(\boldsymbol{F}, q) + 1).$$

The main step in our algorithms is using determinantal homotopy algorithms above. To give concrete algorithms, we will have to specify how to define the polynomials $\boldsymbol{M}$ and the matrix $\boldsymbol{L}$, and how to solve the start system $\boldsymbol{A} = 0$. The construction of the system $\boldsymbol{M}$ will be straightforward. The main difficulty lies in the definition of a matrix $\boldsymbol{L}$ that will respect either the column-degree or the row-degree of $\boldsymbol{F}$, while satisfying all assumptions needed for the determinantal homotopy algorithms and allowing us to solve the resulting system $\boldsymbol{A} = 0$ easily. The column-degree case is treated in Section 6.2, while the more complicated case, using the row-degree, is given in Section 6.3.

Determinantal varieties defined by sparse polynomials and application in weighted domains

Consider polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ and a matrix $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with all elements of $\boldsymbol{G}$ and entries of $\boldsymbol{F}$ being sparse. In this situation, we wish to describe the isolated zeros of our algebraic set $V_p(\boldsymbol{F}, \boldsymbol{G})$ only in the *column-support* case with the row-support case left for future work. The tools used to create our sparse column support homotopy also allows us to build a column homotopy algorithm for determinantal systems for weighted degree polynomials. This work is presented in Chapter 7.

Bound on the number of isolated solutions of $V_p(\boldsymbol{F}, \boldsymbol{G})$**.** For $1 \leq i \leq s$, let $\mathcal{A}_i \subset \mathbb{N}^n$ denote the support of g_i, to which we add the origin $\mathbf{0} \in \mathbb{N}^n$. For $1 \leq k \leq q$, let $\mathcal{B}_j \subset \mathbb{N}^n$ be the union of the supports of the polynomials in the k-th column of $\boldsymbol{F}$, to which we add $\mathbf{0}$ as well. For $1 \leq i \leq s$ and $1 \leq k \leq q$, we let $\mathcal{C}_i$ and $\mathcal{D}_k$ be the convex hulls of respectively $\mathcal{A}_i$ and $\mathcal{B}_k$.

We show that the sum of multiplicities of isolated points in $V_p(\boldsymbol{F}, \boldsymbol{G})$ is at most

$$\chi = \sum_{\boldsymbol{i} \subset \{1,\ldots,q\}^{n-s}} \mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_s, \mathcal{D}_{i_1}, \ldots, \mathcal{D}_{i_{n-s}}),$$

where $\mathsf{MV}(\cdot)$ denotes the mixed volume of some Newton polytopes.

Computing zero-dimensional parametrization of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$**.** Having in mind to apply the determinantal homotopy algorithms, we determine a family of possible start systems, that is, a family of polynomials $\boldsymbol{M}$ and matrix $\boldsymbol{L}$, and we show that a generic member of this family allows us to carry out the procedure successfully; we also show how to compute the solutions of this start system.

Our runtime is polynomial in the bound χ on the number of isolated points in $V_p(\boldsymbol{F}, \boldsymbol{G})$ and the degree of the homotopy curve, both depending on certain mixed volumes related to the polynomials $\boldsymbol{G}$ and the columns of $\boldsymbol{F}$.

Note that we can compute the simple solutions of $V_p(\boldsymbol{G}, \boldsymbol{F})$ as well by using the determinantal homotopy algorithms for computing the simple points which does not require any extra work.

Weighted determinantal varieties. Let $\boldsymbol{w} = (w_1, \ldots, w_n)$ be positive integers and let $\mathbb{K}[x_1, \ldots, x_n]_{\boldsymbol{w}}$ be a polynomial ring of weights $\boldsymbol{w}$. Consider a sequence of polynomials $\boldsymbol{G}$ in $\mathbb{K}[\boldsymbol{X}]_{\boldsymbol{w}}$, with $\boldsymbol{X} = (x_1, \ldots, x_n)$, and a matrix $\boldsymbol{F} = [f_{i,j}]_{1 \leq i \leq p, 1 \leq j, \leq q}$ in $\mathbb{K}[\boldsymbol{X}]_{\boldsymbol{w}}^{p \times q}$.

We prove that the number of isolated points in $V_p(\boldsymbol{F}, \boldsymbol{G})$ is decreased by a factor of $w_1 \cdots w_n$, when compared to the problem that we study in classical domains (the polynomial rings with weights $\boldsymbol{w} = (1, \ldots, 1)$). That is, the sum of multiplicities of the isolated

points in $\boldsymbol{V}_p(\boldsymbol{F}, \boldsymbol{G})$ is bounded by

$$\frac{1}{w_1 \cdots w_n} \cdot \mathrm{wdeg}(g_1) \cdots \mathrm{wdeg}(g_s) \cdot \eta_{n-s}(\mathrm{wcdeg}(\boldsymbol{F}, 1) \cdots, \mathrm{wcdeg}(\boldsymbol{F}, q)),$$

where, for $1 \leq k \leq q$, $\mathrm{wcdeg}(\boldsymbol{F}, k) = \max_{1 \leq k \leq q}(\mathrm{wdeg}(f_{i,k}))$ is the weighted degree of the k-th column of $\boldsymbol{F}$.

We apply the determinantal homotopy algorithms once again; however, we do not need to verify all assumptions in order to use these algorithms since we have mentioned that weighted domains have a natural sparse structure, when compared to polynomials in classical domains. We show that one obtains a speed-up which is polynomial in the product of the weights to compute the isolated solutions of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

Invariant algebraic systems

We now move to our contribution for the problem of computing critical points defined by symmetric polynomials. Given $\mathcal{S}_n$-invariant polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ and ϕ. We want to describe the set $W(\phi, \boldsymbol{G})$ of points in $\overline{\mathbb{K}}^n$ at which $\boldsymbol{G}$ vanish and $\mathrm{Jac}(\boldsymbol{G}, \phi)$ has not full rank. One can verify that although the equations defining $W(\phi, \boldsymbol{G})$ are not invariant, they form an equivariant system and the defined algebraic set $W(\phi, \boldsymbol{G})$ is invariant (see Chapter 8 for more details).

Algorithm to turn an equivariant system into an invariant one. For positive integers $\ell_1, \ldots, \ell_r$, let $\boldsymbol{Z}_i = (z_{i,1}, \ldots, z_{i,\ell_i})$ be a set of ℓ_i indeterminates, for $i = 1, \ldots, r$. The group $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$ acts naturally on $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]$; it can be seen as a subgroup of the permutation group $\mathcal{S}_\ell$ of $\{1, \ldots, \ell\}$, with $\ell = \ell_1 + \cdots + \ell_r$, where $\mathcal{S}_{\ell_1}$ acts on the first ℓ_1 indices, $\mathcal{S}_{\ell_2}$ acts on the next indices, and so on.

A sequence of polynomials $\boldsymbol{q} = (q_1, \ldots, q_\ell)$ in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]$ is called $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$-equivariant if for any σ in $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$ and i in $\{1, \ldots, \ell\}$, we have $\sigma(q_i) = q_{\sigma(i)}$. Geometrically, the zero-set of $V(\boldsymbol{q})$ in $\overline{\mathbb{K}}^\ell$ is $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$-invariant, although the equations themselves may not be invariant.

Consider a sequence of $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$-invariant polynomials $\boldsymbol{p} = (p_1, \ldots, p_\ell)$. The fundamental theorem of symmetric polynomials allows us to work with polynomials in $\mathbb{K}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r]$, with $\boldsymbol{e}_i = (e_{i,1}, \ldots, e_{i,\ell_i})$ for $i = 1, \ldots, r$, in order to represent a certain "compressed" image $V(\boldsymbol{p})' \subset \overline{\mathbb{K}}^\ell$ of $V(\boldsymbol{p})$. Here $(e_{i,1}, \ldots, e_{i,\ell_i})$ are variables standing for the elementary symmetric functions in $\boldsymbol{Z}_i = (z_{i,1}, \ldots, z_{i,\ell_i})$. Computing this compression saves considerable computations, indeed reducing the number by a factor of $\ell_1! \cdots \ell_r!$, when compared to describing the set $V(\boldsymbol{p})$. Therefore, it is meaningful to have an efficient algorithm which turns an $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$-equivariant system into one which is $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$-invariant.

Given an $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$-equivariant polynomials $\boldsymbol{q} = (q_1, \ldots, q_\ell)$ of degrees at most d. Our algorithm takes as input $\boldsymbol{q}$ and computes a sequence of $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$-invariant polynomials $\boldsymbol{p} = (p_1, \ldots, p_\ell)$ such that $V(\boldsymbol{q})$ and $V(\boldsymbol{p})$ are the same in a suitable localization. The complexity of our algorithm is polynomial in ℓ and $\binom{\ell+d}{d}$.

Algorithm to compute a symmetric representation of $W(\phi, \boldsymbol{G})$**.** The global invariance property of $W(\phi, \boldsymbol{G})$ allows us to split the set $W(\phi, \boldsymbol{G})$ into orbits under the action of the symmetric group. The output of our algorithm will be a collection of zero-dimensional parametrizations, one for each of the sets of the compression of the orbits of $W(\phi, \boldsymbol{G})$. We will call such a data structure a *symmetric representation* of $W(\phi, G)$ (precise definitions are in Section 9.2).

Suppose $\boldsymbol{G} = (g_1, \ldots, g_s)$ and ϕ are $\mathcal{S}_n$-invariant polynomials in $\mathbb{K}[x_1, \ldots, x_n]$, with the degree at most d, and suppose that $W(\phi, \boldsymbol{G})$ is finite. We provide a randomized algorithm that takes as input $\boldsymbol{G}$ and ϕ and outputs a symmetric representation for $W(\phi, \boldsymbol{G})$. The runtime of our algorithm is polynomial in $d^s, \binom{n+d}{d}, \binom{n}{s+1}$, with the size of the output of our algorithm being at most $d^s\binom{n+d-1}{n}$.

1.5 Related work

Bounds on the number of isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$, the general case

Pioneering work of Giambelli-Thom-Porteous (see e.g. [74] or [72]) already established similar bounds under regularity assumptions (when $V(\boldsymbol{G})$ is smooth and/or $V_p(\boldsymbol{F}, \boldsymbol{G})$ has the expected codimension). We are not aware of further generalizations focusing on isolated points and taking into account multiplicities.

Previous work by Miller and Sturmfels [136, Chapter 15] proved general results on the multi-degrees of determinantal ideals built from matrices with indeterminate entries (here $s = 0$, but the assumption $n = q - p + 1$ does not hold); they obtain analogues and generalizations of our result in that context.

Nie and Ranestad proved in [144] that the bounds in our result for the sum of multiplicities of isolated points in $V_p(\boldsymbol{F}, \boldsymbol{G})$ are tight for two families of polynomials when all entries of $\boldsymbol{F} = [f_{i,j}]$ in $\mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ are generic and homogeneous in $n + 1$ variables

- when $\deg(f_{i,j}) = \operatorname{cdeg}(\boldsymbol{F}, j)$ for all i, j, then the degree of the ideal generated by all maximal minors of $\boldsymbol{F}$ is $\eta_n(\operatorname{cdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{cdeg}(\boldsymbol{F}, q))$;
- when $\deg(f_{i,j}) = \operatorname{rdeg}(\boldsymbol{F}, i)$ for all i, j, then the degree of the ideal generated by all maximal minors of $\boldsymbol{F}$ is $h_n(\operatorname{cdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{cdeg}(\boldsymbol{F}, q))$.

From this, they deduce that the degree of the ideal generated by $\boldsymbol{G}$ and all maximal minors of $\boldsymbol{F}$ is at most $\deg(g_1)\cdots\deg(g_s)h_{n-s}(\mathrm{rdeg}(\boldsymbol{F},1),\ldots,\mathrm{rdeg}(\boldsymbol{F},p))$, for systems coming from optimization, assuming that this ideal has dimension zero. In addition, Spaenlehauer also gave in [167] explicitly the Hilbert function of this ideal, for a generic input $(\boldsymbol{F},\boldsymbol{G})$.

Algorithms to describe $V_p(\boldsymbol{F},\boldsymbol{G})$

It is well-known that Gröbner bases behave rather well on over-determined systems. Starting from the determination of the Hilbert function of a determinantal ring due to Conca and Herzog [43], complexity estimates are given in [66, 65] for computing Gröbner bases of ideals generated by either r-minors of $\boldsymbol{F}$, for some integer $1 \leq r \leq p$, or $\boldsymbol{G}$ and all r-minors of $\boldsymbol{F}$ for inputs coming from optimization problems. However, these require some genericity assumptions on the entries of $\boldsymbol{F}$ or $\boldsymbol{G}$ and in addition the input polynomials must also have all the same degree. These works culminated with the result by Spaenlehauer in [167] when he removes this latter degree assumption and provides sharp complexity statements, still under genericity assumptions on the input $(\boldsymbol{F},\boldsymbol{G})$.

Systems encoding rank defects in polynomial matrices have also been studied in the scope of the so-called geometric resolution algorithm in [9] and [160]. The algorithms in these references describe only points in $V_p(\boldsymbol{F},\boldsymbol{G})$ at which isolated solutions which are not simple are not considered. Computing isolated points of $V_p(\boldsymbol{F},\boldsymbol{G})$ could be done using Lecerf's equidimensional decomposition algorithm, still based on the geometric resolution [123, 124]. The cost of these algorithms is quadratic in certain geometric quantities (the degree of algebraic sets defined by subsystems of the determinantal equations we are dealing with). This compares with the runtimes (see Theorem 4.2.3 for more details), where the main contributions are the products $\binom{q}{p}ce$, respectively $\binom{q}{p}c'e'$, and where ce and $c'e'$, are also of a geometric nature. Further work is needed to compare the degrees involved in these complexity estimates with ours, and the resulting runtimes.

As previously mentioned, our algorithms are based on a symbolic homotopy continuation with the references for this method in Section 1.3. Most aforementioned algorithms solve square systems, that is, systems with as many equations as unknowns; though extensions can deal with systems of positive dimension by using variants of algorithms for square systems. On the other hand, we deal with determinantal systems of equations, which are in essence over-determined, with more equations than unknowns which is made possible by the algebraic properties of determinantal ideals.

Finally, algorithms in [159] can be used to find the isolated solutions of $V_p(\boldsymbol{F},\boldsymbol{G})$, however, the complexity estimates obtained there depend on multi-homogeneous Bézout bounds involving the maxima of $\mathrm{rdeg}(\boldsymbol{F},1),\ldots,\mathrm{rdeg}(\boldsymbol{F},p)$ or $\mathrm{cdeg}(\boldsymbol{F},1),\ldots,\mathrm{cdeg}\ (\boldsymbol{F},q)$.

Sparse systems and weighted domains

Our results for sparse determinantal ideals gives the first set of homotopy algorithms which simultaneously exploits both the determinantal structure and sparsity.

We remark that one can encode rank deficiencies in a polynomial matrix using extra variables (sometimes called Lagrange multipliers in the context of polynomial optimization) to encode that the kernel of the considered matrix is non-trivial. This would lead to systems with a sparse structure, which could be solved using homotopy techniques, for example, from [110] and [100, 101, 102]. However this technique does not work when isolated solutions to our determinantal system lead to rank deficiencies higher than one. Such isolated points of our determinantal system do not correspond to isolated points of the Lagrange system.

Note also that the same reason can be seen when one wants to compute isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$ in general. Furthermore, even when all isolated solutions to our determinantal system lead to rank deficiency one, then using symbolic homotopy algorithms for the new square system with Lagrange multipliers has the complexity depending on $\deg(g_1)\cdots\deg(g_s)(\mathrm{cdeg}(\boldsymbol{F},1)+1)\cdots(\mathrm{cdeg}(\boldsymbol{F},1)+1)$ (this quantity is greater than our bound c) which is slower than our algorithms. Also, determinantal systems in the context of Gröbner bases [66, 65, 167] do not take into account the sparsity of the entries.

Weighted homogeneous systems have been studied before including some results about weighted Bézout's theorem, the Hilbert series, and the Hilbert function of weighted homogeneous ideal. There are also several works for the computation strategy for weighted systems (see e.g. [67, 68] and references therein). To the best of our knowledge, there is no previous work that exploits determinantal systems in the weighted structure of polynomials.

Computing critical points for invariant systems

Pioneering work in [20, Section 14.2] and [65, 167] has established algorithms for determining critical points of a given function. When ϕ is linear, there exist algorithms to compute such points using $d^{O(n)}$ operations in $\mathbb{K}$ [20, Section 14.2]. More precisely, using Gröbner basis techniques, the paper [65, Corollary 3] establishes that, if the polynomials $f_1,\ldots,f_s$ are generic enough of degree d, then this computation can be done using

$$O\left(\binom{n+D_{\mathrm{reg}}}{n}^{\omega}+n\left(d^s\,(d-1)^{n-s}\binom{n-1}{s-1}\right)^3\right)$$

operations in $\mathbb{K}$. Here $D_{\mathrm{reg}}=d(s-1)+(d-2)n+2$, and ω is the exponent of multiplying two $(n\times n)$-matrices with coefficients in $\mathbb{K}$. A generalization to systems with mixed degrees can be found in [167]. In our algorithms, we do not need the genericity assumption of the input.

On the other hand, there has been considerable work on solving symmetric algebraic systems. Indeed, while it is always possible to compute the Gröbner basis of a set of symmetric polynomials, symmetries of the initial system are lost during the computation. In [41], for a finite symmetry group, Colin proposed to use primary and secondary invariants [170] to reformulate the problem. For the particular case of $\mathcal{S}_n$-invariant equations, in [64], the authors compute a SAGBI-Gröbner basis in the ring $\mathbb{K}[e_1, \ldots, e_n]$, where e_i is a variable corresponding to i-th elementary symmetric polynomial η_i in $(x_1, \ldots, x_n)$. However, the polynomials defines $W(\phi, \boldsymbol{G})$ ($\boldsymbol{G}$ and all $(s+1)$-minors of $\mathrm{Jac}(\boldsymbol{G}, \phi)$) are usually not invariant, so these technique cannot be directly applied to our problem.

Note that although the system defines $W(\phi, \boldsymbol{G})$ is not invariant under the action of the symmetric group $\mathcal{S}_n$, it is $\mathcal{S}_n$-equivariant. For such $\mathcal{S}_n$-equivariant systems, following [62], the authors in [69] used divided differences to construct a new system which is $\mathcal{S}_n$-invariant. Our work is inspired by this reference, but the specific type of the equations that we solve, involving minors of a Jacobian matrix, requires us to extend the work from [69]. Furthermore, no complexity analysis is given in that reference.

Finally, Nie and Ranestad proved in [144, Theorem 2.2] the size of $W(\phi, \boldsymbol{G})$ is bounded by $\tilde{\mathfrak{c}} = d^s\,(d-1)^{n-s}\binom{n}{s}$ which is larger than our bound $\mathfrak{c} = d^s\binom{n+d-1}{n}$ for the number of points that our algorithm outputs. For example, when $d = 2$, we have $\mathfrak{c} = 2^s(n+1)$ while $\tilde{\mathfrak{c}} = 2^s\binom{n}{s}$. More generally, when d and s are fixed, $\mathfrak{c}$ is polynomial in n (since it is bounded above by $d^s(n+d-1)^d$) while $\tilde{\mathfrak{c}}$ is exponential in n (since it is greater than $(d-1)^n$). When s is fixed and $d = n$, $\mathfrak{c}$ is $n^{O(1)}2^n$, whereas $\tilde{\mathfrak{c}}$ is $n^{O(1)}(n-1)^{n-s}$.

1.6 Organization of the thesis

This thesis consists of two main parts: Part I (from Chapter 4 to Chapter 7) contains our results for determinantal systems and Part II (from Chapter 8 to Chapter 10) is devoted for our contribution for invariant systems. The chapter contents are organized as follows:

- In Chapter 3, we recall some notions, notations, and some known properties of commutative algebra and algebraic geometry, polynomial rings. The complexity model, complexity estimates, and the data structures which are used in the thesis are also included in this chapter; at the end of it, we introduce the basic ideas of symbolic homotopy methods for polynomial system solving.

- In Chapter 4, we define precisely the problems that we are going to solve in the determinantal ideals. We also give a summary for our results and a roadmap on how to obtain them in this chapter.

- In Chapter 5, we provide an algorithm to decide whether a point in the zero-set of a polynomial system is isolated. Our symbolic determinantal homotopy algorithms to solve determinantal systems are given in this chapter as well.

- In Chapter 6, we study two degree measures for the matrix, the column-degree case and the row-degree one, and show how to use the determinantal homotopy algorithms in each situation.
- In Chapter 7, we show how to use the determinantal homotopy algorithms when all entries of the input are sparse polynomials or in weighted polynomial rings.
- In Chapter 8, we give a detailed description for the problem that we would like to treat in invariant polynomial systems and our contribution on this problem.
- In Chapter 9, we present how to describe group orbits of invariant sets, by means of partitions of positive integers, and the data structure that we use to represent invariant sets and some basic algorithms related to it. Our algorithm which turns a block equivariant system into one which is block invariant is also presented in this chapter.
- In Chapter 10, we show how to compute the data structure of the set of points at which the symmetric polynomials $\boldsymbol{G}$ vanish and the Jacobian matrix $\mathrm{Jac}(\boldsymbol{G}, \phi)$ associated to $\boldsymbol{G}$ and the symmetric polynomial ϕ is not full rank.
- In Chapter 11, we summarize our findings and provide some topics for future research.

Results in this thesis are papers as follows.

- **Solving determinantal systems using homotopy techniques.** Jon D. Hauenstein, Mohab Safey El Din, Éric Schost, and Thi Xuan Vu, accepted to Journal of Symbolic Computation.

  This article contains the results of Chapter 5 and Chapter 6.
- **Homotopy techniques for solving sparse column support determinantal polynomial systems.** George Labahn, Mohab Safey El Din, Éric Schost, and Thi Xuan Vu (submitted).

  This article contains the results of Chapter 7.
- **Computing critical points for invariant algebraic systems.** Jean-Charles Faugère, George Labahn, Mohab Safey El Din, Éric Schost, and Thi Xuan Vu (submitted).

  This article contains the results of Chapter 9 and Chapter 10.

Chapter 2

Résumé en Français

2.1 Motivations et problématiques

Le sujet central de cette thèse porte sur la conception d'algorithmes efficaces pour la résolution de systèmes polynomiaux (également appelés "systèmes algébriques") à coefficients dans un corps $\mathbb{K}$ qu'on supposera souvent de caractéristique zéro (à l'instar de $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$) ou bien de caractéristique suffisamment grande.

De tels systèmes modélisent des phénomènes non-linéaires et statiques. Ceux-ci sont légions notamment car l'essentiel des contraintes de la géométrie euclidienne (distance, colinéarité, orthogonalité, etc.) s'expriment algébriquement. Ainsi, la résolution de systèmes polynomiaux apparaît dans de nombreuses applications des sciences de l'ingénieur, par exemple en robotique [147], théorie du signal [89], chimie et biologie [140], et des sciences du numérique comme, par exemple, la cryptologie (voir par exemples [88, 137, 138, 50]), la géométrie algorithmique [20, 45, 46], la vision par ordinateur [145] ou encore la vérification de programmes.

On distingue classiquement les systèmes polynomiaux qui admettent un nombre fini de solutions dans une clôture algébrique $\overline{\mathbb{K}}$ de $\mathbb{K}$ (ils sont dits de "dimension zéro" par abus de langage) des autres qui sont alors dits de dimension positive. Dans cette thèse, on s'intéresse plus spécifiquement à la conception d'algorithmes pour la résolution de systèmes polynomiaux de dimension zéro.

Le caractère non-linéaire des problèmes abordés rend parfois les méthodes numériques délicates à certifier, qu'elles soient locales (comme celles fondées sur des itérations de Newton) ou globales (comme celles fondées sur des homotopies numériques).

Ceci nous fait privilégier les méthodes algébriques, du calcul formel. Ces méthodes peuvent parfois être plus lentes en pratique mais, d'une part, elles sont plus robustes à tout point de vue (notamment les sorties calculées sont des codages exacts des solutions) et d'autre part, nombre des applications mentionnées plus haut ne nécessitent pas de réponse

en temps réel. Enfin, le caractère algébrique des calculs menés permet de s'appuyer sur des résultats de complexité théorique qui, bien souvent, ont un impact pratique très concret.

Ainsi, dans notre contexte, "résoudre" des systèmes polynomiaux à coefficients dans $\mathbb{K}$ de dimension zéro va consister à calculer une représentation exacte des solutions dans $\overline{\mathbb{K}}$. Comme on l'a dit, les solutions sont en nombre fini et les coordonnées de ces solutions sont $\mathbb{K}$-algébriques (c'est-à-dire qu'elles sont racines de polynômes univariés à coefficients dans $\mathbb{K}$).

La représentation, classique, qui sera calculée par les algorithmes de cette thèse, s'inspire du théorème de l'élément primitif et trouve ses origines dans les travaux de Kronecker [119]. Il s'agit de représenter les coordonnées des solutions par l'évaluation de polynômes (ou fractions rationnelles) univariées à coefficients dans $\mathbb{K}$ en les racines d'un polynôme univarié à coefficients dans $\mathbb{K}$ également.

Par exemple, il est aisé, par un calcul simple d'algèbre linéaire, de représenter $(\sqrt{2}, \sqrt{3})$ en fonction de $\vartheta = \sqrt{2} + \sqrt{3}$, en développant $1, \vartheta, \vartheta^2, \vartheta^3$. Ainsi, de manière générale, on représentera les solutions de systèmes polynomiaux dans $\mathbb{K}[x_1, \ldots, x_n]$, de dimension zéro, dont l'ensemble des solutions dans $\overline{\mathbb{K}}^n$ est noté V, par la donnée de $(q, v_1, \ldots, v_n)$ dans $\mathbb{K}[y]$ (où y sera une nouvelle variable) via la paramétrisations rationnelle

$$V = \left\{ \left(\frac{v_1(\tau)}{q'(\tau)}, \ldots, \frac{v_n(\tau)}{q'(\tau)} \right) \in \overline{\mathbb{K}}^n \mid q(\tau) = 0 \right\}$$

où q est sans facteur carré, les v_i de degrés inférieurs à celui de q et q' est la dérivée de q par rapport à y.

On peut remarquer ici que la cardinalité δ de V coincide avec le degré de V. Ainsi une telle représentation est de *taille* $(n+1)\delta$ (ici la taille est simplement le nombre de coefficients dans $\mathbb{K}$ dont on a besoin pour stocker ces polynômes dans la base monomiale standard).

Le théorème de Bézout (voir par exemple [30]) permet de borner δ par le produit des degrés des polynômes du système de départ définissant V. Si D est le maximum de ces degrés on a donc $\delta \leq D^n$ et ce majorant est atteint lorsque les polynômes de départ sont choisis *génériquement* (c'est-à-dire que les coefficients des systèmes polynomiaux qui ne satisfont pas cette propriété annulent une équation polynomiale non triviale).

Dans cette thèse, nous portons notre attention sur des *familles* de systèmes polynomiaux particulièrement structurées et qui interviennent dans diverses applications, notamment celles de l'optimisation polynomiale, ou en robotique. Dans ces contextes, il est fréquent de vouloir identifier des *singularités* qui sont définies par une chute de rang dans une matrice à entrées polynomiales et d'éventuelles autres équations polynomiales.

Ainsi, sous des hypothèses de régularité (satisfaites génériquement), les points critiques d'une application polynomiale $\boldsymbol{x} \to \phi(\boldsymbol{x})$ restreintes à une variété définie par l'annulation simultanée de polynômes $\boldsymbol{G} = (g_1, \ldots, g_s)$ sont définies par une chute de rang dans la

jacobienne $\boldsymbol{F}$, de taille $(s+1, n)$ associée à $\boldsymbol{G}, \phi$ et bien sûr l'annulation simultanée des entrées de $\boldsymbol{G}$.

Ce type structure a un impact sur la valeur de δ et, dans ce cas précis, la borne de Bézout précédemment mentionnée n'est pas atteinte.

On s'intéresse donc en premier lieu au problème algorithmique suivant.

Problème. *Soit $\boldsymbol{G} = (g_1, \ldots, g_s)$ une suite finie de polynômes et $\boldsymbol{F}$ une matrice de taille $p \times q$ (avec $p \leq q$) dont les entrées sont aussi des polynômes, tous ces polynômes appartenant à $\mathbb{K}[x_1, \ldots, x_n]$ et tels que $n = q - p + s + 1$. Calculer les points isolés de l'ensemble des points de $\overline{\mathbb{K}}^n$ qui annulent simultanément les entrées de $\boldsymbol{G}$ et en lesquels le rang de $\boldsymbol{F}$ chute.*

Nous considérerons plusieurs variantes de ce problème, notamment celles où les entrées de $\boldsymbol{G}$ et $\boldsymbol{F}$ sont creuses ou bien bénéficient de propriétés d'invariance par action du groupe symétrique.

2.2 Méthodes pour la résolution de systèmes polynomiaux

La résolution effective de systèmes polynomiaux est étudiée depuis maintenant de nombreuses années et diverses méthodes ont été conçues pour apporter des solutions algorithmiques efficaces qui ont chacune leurs spécificités.

Dans cette section, nous faisons un tour d'horizon, non exhaustif, des méthodes de résolution des systèmes polynomiaux sur lesquelles nous nous appuyons dans cette thèse.

Homotopies. Ces méthodes s'appuient sur l'idée fondamentale suivante. On cherche à "résoudre" (c'est-à-dire calculer les points isolés) d'un système d'équations polynomiales donné $a_1 = \cdots = a_N = 0$ dans $\mathbb{K}[x_1, \ldots, x_n]$. Pour cela, on tente d'identifier un système d'équations polynomiales $b_1 = \cdots = b_N = 0$ dont on connaît *a priori* (souvent par construction) les solutions dans $\overline{\mathbb{K}}^n$ et on attend que l'ensemble des solutions de ce dernier soit de cardinalité supérieure ou égale au nombre de points isolés de notre système de départ. On construit alors le système définissant une *courbe d'homotopie*

$$ta_1 + (1-t)b_1 = \cdots = ta_N + (1-t)b_N = 0$$

où t est une nouvelle variable. Il s'agit alors de *suivre* les solutions du système $b_1 = \cdots = b_N = 0$ en faisant varier le paramètre d'homotopie de 0 à 1.

Le système $a_1 = \cdots = a_N = 0$ est parfois appelé "système cible" et le système $b_1 = \cdots = b_N = 0$ est lui parfois appelé "système source".

Cette idée facile à énoncer trouve des déclinaisons tant numériques que symboliques et leur mise en œuvre nécessite de résoudre plusieurs problèmes intermédiaires ; nous en mentionnons quelques-unes ci-dessous :

- comment construire le système dont on connaît les solutions?
- comment garantir qu'il suffit de suivre les solutions à $t = 0$ pour récupérer celles correspondant à $t = 1$?
- comment garantir le comportement numérique du suivi des solutions de $t = 0$ à $t = 1$?
- comment faire ce suivi de solutions dans le contexte du calcul formel?

La littérature concernant les méthodes d'homotopie tant numériques que symboliques est riche (voir par exemples [4, 25, 33, 96, 129, 126, 165, 139]) et apporte des solutions à ces questions dans bien des cas mais pas dans le contexte déterminantiel évoqué ci-dessus.

Dans cette thèse, nous donnons en Section 3.7 une réponse précise et rigoureuse à la première question et développons principalement des algorithmes d'homotopie symboliques pour résoudre les problèmes déterminantiels décrits dans le paragraphe précédent.

Résolution géométrique. Si le cœur méthodologique de cette thèse se situe dans la conception d'homotopies adaptées au contexte déterminantiel, nous utiliserons quand même, dans certaines situations, et en interne dans nos algorithme, l'algorithme de résolution géométrique pour résoudre des systèmes polynomiaux intermédiaires dont l'union des solutions constituera l'ensemble des solutions du problème déterminantiel source.

Cet algorithme de résolution géométrique trouve ses origines dans [86, 84, 85] et est décrit dans [123, 87, 124]. Étant donné un système $a_1 = \cdots = a_N = 0$ dans $\mathbb{K}[x_1, \ldots, x_n]$, il procède incrémentalement en calculant les solutions de l'intersection de $n - i$ hyperplans génériques $H_1, \ldots, H_{n-i}$ avec l'ensemble V_i des solutions dy système $a_1 = \cdots = a_i = 0$. Ces solutions sont encodées par une paramétrisation rationnelle. À partir de ces solutions, on utilise un itérateur de Newton symbolique (communément appelé remontée de Hensel en calcul formel) pour obtenir un développement série définissant les voisinages de ces points sur la courbe, dite courbe de remontée, définie par l'intersection de V_i avec les hyperplans $H_1, \ldots, H_{n-i-1}$. Une étape de reconstruction rationnelle permet ensuite d'obtenir une paramétrisation rationnelle de cette courbe (qui est valable globalement, hormis certains points exceptionnels de la courbe). On continue le process de résolution en calculant une paramétrisation de l'intersection cette courbe de remontée avec l'hypersurface définie par $a_{i+1} = 0$, et ainsi de suite. Cette dernière étape d'intersection se ramène à la résolution de systèmes bivariés.

En plus de n et N, les deux paramètres qui interviennent dans l'analyse de complexité de cet algorithme sont :

- la complexité d'évaluation L du système de départ lorsqu'il est donné par un programme d'évaluation (sans boucles ni division de polynômes);
- le maximum δ des degrés des variétés algébriques V_i pour $1 \leq i \leq N$.

Au final, l'algorithme de résolution géométrique de [87] est linéaire en L, polynomial en n et N et quadratique en δ (à des facteurs logarithmiques près).

Dans nos algorithmes d'homotopies symboliques dédiées aux structures déterminantielles, on s'appuiera sur des remontées de Hensel similaires à celles évoquées plus haut pour calculer une paramétrisation rationnelle de courbes d'homotopie.

Comme déjà évoqué, on utilisera aussi directement l'algorithme de résolution géométrique pour résoudre des systèmes dont l'union de l'ensemble des solutions forme l'ensemble des solutions de problèmes déterminantiels sources.

Bases de Gröbner. Obtenir des implantations efficaces des algorithmes précédemment évoqués est un problème en soi car il faut pour cela pouvoir s'appuyer sur des bibliothèques particulièrement optimisées pour l'arithmétique polynomiale et capables de manipuler efficacement des programmes d'évaluation. Même si des progrès récents ont été effectués, dans cette thèse on validera certains de nos résultats de complexité (notamment concernant les problèmes invariants par symétries) en remplaçant les calculs de résolutions géométriques et d'homotopies symboliques par des calculs de *bases de Gröbner*.

Les bases de Gröbner et l'algorithme de Buchberger sont introduits dans [36]. Il s'agit d'un object fondamental permettant de définir une forme normale dans l'anneau des polynômes $\mathbb{K}[x_1, \ldots, x_n]$ quotienté par l'idéal engendré par les équations considérées et ainsi résoudre le problème d'appartenance aux idéaux polynomiaux.

Ces bases de Gröbner sont calculées en fonction d'ordres monomiaux admissibles qui permettent définir une division polynomiale multivariée. Les bases de Gröbner d'idéaux de dimension zéro calculées pour l'ordre lexicographique sur les variables, sous réserve que celles-ci soient en position générique et que l'idéal soit radical, sont dites en position *shape lemma*, c'est-à-dire que les coordonnées des solutions sont polynomialement paramétrées par la dernière variable pour l'ordre lexicographique. Cette sortie est ainsi très similaire aux paramétrisations rationnelles qu'on cherche à calculer.

Les algorithmes F_4 et F_5 dus à J.-C. Faugère [58, 59] ont sensiblement amélioré les calculs de bases de Gröbner en pratique. Ils s'appuient sur des réductions à des opérations d'algèbre linéaire efficaces. Divers logiciels implantent ces algorithmes efficacement et nous les utilisons pour valider expérimentalement les résultats obtenus sur les problèmes déterminantiels invariants par action du groupe symétrique.

2.3 Contributions

Dans la suite on considère s polynômes $\boldsymbol{G} = (g_1, \ldots, g_s)$ dans $\mathbb{K}[x_1, \ldots, x_n]$ et une matrice $\boldsymbol{F}$ dans $\mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ avec $p \leq q$ et $n = q - p + s + 1$. L'ensemble des points de $\overline{\mathbb{K}}^n$, où les polynômes de $\boldsymbol{G}$ s'annulent et où la matrice $\boldsymbol{F}$ n'est pas de rang maximal est noté $V_p(\boldsymbol{F}, \boldsymbol{G})$. On fera l'hypothèse naturelle que $n = q - p + s + 1$.

Un test de dimension locale

Remarquons que $V_p(\boldsymbol{F}, \boldsymbol{G})$ coincide avec l'ensemble algébrique $V(\boldsymbol{C})$ avec $\boldsymbol{C} = (c_1, \ldots, c_s, c_{s+1}, \ldots, c_m)$ dans $\mathbb{K}[x_1, \ldots, x_n]$, avec $m = s + \binom{q}{p}$, $(c_1, \ldots, c_s) = \boldsymbol{G}$ et $(c_{s+1}, \ldots, c_m)$ est la suite des p-mineurs de $\boldsymbol{F}$.

Notre première contribution est un algorithme qui prend en entrée une suite de polynômes $\boldsymbol{C} = (c_1, \ldots, c_m)$ et un point $\boldsymbol{x} \in \overline{\mathbb{K}}^n$ dans $V(\boldsymbol{C})$, et qui décide si $\boldsymbol{x}$ est un point isolé dans $V(\boldsymbol{C})$.

Nous montrons que si on connaît une borne μ sur la multiplicité de $\boldsymbol{x}$ en tant que racine de $\boldsymbol{C}$, on peut décider si $\boldsymbol{x}$ est isolé dans $V(\boldsymbol{C})$ en temps polynomial en μ, le nombre d'équations m, le nombre de variables n, et la complexité d'évaluation de $\boldsymbol{C}$. Ce résultat est décrit plus précisément dans Section 5.1, Chapter 5.

Algorithmes d'homotopies déterminantielles

Sous l'hypothèse d'avoir une déformation convenable pour mettre en œuvre une homotopie, on donne un algorithme qui prend en entrée $\boldsymbol{C} = (c_1, \ldots, c_m)$ et qui calcule une paramétrisation rationnelle des points isolés de $V(\boldsymbol{C})$. Cet algorithme s'appuie sur le test de dimension locale évoqué ci-dessus.

Sa complexité dépend linéairement de la complexité d'évaluation de $\boldsymbol{C}$, polynomialement de la somme des multiplicités des points isolés de $V(\boldsymbol{C})$ et du degré de la courbe d'homotopie. Ceci est décrit dans la Section 5.2, Chapter 5.

Nous montrons ensuite comment appliquer cet algorithme dans le contexte des systèmes déterminantiels.

Variétés déterminantielles

Bornes sur le nombre de points isolés dans $V_p(\boldsymbol{F}, \boldsymbol{G})$**.** Nous prouvons que la somme des multiplicités des points isolés de $V_p(\boldsymbol{F}, \boldsymbol{G})$ est au plus $\min(c, c')$, avec

$$c = \deg(g_1) \cdots \deg(g_s) \cdot \eta_{n-s}(\mathrm{cdeg}(\boldsymbol{F}, 1), \ldots, \mathrm{cdeg}(\boldsymbol{F}, q))$$

et

$$c' = \deg(g_1) \cdots \deg(g_s) \cdot h_{n-s}(\mathrm{rdeg}(\boldsymbol{F}, 1), \ldots, \mathrm{rdeg}(\boldsymbol{F}, p)),$$

où $\eta_k(\cdot)$ est la k-ème fonction symmétrique élémentaire et $h_k(\cdot)$ est la k-ème fonction symmétrique complète. Ce résultat est présenté dans le Chapter 6.

Calcul des points isolés/simples de $V_p(\boldsymbol{F}, \boldsymbol{G})$**.** On donne des algorithmes qui prennent en entrée un programme d'évaluation pour $\boldsymbol{G}$ et $\boldsymbol{F}$ et calculent les points isolés/simples de $V_p(\boldsymbol{F}, \boldsymbol{G})$. Leurs complexités sont linéaires en la longueur du programme d'évaluation et polynomiales en la somme des multiplicités des points isolés de $V_p(\boldsymbol{F}, \boldsymbol{G})$ (bornée par $\min(c, c')$) et le degré de la courbe d'homotopie $\min(e, e')$, avec

$$e = (\deg(g_1) + 1) \cdots (\deg(g_s) + 1) \cdot \eta_{n-s}(\operatorname{cdeg}(\boldsymbol{F}, 1) + 1, \ldots, \operatorname{cdeg}(\boldsymbol{F}, q) + 1)$$

et

$$e' = (\deg(g_1) + 1) \cdots (\deg(g_s) + 1) \cdot \eta_{n-s}(\operatorname{rdeg}(\boldsymbol{F}, 1) + 1, \ldots, \operatorname{rdeg}(\boldsymbol{F}, q) + 1).$$

Variétés déterminantielles définies par des polynômes creux et applications aux anneaux de polynômes pondérés

Nous montrons ensuite comment adapter les résultats précédents aux situations où les polynômes donnés en entrée sont creux.

Comme précédemment nous donnons d'abord une borne sur la somme des multiplicités des zéros isolés de $V_p(\boldsymbol{F}, \boldsymbol{G})$ puis un algorithme dédié pour calculer ces points. Cette borne et la complexité de cet algorithme dépendent de volumes mixtes de systèmes constitués d'entrées de $\boldsymbol{F}$ et des entrées de $\boldsymbol{G}$.

Ces résultats sont ensuite spécialisés aux systèmes dits pondérés. On se donne $\boldsymbol{w} = (w_1, \ldots, w_n)$ des enties positifs et on note $\mathbb{K}[x_1, \ldots, x_n]_{\boldsymbol{w}}$ l'anneau des polynômes en les variables $x_1, \ldots, x_n$ qui sont pondérées par $\boldsymbol{w}$. On considère maintenant que les entrées de $\boldsymbol{G}$ et $\boldsymbol{F}$ vivent dans $\mathbb{K}[x_1, \ldots, x_n]_{\boldsymbol{w}}$.

Dans ce cas, on montre que la somme des multiplicités des points isolés de $V_p(\boldsymbol{F}, \boldsymbol{G})$ est bornée par

$$\frac{1}{w_1 \cdots w_n} \cdot \operatorname{wdeg}(g_1) \cdots \operatorname{wdeg}(g_s) \cdot \eta_{n-s}(\operatorname{wcdeg}(\boldsymbol{F}, 1) \cdots, \operatorname{wcdeg}(\boldsymbol{F}, q)),$$

où pour $1 \leq k \leq q$, $\operatorname{wcdeg}(\boldsymbol{F}, k) = \max_{1 \leq k \leq q}(\operatorname{wdeg}(f_{i,k}))$ est le degré pondéré de la k-ème colonne de $\boldsymbol{F}$.

En appliquant nos résultats sur les systèmes creux à ce contexte nous obtenons un algorithme pour calculer ces points dont la complexité est bénéficie d'une accélération de l'ordre du produit des poids.

Systèmes déterminantiels invariants

On considère maintenant le problème de calculer les points critiques de l'application $\boldsymbol{x} \to \phi(\boldsymbol{x})$ (où ϕ est un polynôme) restreinte à la variété $V(\boldsymbol{G})$ dans le cas où ϕ est les entrées de $\boldsymbol{G}$ sont $\mathcal{S}_n$-invariants. On note cet ensemble de points critiques $W(\phi, \boldsymbol{G})$.

On montre comment, en ne calculant qu'un point par orbite, on peut ramener ce problème à la résolution de systèmes déterminantiels dans le contexte pondéré. Ici notre système de poids naturel devient $(1, \ldots, n)$ et on montre que l'algorithme obtenu a une complexité polynomiale en d^s, $\binom{n+d}{d}$, $\binom{n}{s+1}$.

2.4 Organisation de la thèse

Cette thèse est structurée en deux parties. La partie I (qui contient les chapitres 4 à 7) décrit nos résultats sur les systèmes déterminantiels. La partie II (qui contient les chapitresr 8 à 10) décrit nos résultats sur les systèmes déterminantiels invariants par action du groupe symétrique.

Plus précisément, les contenus des chapitres s'articulent comme suit.

- Le Chapitre 3 constitue un rappel des notions préliminaires d'algèbre commutative, de géométrie algébrique qui seront utilisées dans la thèse. Nous rappelons également quelques notions élémentaires liées au modèle de complexité et aux structures de données que nous utilisons et nous introduisons les idées de base sur lesquelles s'appuient les méthodes d'homotopies symboliques.

- Au Chapitre 4, nous définissons avec précision les problèmes algorithmiques portant sur les variétés déterminantielles que nous résolvons dans cette thèse. Ceci nous permet de proposer un survol des résultats obtenus et une grille de lecture des chapitres qui suivent.

- Le Chapitre 5 décrit un algorithme qui permet de décider si un point d'une variété algébrique est isolé dans cette variété étant données quelques informations supplémentaires comme une borne sur la somme des multiplicités des points isolés de cette variété. Cet algorithme est ensuite utilisé dans un algorithme d'homotopie général (qui pré-suppose la connaissance d'un système de départ adéquat) que nous décrivons.

- Au Chapitre 6, nous montrons comment instantier cet algorithme d'homotopie général pour résoudre nos problèmes déterminantiels. Nous utilisons deux mesures de degré sur la matrice donnée en entrée : d'une part le degré par colonnes (qui n'est autre que le maximum des degrés par colonne) et d'autre par le degré par lignes (qui est le maximum des degrés par ligne). Pour chacune de ces mesures, nous donnons un algorithme d'homotopie déterminantielle dédié.

- Au Chapitre 7, nous montrons comment utiliser et adapter ces algorithmes d'homotopie pour le cas du degré par colonnes lorsque les polynômes de notre problème sont creux ou quasi-homogènes.
- Au Chapitre 8, on décrit dans le détail les problèmes algorithmiques considérés pour le cas des systèmes déterminantiels invariants par l'action du groupe symétrique.
- Le Chapitre 9 décrit les notions préliminaires permettant de décrire les orbites des solutions des problèmes de calculs de points critiques invariants par action du groupe symétrique. Nous donnons ensuite un algorithme qui prend en entrée les données de notre problème de calcul de points critiques ainsi qu'une caractérisation des orbites qu'on cherche à calculer en termes de partitions d'entiers, et qui renvoie un système algébrique encodant les solutions de l'orbite cible.
- Au Chapitre 10, nous montrons comment calculer une structure de données qui décrit les points où les polynômes symétriques $\boldsymbol{G}$ s'annulent, et où la matrice jacobienne $\mathrm{Jac}(\boldsymbol{G}, \phi)$ associée à $\boldsymbol{G}$ et au polynôme symétrique phi n'a pas rang plein.
- Le Chapitre 11 conclut cette thèse en résumant les résultats obtenus et proposant quelques perspectives de recherche.

Les résultats obtenus font l'objet des trois articles ci-dessous :

- **Solving determinantal systems using homotopy techniques.** Jon D. Hauenstein, Mohab Safey El Din, Éric Schost, et Thi Xuan Vu, accepté au Journal of Symbolic Computation.

  Cet article contient les résultats des chapitres 5 et 6.
- **Homotopy techniques for solving sparse column support determinantal polynomial systems.** George Labahn, Mohab Safey El Din, Éric Schost, and Thi Xuan Vu, soumis au Journal of Complexity.

  Cet article contient les résultats du Chapitre 7.
- **Computing critical points for invariant algebraic systems.** Jean-Charles Faugère, George Labahn, Mohab Safey El Din, Éric Schost, and Thi Xuan Vu, soumis au SIAM Journal on Applied Algebra and Geometry.

  Cet article contient les résultats des chapitres 9 et 10:

Chapter 3

Preliminaries

Throughout this thesis we let $\boldsymbol{X}$ denote the set of variables $(x_1, \ldots, x_n)$.

3.1 Commutative algebra and algebraic geometry

In this section, we recall some standard notions and notations of commutative algebra and algebraic geometry. We refer the reader to the books [135, 53, 46] for more detailed descriptions.

3.1.1 Ideals

A nonempty subset I of a ring R is called an *ideal* if $0_R \in I$ and for all x, y in I and $r \in R$, $x + y \in I$ and $rx \in I$. Let R be a commutative ring with identity and S be a subset of R. The *ideal generated* by S is the subset

$$\langle S \rangle = \{r_1 s_1 + \cdots + r_k s_k \,:\, r_1, \ldots r_k \in R, s_1, \ldots, s_k \in S, k \in \mathbb{N}\}.$$

If S has a single element s, this is called the *principal ideal generated* by s. An ideal I in a commutative ring R is said to be

- *maximal* if there is no ideal J of R such that $I \subset J \subset R$ with $I \neq J$ and $J \neq R$.
- *prime* if whenever a, b in R and $ab \in I$, then either $a \in I$ or $b \in I$.
- *primary* if $ab \in I$ implies that either $a \in I$ or $b^k \in I$ for some positive integer k.
- *radical* if $a^k \in I$ for any positive integer k implies that $a \in I$.

The *radical* of an ideal I in a commutative ring R, denoted by $\sqrt{I}$, is defined as

$$\sqrt{I} = \{r \in R : r^k \in I \text{ for some } k \in \mathbb{N}\};$$

this set is a radical ideal of R. We have some basic properties as follows: a prime ideal is primary; if I is primary, then $\sqrt{I}$ is prime; if I is prime, then $\sqrt{I} = I$; every maximal ideal of a commutative ring with identity is prime (the converse, however, is not true for example, when $R = \mathbb{Q}[x_1, x_2]$ and $I = \langle x_1 \rangle$).

Let I and J be ideals in a commutative ring R.

- The *sum* of I and J, denoted by $I + J$, is the set $I + J = \{a + b : a \in I \text{ and } b \in J\}$.
- The *product* of I and J, denoted by IJ, is the set $IJ = \{a \cdot b : a \in I \text{ and } b \in J\}$.
- The *intersection* of I and J, denoted by $I \cap J$, is the set $I \cap J = \{a \in R : a \in I, J\}$.
- The *colon* of I and J, denoted by $I : J$, is the ideal $I : J = \{r \in R : r \cdot J \subset I\}$.
- The *saturation* of I and J, denoted by $I : J^\infty$, is the ideal $I : J^\infty = \cup_{n \geq 1}(I : J^n)$.

In general, for ideals I and J of R, the product IJ is contained in $I \cap J$, but does not need to coincide with it. In addition, if I and J are any ideals, then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Let R be a ring. The *Krull dimension* (or simply the dimension) of R, denoted by $\dim(A)$, is the supremum of the lengths r of all strictly decreasing chains $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_r$ of prime ideals of A.

For a prime ideal $\mathfrak{p}$ of R, the *height* or the *codimension* of $\mathfrak{p}$, denoted by $\text{height}(\mathfrak{p})$, is the supremum of the lengths of all strictly decreasing chains of prime ideals

$$\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_r;$$

and the *coheight*, written $\text{coheight}(\mathfrak{p})$, is the supremum of the lengths of all strictly increasing chains of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r$. Then

$$\text{coheight}(\mathfrak{p}) = \dim(R/\mathfrak{p}) \,\text{and}\, \text{height}(\mathfrak{p}) + \text{coheight}(\mathfrak{p}) \leq \dim(R).$$

Note that, in some terminology, $\text{height}(\mathfrak{p})$ is called the *rank* of $\mathfrak{p}$, and $\text{coheight}(\mathfrak{p})$ the dimension of $\mathfrak{p}$.

For a general ideal $I \subset R$, the height of I is defined as the infimum of the heights of prime ideals containing I:

$$\text{height}(I) = \inf\{\text{height}(\mathfrak{p}) : I \subset \mathfrak{p}, \mathfrak{p} \text{ is a prime ideal of } R\}.$$

Since prime ideals in R/I correspond to the prime ideals in R containing I, then

$$\text{coheight}(I) = \dim(R/I).$$

We also have

$$\text{height}(I) + \dim(R/I) \leq \dim(R).$$

For any R-module A, an element in r in R is called a *zero divisor* on A if $ra = 0$ for some non-zero $a \in A$. A commutative ring with identity having no zero divisors is an *integral domain*. If a and b are in a field with $ab = 0$, then if $a \neq 0$, it has an inverse a^{-1}, and so multiplying both sides by a^{-1} gives $b = 0$; in other words, every field is an integral domain.

Theorem 3.1.1. [94, Theorem 18.A] *Let R be an integral domain of finite Krull dimension. For any $\mathfrak{p}$ be a prime ideal of R, we have*

$$\text{height}(\mathfrak{p}) + \dim(R/\mathfrak{p}) = \dim(R).$$

In addition, rings of polynomials are integral domains if the coefficients come from an integral domain. Therefore, if $\mathbb{K}$ is a field, the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ is an integral domain.

3.1.2 Algebraic sets and Zariski topology

A subset $V \subset \overline{\mathbb{K}}^n$ is said to be a $\mathbb{K}$-*algebraic set* (or $\mathbb{K}$-*algebraic variety*) if there exist $\boldsymbol{f} = (f_1, \ldots, f_m)$ in $\mathbb{K}[\boldsymbol{X}]$ such that V is the zero set in $\overline{\mathbb{K}}^n$ of the system $\boldsymbol{f} = 0$, that is,

$$V = V(\boldsymbol{f}) = \{\boldsymbol{a} \in \overline{\mathbb{K}}^n \,:\, \boldsymbol{f}(\boldsymbol{a}) = 0\}.$$

If the algebraic set V is the zero locus of a single polynomial, then V is called a *hypersurface*. When this single polynomial is linear, V is called a *hyperplane*. Sometimes in the thesis, we also write $Z(\boldsymbol{f})$ for the algebraic set defined by $\boldsymbol{f}$.

If V is a subset of $\overline{\mathbb{K}}^n$, we let $\mathcal{I}(V)$ denote the ideal of the polynomials vanishing on all points of V, that is, $\mathcal{I}(V) = \{f \in \mathbb{K}[\boldsymbol{X}] \,:\, f(\boldsymbol{a}) = 0 \text{ for all } \boldsymbol{a} \in V\}$. By Hilbert's Nullstellensatz [45, Theorem 2–Section 1–Chapter 4] we know that $\mathcal{I}(V)$ is a radical ideal.

Proposition 3.1.2. [94, Chapter I] *Algebraic sets have the following properties*

- *$\emptyset$ is an algebraic set;*
- *$\overline{\mathbb{K}}^n$ is an algebraic set;*
- *the intersection of any collection of algebraic sets is an algebraic set;*
- *the union of any finite collection of algebraic sets is an algebraic set.*

Proposition 3.1.2 shows that algebraic varieties have the same properties as the closed sets of a topology on $\overline{\mathbb{K}}^n$.

Definition 3.1.3. *An algebraic set is called a* Zariski closed set. *The complement of a Zariski closed set is a* Zariski open set. *The* Zariski topology *on $\overline{\mathbb{K}}^n$ is the topology whose closed sets are the algebraic varieties. The* Zariski closure *of a set $V \subset \overline{\mathbb{K}}^n$ is the smallest algebraic set containing V. A subset $W \subset V$ of a variety V is* Zariski dense *in V if its closure is V.*

It can be shown, for example, in [45], that the Zariski closure of a set $U \subset \overline{\mathbb{K}}^n$ is $V(\mathcal{I}(U))$, the set of points in $\overline{\mathbb{K}}^n$ where all polynomials that vanish identically on U also vanish.

3.1.3 Generic properties of varieties

In algebraic geometry, there are some properties which hold for most objects of a given type. For example, most square matrices are invertible and most univariate polynomials of degree d have d distinct solutions. We use the term of "generic" to describe such a situation.

Definition 3.1.4. *Let X be a variety. Then a subset $Y \subset X$ is called* generic *if it contains a non-empty Zariski open subset of X. A property is* generic *if the set of points on which that property holds is a generic set.*

Thus a property is said to hold generically for a polynomial system $\boldsymbol{f}$ if there exists a nonzero polynomial in the coefficients of $\boldsymbol{f}$ such that this property holds for all $\boldsymbol{f}$ for which the polynomial does not vanish. Note that the notion of genericity depends on the context, and so care must be exercised in its use.

For example, consider a quadratic polynomial $ax^2 + bx + c$. Generically, the equation $ax^2 + bx + c = 0$ has two solutions in $\overline{\mathbb{K}}$, counted with multiplicity. This property holds when $a \neq 0$. Let $\mathcal{O}$ be a non-empty Zariski open subset of $\overline{\mathbb{K}}$ defined as the complement of the Zariski closed set $V(a)$ in $\overline{\mathbb{K}}$. Then, for any $a \in \mathcal{O}$, the equation $ax^2 + bx + c = 0$ has two solutions in $\overline{\mathbb{K}}$, counted with multiplicity.

On the other hand, generically, the equation $ax^2 + bx + c = 0$ also has two distinct solutions in $\overline{\mathbb{K}}$ with this property holding when $a(b^2 - 4ac) \neq 0$. Therefore, if we define the non-empty Zariski open subset $\mathcal{O}'$ of $\overline{\mathbb{K}}^3$ as the complement of the Zariski closed set $V(a(b^2 - 4ac))$ in $\overline{\mathbb{K}}^3$, that is, $\mathcal{O}' := \overline{\mathbb{K}}^3 \setminus V(a(b^2 - 4ac))$, then for any point (a, b, c) in $\mathcal{O}'$, the equation $ax^2 + bx + c = 0$ has two distinct solutions in $\overline{\mathbb{K}}$.

3.1.4 Irredudant decomposition

A variety V is *irreducible* if it cannot be written as a union of proper subvarieties. That is, if $V = Y \cup Z$ with Y, Z being subvarieties of V, then either $V = Y$ or $V = Z$. A variety V has an *irredundant decomposition* into irreducible subvarieties, $V = V_1 \cup \cdots \cup V_r$, which

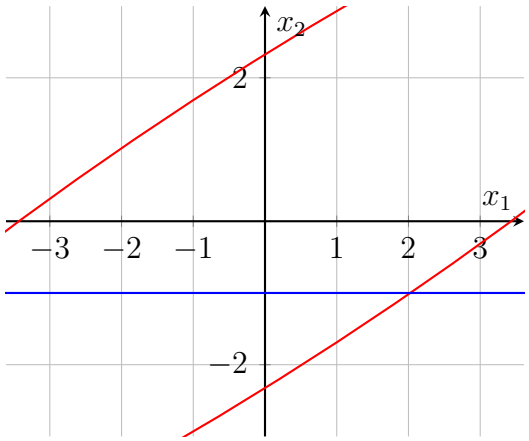


Figure 3.1: Irreducible components of $V(x_1^2x_2 + x_2^3 + x_1^2 + x_2^2 - 4x_2 - 4)$

is unique in that each V_i is an irreducible subvariety of V and if $i \neq j$, then $V_i \not\subset V_j$. We call the subvarieties $V_1, \ldots, V_r$ the *irreducible components* of V.

Theorem 3.1.5. [45, Theorem 4–Section 6–Chapter 4] *Every nonempty variety V can be decomposed as a finite union*

$$V = V_1 \cup \cdots \cup V_r$$

of irreducible varieties, with no V_i being a subset of any V_j when $i \neq j$.

For a hypersurface defined by polynomial f, finding its irredundant decomposition is equivalent to factoring f into irreducible polynomials.

Example 3.1.1. For the curve defined by $V(x_1^2x_2+x_2^3+x_1^2+x_2^2-4x_2-4)$, its components are the circle defined by $x_1^2 + x_2^2 = 4$ and the line $x_2 = -1$ (in Figure 3.1). This follows from

$$x_1^2x_2 + x_2^3 + x_1^2 + x_2^2 - 4x_2 - 4 = (x_1^2 + x_2^2 - 4)(x_2 + 1).$$

Definition 3.1.6. *The* dimension *of an algebraic set V in $\overline{\mathbb{K}}^n$, denoted by $\dim(V)$, is the largest integer d such that there exists $\{i_1, \ldots, i_d\}$ for which the projection of V on $x_{i_1}, \ldots, x_{i_d}$ has nonempty interior. The codimension of V is then defined as $n - \dim(V)$.*

The variety is equidimensional *of dimension d if all its irreducible components have dimension d.*

By convention, the dimension of the empty set is -1. An algebraic set of dimension zero is nonempty and finite.

Note that there are several equivalent definitions for the dimension of an algebraic set. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be the ideal defining the algebraic set $V = V(I) \subset \overline{\mathbb{K}}^n$. Then the dimension of V is the Krull dimension of $\mathbb{K}[x_1, \ldots, x_n]/I$, that is,

$$\dim(V(I)) = \dim(\mathbb{K}[x_1, \ldots, x_n]/I).$$

Furthermore, the dimension of a variety $V \subset \overline{\mathbb{K}}^n$ equals the number of hyperplanes in general position such that the intersection of these hyperplanes with V is a nonzero finite number of points in $\overline{\mathbb{K}}^n$.

Definition 3.1.7. *Let V be an irreducible variety of dimension d. The* degree *of an V is the number of points in the intersection of V with d generic hyperplanes.*

If V is an arbitrary algebraic variety, its degree *is defined as the sum of the degrees of its irreducible components.*

Example 3.1.2. Let V be the curve defined in Example 3.1.1. Then V is equidimensional of dimension 1 since all its irreducible components (a circle and a line) are one-dimensional. The degrees of the circle and the line equal 2 and 1, respectively. So V has degree 3.

3.1.5 Regular, singular, and critical points

Let $V \subset \overline{\mathbb{K}}^n$ and $\mathcal{I}(V) \subset \mathbb{K}[x_1, \ldots, x_n]$ be the ideal associated to V. The *tangent space* to V at $\boldsymbol{x} \in V$ is the vector space $T_{\boldsymbol{x}}V$ defined by the equations

$$\frac{\partial f}{\partial x_1}(\boldsymbol{x})v_1 + \cdots + \frac{\partial f}{\partial x_n}(\boldsymbol{x})v_n = 0,$$

for all f in $\mathcal{I}(V)$. Let $\boldsymbol{f} = (f_1, \ldots, f_m)$ be generators of $\mathcal{I}(V)$. Then, for any polynomial $f \in \mathcal{I}(V)$, there exist polynomials $g_1, \ldots, g_m$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that $f = g_1 f_1 + \cdots + g_m f_m$. The tangent space to V at $\boldsymbol{x} \in V$ is the right kernel of the *Jacobian* matrix associated to polynomials $\boldsymbol{f}$

$$\mathrm{Jac}(\boldsymbol{f}) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_s}{\partial x_1} & \cdots & \frac{\partial f_s}{\partial x_n} \end{bmatrix}$$

evaluated at $\boldsymbol{x}$.

Suppose that V is equidimensional, then a point x in V is called *regular* or *nonsingular* if $\dim(T_{\boldsymbol{x}}V) = \dim(V)$; the *singular points* are those points of V which are not regular. A variety V is nonsingular or *smooth* if it is nonsingular at every point in V.

Lemma 3.1.8 (Jacobian criterion)**.** [53, Theorem 16.19] *Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ be a sequence of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Assume that at any point $\boldsymbol{x}$ of $V(\boldsymbol{f})$, the Jacobian matrix associated to $\boldsymbol{f}$ has rank s. Then the ideal generated by $\boldsymbol{f}$ is radical and the variety $V(\boldsymbol{f})$ is either empty or smooth and equidimensional of codimension s.*

Corollary 3.1.9. *Let V be a d-equidimensional variety and $\boldsymbol{f}$ be a set of generators of the ideal defining a variety V. Then a point $\boldsymbol{x} \in V$ is regular if the rank of the Jacobian matrix* $\mathrm{Jac}(\boldsymbol{f})$ *associated to $\boldsymbol{f}$ at $\boldsymbol{x}$ is $n - d$.*

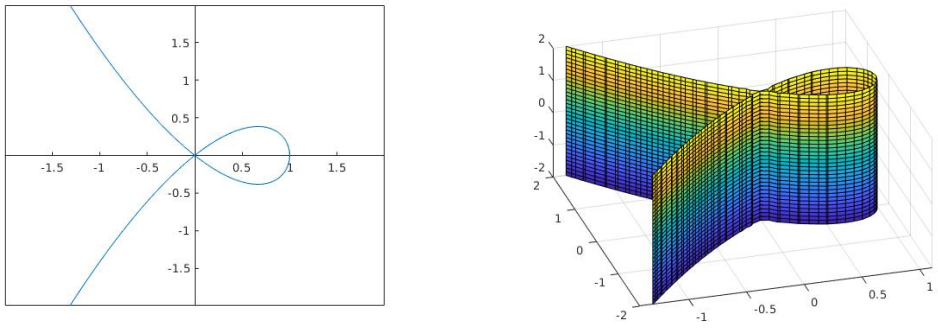
Consequently, the set of singular points of a variety V of dimension d is a closed set; its defining ideal is generated by the vanishing of the polynomials in $\boldsymbol{f}$ and the $(n-d)$-minors of $\mathrm{Jac}(\boldsymbol{f})$.

Example 3.1.3. The variety $V(x_1^3 - x_1^2 + x_2^2) \subset \mathbb{C}^2$ (Figure 3.2(a)) has singularity at the origin. To find all singularities, we need to find common solutions of

$$x_1^3 - x_1^2 + x_2^2 = 3x_1^2 - 2x_1 = 2x_2 = 0 \tag{3.1}$$

with the last two equations being partial derivatives of $x_1^3 - x_1^2 + x_2^2$ with respect to x_1 and x_2. Clearly, only $(0, 0)$ is the solution of (3.1), so $V(x_1^3 - x_1^2 + x_2^2) \subset \mathbb{C}^2$ has only one singular point.

On the other hand, if we see the variety $V(x_1^3 - x_1^2 + x_2^2) \subset \mathbb{C}^3$ (Figure 3.2(b)), we have x_3 is a variable. Then, all points of the form $[0, 0, t]$, with $t \in \mathbb{C}$, are singularities of $V(x_1^3 - x_1^2 + x_2^2) \subset \mathbb{C}^3$.



(a) $V(x_1^3 - x_1^2 + x_2^2) \subset \mathbb{C}^2$ (b) $V(x_1^3 - x_1^2 + x_2^2) \subset \mathbb{C}^3$

Figure 3.2: Singularities

Consider an equidimensional variety $V \subset \overline{\mathbb{K}}^n$. Let φ be a polynomial mapping $V \to \overline{\mathbb{K}}^m$, for some positive integer m. The differential of φ at a regular point $\boldsymbol{x}$ in V is denoted by $d_{\boldsymbol{x}}\varphi$. A regular point x in V is called a *critical point* of the restriction of φ to V if $d_{\boldsymbol{x}}\varphi(T_{\boldsymbol{x}}V) \neq \overline{\mathbb{K}}^m$. In other words, a point $\boldsymbol{x}$ in V is a critical point of the restriction of φ to V if and only if $\boldsymbol{x}$ is nonsingluar and $\dim(d_{\boldsymbol{x}}\varphi(T_{\boldsymbol{x}}V)) < m$. The first condition means the rank the matrix $\mathrm{Jac}(\boldsymbol{f})$ evaluated at $\boldsymbol{x}$ is $n-d$, and then the second one, together with the fact that $T_{\boldsymbol{x}}V$ is the nullspace of $\mathrm{Jac}(\boldsymbol{f})(\boldsymbol{x})$, implies that the matrix $\begin{bmatrix}\mathrm{Jac}(\boldsymbol{f}) \\ \mathrm{Jac}(\varphi)\end{bmatrix}$ has not full rank at $\boldsymbol{x}$. We have the following result.

Lemma 3.1.10. [158, Lemma A.2] *Suppose that V is d-equidimensional. Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ be a set of generators of the ideal defining V. Then the set of critical points of the restriction*

of a polynomial mapping $\varphi : V \to \overline{\mathbb{K}}^m$ *is*

$$\left\{ \boldsymbol{x} \in V \,:\, \operatorname{rank}(\operatorname{Jac}_{\boldsymbol{x}}(\boldsymbol{f})) = n - d \text{ and } \operatorname{rank} \begin{bmatrix} \operatorname{Jac}_{\boldsymbol{x}}(\boldsymbol{f}) \\ \operatorname{Jac}_{\boldsymbol{x}}(\varphi) \end{bmatrix} < n - d + m \right\}.$$

3.1.6 Primary decomposition of ideals

In the view of Theorem 3.1.5 and the ideal-variety correspondence, every radical ideal in $\overline{\mathbb{K}}[x_1, \ldots, x_n]$ can be written uniquely as a finite intersection of prime ideals, $I = P_1 \cap \cdots \cap P_r$, where $P_i \not\subset P_j$ for $i \neq j$. It is not correct that any arbitrary ideal I can be written as an intersection of prime ideals since the intersection of prime ideals is radical. However, we can decompose an ideal into an intersection of primary ideals.

For a primary ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, the radical ideal $\sqrt{I}$ of I is prime and is the smallest ideal in $\mathbb{K}[x_1, \ldots, x_n]$ containing I. If I is primary and $\sqrt{I} = P$, then we say that I is *P-primary* and P is called the *associated prime ideal* of I. A *primary decomposition* of an ideal I is an expression of I as an intersection

$$I = Q_1 \cap \cdots \cap Q_r,$$

where $Q_1, \ldots, Q_r$ are primary ideals; this decomposition is called *minimal* or *irredundant* if $\sqrt{Q_i} \neq \sqrt{Q_k}$ for all $i \neq k$ and then the radicals $P_i = \sqrt{Q_i}$ are then called the associated primes of I.

Theorem 3.1.11. [45, Theorem 7–Section 7–Chapter 4] *Every ideal in* $\mathbb{K}[x_1, \ldots, x_n]$ *has a minimal primary decomposition.*

Example 3.1.4. Let $I = \langle x_1x_2, x_1x_3 \rangle$ be an ideal in $\mathbb{K}[x_1, x_2, x_3]$. The primary decomposition of I is $I = \langle x_1 \rangle \cap \langle x_2, x_3 \rangle$ and $V(I) = \{(0, x_2, x_3) : x_2, x_3 \in \overline{\mathbb{K}}\} \cup \{(x_1, 0, 0) : x_1 \in \overline{\mathbb{K}}\}$.

For the example above, there is a one-to-one correspondence between the primary decomposition of I and the irreducible decomposition of its zero set $V(I)$. In general, unlike the case of varieties or radical ideals, minimal primary decomposition need not be unique. When there are embedded primes, primary decompositions are not unique. The associated primes minimal with respect to inclusion are called the *minimal primes*, the others are called *embedded primes*. Although minimal primary decomposition need not be unique, the associated primes are uniquely determined [6, Theorem 4.5].

Example 3.1.5. Let $I = \langle x_1^2, x_1x_2 \rangle$ be an ideal in $\mathbb{K}[x_1, x_2]$. For each $k \geq 1$, we have different minimal primary decompositions

$$\langle x_1^2, x_1x_2 \rangle = \langle x_1 \rangle \cap \langle x_1^2, x_2 \rangle = \langle x_1 \rangle \cap \langle x_1^2, x_1x_2, x_2^k \rangle.$$

The associated primes of I are $P_1 = \langle x_1 \rangle$ and $P_2 = \langle x_1, x_2 \rangle$; the associated prime P_2 is an embedded prime of I since $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle$.

3.1.7 Localization

Let R be a ring. A subset $S \subset R$ is called *multiplicatively closed* if $1 \in S$ and for all a, b in S implies $ab \in S$. Let S be a multiplicatively closed set of R. We can define an *equivalence relation* $\sim$ on $R \times S$ by $(a, s) \sim (a', s')$ if and only if there is an element $u \in S$ such that $u(as' - a's) = 0$. We denote the equivalence class of a pair $(a, s) \in R \times S$ by $\frac{a}{s}$. The set of all equivalence classes

$$R_S = \left\{ \frac{a}{s} \,:\, a \in R \text{ and } s \in S \right\}$$

is called the *localization* of R at the multiplicatively closed set S. This localization is a ring with addition and multiplication given by

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \text{ and } \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}.$$

All ideals of R_S are of the form IR_S, with I is an ideal of R.

Proposition 3.1.12. [6, Proposition 4.9] *Let S be a multiplicatively closed set of R. Let I be an ideal of R and*

$$I = Q_1 \cap \cdots \cap Q_r$$

be a minimal primary decomposition of I. For any $\ell \leq r$, let $P_1, \ldots, P_\ell$ be minimal primes of I. Then

$$I_S = Q_{1\,S} \cap \cdots \cap Q_{\ell\,S}$$

is a minimal primary decomposition of I_S in R_S, where for $i = 1, \ldots, \ell$, $Q_{i\,S}$ is the localization of Q_i at S. In addition, the minimal primes of I_S are $P_{1\,S}, \ldots, P_{\ell\,S}$.

If $\mathfrak{p}$ is a prime ideal of R, then the set $S = R \setminus \mathfrak{p}$ is multiplicatively closed since $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$ implies $ab \notin \mathfrak{p}$. In this case, the localization R_S which is denoted by $R_\mathfrak{p}$ is called the localization of R at $\mathfrak{p}$. This is in spite of the fact that we actually localize R at $R \setminus \mathfrak{p}$. For a prime ideal $\mathfrak{p}$ of R, the prime ideals in the localization $R_\mathfrak{p}$ are in one-to-one correspondence with the prime ideals of R contained in $\mathfrak{p}$. Therefore,

$$\text{height}(\mathfrak{p}) = \dim(R_\mathfrak{p}).$$

A ring R is called *local* if it has exactly one maximal ideal.

Lemma 3.1.13. *If R is a local ring and I is a proper ideal of R, then R/I is also local.*

Proof. Let us consider the map $\pi : R \to R/I$ given by $\pi(r) = r + I$. This map is a surjective since any coset $r + I$ is the image of R/I. Let $\mathfrak{m}$ be the maximal ideal of R. If R/I has a maximal ideal $\mathfrak{m}' \neq \mathfrak{m}$, then $\pi^{-1}(\mathfrak{m}') \neq \mathfrak{m}$ is a maximal ideal of R, which is a contradiction with the fact that R is a local ring. □

If $\mathfrak{p}$ is a prime ideal of R, the ring $R_\mathfrak{p}$ is local with its maximal ideal being

$$\mathfrak{p}R_\mathfrak{p} = \left\{ \frac{a}{s} \,:\, a \in \mathfrak{p}, s \notin \mathfrak{p} \right\}.$$

3.1.8 Cohen-Macaulay rings

Let R be a ring and let M be an R-module. A sequence of elements $r_1, \ldots, r_s$ in R is called a *regular sequence* on M (or an *M-sequence*) if $(r_1, \ldots, r_s)M \neq M$, and for $i = 1, \ldots, s$, r_i is a non-zero divisor on $M/(r_1, \ldots, r_{i-1})M$.

If $I \subset R$ is an ideal, and M is a finite R-module such that $IM \neq M$, then the *depth* of I on M, denoted by $\operatorname{depth}(I)$, is the length of any maximal M-sequences in I. A ring R such that, for every maximal ideal $\mathfrak{m}$ of R,

$$\operatorname{depth}(\mathfrak{m}) = \operatorname{codim}(\mathfrak{m})$$

is called *Cohen-Macaulay*. The Cohen-Macaulay property passes to polynomial rings.

Proposition 3.1.14. [53, Proposition 18.9] *A ring R is Cohen-Macaulay if and only if the polynomial ring $R[x_1, \ldots, x_n]$ is Cohen-Macaulay.*

The Cohen-Macaulayness also passes to localizations.

Proposition 3.1.15. [53, Proposition 18.8] *A ring R is Cohen-Macaulay if and only if $R_{\mathfrak{p}}$ is Cohen–Macaulay for every prime ideal $\mathfrak{p}$ of R.*

Theorem 3.1.16. [135, Theorem 17.4(i)] *Let R be a Cohen-Macaulay local ring. For a proper ideal I of R, we have*

$$\operatorname{height}(I) + \dim(R/I) = \dim(R).$$

3.2 Determinantal varieties

In this section, we will present an important class of varieties, whose equations take the forms of the minors of a matrix; this is the main subject of the thesis. In what follows, rings are commutative and noetherian.

3.2.1 Determinantal ideals

Let $\boldsymbol{L}$ be a $p \times q$ matrix with entries in a ring R. For a positive integer t with $t \leq p$, a *t-minor* of $\boldsymbol{L}$ is the determinant of some $t \times t$ submatrix of $\boldsymbol{L}$. The ideal $I_t(\boldsymbol{L})$ in R which is generated by all t-minors of $\boldsymbol{L}$ is called the *t-determinantal ideal* of $\boldsymbol{L}$. If we denote by $M_t(\boldsymbol{L})$ the set of all t-minors of $\boldsymbol{L}$, then $I_t(\boldsymbol{L}) = \langle M_t(\boldsymbol{L}) \rangle \subset R$.

If $t = 1$ and $p = 1$, then the codimension of a minimal prime of $I_t(\boldsymbol{L})$ is bounded by q by using Krull's theorem [53, Theorem 10.2]. Macaulay [131] generalized this result to the case $t = p$ arbitrary, giving the bound $q - p + 1$ for the codimension of $V_p(\boldsymbol{L})$. Latter on, Eagon and Northcott [52] give a generalization to the case when both t and p are arbitrary.

Lemma 3.2.1. [52] *Let R be a Cohen-Macaulay ring and $\boldsymbol{L}$ be in $R^{p\times q}$. Then:*

(i) *if $I_p(\boldsymbol{L}) \neq R$, then the height of I is at most $q-p+1$;*

(ii) *if $I_p(\boldsymbol{L})$ has height $q-p+1$, then I is unmixed (all associated primes have height $q-p+1$).*

The following result gives a condition when the ring $R/I_t(\boldsymbol{L})$ is Cohen-Macaulay.

Theorem 3.2.2. [53, Theorem 18.18] *Let R be a Cohen-Macaulay ring. Let $\boldsymbol{L}$ be in $R^{p\times q}$ and t be a positive integer at most p. If the codimension of $I_t(\boldsymbol{L})$ equals $(q-t+1)(p-t+1)$, then $R/I_t(\boldsymbol{L})$ is a Cohen-Macaulay ring.*

For instance, if R is a polynomial ring in pq indeterminates $(x_{i,j})$ and $\boldsymbol{L} = [x_{i,j}]_{1\leq i\leq p, 1\leq j\leq q}$ is a matrix in $R^{p\times q}$, then, for any $t \leq p$, the ring $R/I_t(\boldsymbol{L})$ is Cohen-Macaulay (see e.g. [37]).

3.2.2 Left-hand diagonal block matrices

In what follows, for any ring R and matrix $\boldsymbol{L}$ in $R^{p\times q}$, if S and U are subsequences of $(1,\dots,p)$ and $(1,\dots q)$ respectively, $\boldsymbol{L}_{S,U}$ is the submatrix of $\boldsymbol{L}$ obtained by keeping rows indexed by S and columns indexed by U. Sometimes in the thesis, we also call this the (S,U)-submatrix of $\boldsymbol{L}$. When $R = \mathbb{K}[x_1,\dots,x_n]$, a polynomial ring, the *t-determinantal variety* $V_t(\boldsymbol{L})$ of $\boldsymbol{L}$ in $\overline{\mathbb{K}}^n$ is then defined as $V_t(\boldsymbol{L}) = V(I_t(\boldsymbol{L}))$. It is easy to see that $\boldsymbol{L}$ is not full rank at any point $\boldsymbol{x} \in V_t(\boldsymbol{L})$.

In the next part of the thesis, matrices with the following pattern are used frequently. Consider a matrix

$$\boldsymbol{L} = \begin{bmatrix} \ell_{1,1} & 0 & 0 & \ell_{1,p+1} & \cdots & \ell_{1,q} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ell_{p,p} & \ell_{p,p+1} & \cdots & \ell_{p,q} \end{bmatrix} \in \mathbb{K}[x_1,\dots,x_n]^{p\times q}. \tag{3.2}$$

For $t \leq p$, any polynomial of the form $\ell_{i_1,i_1}\cdots\ell_{i_t,i_t}$ is in $M_t(\boldsymbol{L})$, where $(i_1,\dots,i_t)$ is a subset of $(1,\dots,p)$ of cardinality t. Therefore, for a matrix such as $\boldsymbol{L}$ to be rank-deficient at $\boldsymbol{x} \in \overline{\mathbb{K}}^n$, at least one of $\ell_{1,1},\dots,\ell_{p,p}$ much vanish at $\boldsymbol{x}$.

Lemma 3.2.3. *Let $\boldsymbol{L}$ be a matrix in $\mathbb{K}[x_1,\dots,x_n]^{p\times q}$ of the form as in (3.2). For $\boldsymbol{x} \in V_t(\boldsymbol{L})$, suppose $\ell_{i_1,i_1}(\boldsymbol{x}) = \cdots = \ell_{i_k,i_k}(\boldsymbol{x}) = 0$, for some $k \leq \min(t,n)$, while all other terms are non-zero. Then the $((i_1,\dots,i_k),(p+1,\dots,q))$-submatrix of $\boldsymbol{L}$ has rank less than $t-(p-k)$. In particular, one has $k \geq p-t+1$.*

Proof. Let $(i_{k+1},\dots,i_p)$ be the complement of $(i_1,\dots,i_k)$ in $(1,\dots,p)$. That is $\ell_{i_r,i_r}(\boldsymbol{x}) \neq 0$ for all $r = k+1,\dots,p$. For any subsequence $\boldsymbol{i} = (j_1,\dots,j_{t-(p-k)})$ of $(p+1,\dots,q)$, with

$t > p - k$ (so $k \geq p - t + 1$), the determinant of a submatrix of $\boldsymbol{L}$ with columns indexed by $(i_{k+1}, \ldots, i_p) \cup \boldsymbol{i}$ is a t-minor of $\boldsymbol{L}$. This determinant equals

$$\ell_{i_{k+1},i_{k+1}} \cdots \ell_{i_p,i_p} \cdot m_{\boldsymbol{i}},$$

where $m_{\boldsymbol{i}}$ is a $t - (p - k)$-minor of the submatrix $\boldsymbol{L}_{(i_1,\ldots,i_k),(p+1,\ldots,q)}$ with columns indexed by $\boldsymbol{i}$.

Since $\ell_{i_r,i_r}(\boldsymbol{x}) \neq 0$ for all $r = k+1, \ldots, t$, then $\ell_{i_{k+1},i_{k+1}} \cdots \ell_{i_p,i_p} \cdot m_{\boldsymbol{i}}$ vanishes at $\boldsymbol{x}$ if and only if $m_{\boldsymbol{i}}(\boldsymbol{x}) = 0$. Note also that these $m_{\boldsymbol{i}}$'s polynomials are all $(t - (p - k))$-minors of $\boldsymbol{L}_{(i_1,\ldots,i_k),(p+1,\ldots,q)}$. This gives our claim. □

3.3 Sparse polynomial systems

Consider a system of n polynomials in n variables

$$f_1(\boldsymbol{X}) = \cdots = f_n(\boldsymbol{X}) = 0,$$

where the polynomial f_i has total degree d_i. By Bézout's theorem [30], this system has at most $d_1 \cdots d_n$ isolated solutions, and exactly that number if the polynomials are generic among all polynomials with the given degrees.

Polynomials from applications are not necessarily generic as they often have some additional structure which we would like our count of solutions to reflect. For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$, we denote by $\boldsymbol{X}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Definition 3.3.1. *Laurent polynomials are polynomials represented in the form of finite sum* $f = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \boldsymbol{X}^{\boldsymbol{\alpha}}$ *with the set* $\{\boldsymbol{\alpha} \in \mathbb{Z}^n : c_{\boldsymbol{\alpha}} \neq 0\}$ *being the support* $\mathrm{supp}(f)$ *of* f*. The Newton polytope of* f*, denoted by* $\mathrm{conv}(f)$*, is the convex hull of the support of* f *in* $\mathbb{R}^n$*.*

For a polytope $\mathcal{C}$ in $\mathbb{R}^n$, the Euclidean volume of $\mathcal{C}$ in $\mathbb{R}^n$ is denoted by $\mathrm{vol}_n(\mathcal{C})$. Let then $\mathcal{C}_1, \ldots, \mathcal{C}_n$ be polytopes in $\mathbb{R}^n$ and consider the function

$$\varphi : (\lambda_1, \ldots, \lambda_n) \mapsto \mathrm{vol}_n(\lambda_1 \mathcal{C}_1 + \cdots + \lambda_n \mathcal{C}_n),$$

where

$$\lambda_1 \mathcal{C}_1 + \cdots + \lambda_n \mathcal{C}_n = \left\{ \boldsymbol{a} \in \mathbb{R}^n : \boldsymbol{a} = \sum_{i=1}^{n} \lambda_i \, a_i \text{ with } a_i \in \mathcal{C}_i \right\}$$

is the Minkowski sum of the polytopes. The function φ is a homogeneous polynomial function of degree n in λ_i (see e.g. [46, Proposition 4.9]).

Definition 3.3.2. *The* mixed volume $\mathsf{MV}(\boldsymbol{\mathcal{C}})$ *of polytopes* $\boldsymbol{\mathcal{C}} = (\mathcal{C}_1, \ldots, \mathcal{C}_n)$ *in* $\mathbb{Z}^n$ *is the coefficient of the monomial* $\lambda_1 \ldots \lambda_n$ *in* $\varphi(\lambda_1, \ldots, \lambda_n)$*.*

The following theorem gives a way to compute the mixed volume of a given collection of polytopes in $\mathbb{R}^n$. Efficient calculations of mixed volumes can be found in [47], [127], [171], and [76, 75, 78].

Theorem 3.3.3. [46, Theorem 4.12] *Let $\boldsymbol{\mathcal{C}} = (\mathcal{C}_1, \ldots, \mathcal{C}_n)$ be polytopes in $\mathbb{R}^n$. Then the mixed volume of $\boldsymbol{\mathcal{C}}$ can be computed as*

$$\mathsf{MV}(\boldsymbol{\mathcal{C}}) = \sum_{k=1}^{n} (-1)^{n-k} \sum_{I \subset \{1,\ldots,n\}, |I|=k} \mathrm{vol}_n\Big(\sum_{i \in I} \mathcal{C}_i\Big),$$

where $\sum_{i\in I} \mathcal{C}_i$ is the Minkowski sum of polytopes.

Example 3.3.1. Let $\mathcal{A}_1 = \{(3,1),(1,2),(0,0)\}$ and $\mathcal{A}_2 = \{(4,0),(1,1),(0,0)\}$ in $\mathbb{Z}^2$. A sparse polynomial system with supports $\mathcal{A}_1, \mathcal{A}_2$ is a system defined by polynomials of the following type:

$$f_1(x_1,x_2) = ax_1^3x_2 + bx_1x_2^2 + c \quad \text{and} \quad f_2(x_1,x_2) = dx_1^4 + ex_1x_2 + f, \tag{3.3}$$

with $a, \ldots, f$ are all non-zero in $\mathbb{C}$.

The convex hull of $f_i(x_1,x_2)$ is $\mathcal{C}_i = \mathcal{A}_i$ for $i = 1,2$, and the Minkowski sum of the polytopes $\mathcal{C}_1, \mathcal{C}_2$ is a convex hexagon with vertices $(0,0),(1,2),(2,3),(5,2),(7,1)$ and $(4,0)$. Figure 3.3 plots the polytopes $\mathcal{C}_1$, $\mathcal{C}_2$, and the Minkowski sum of $\mathcal{C}_1$ and $\mathcal{C}_2$.

The Euclidean volume of $\mathcal{C}_1$ (resp. $\mathcal{C}_2$) which is the area of $\mathcal{C}_1$ (resp. $\mathcal{C}_2$) is $5/2$ (resp. 2); in other words, $\mathrm{vol}_2(\mathcal{C}_1) = 5/2$ and $\mathrm{vol}_2(\mathcal{C}_1) = 2$. In addition, the area of the Minkowski sum $\mathcal{C}_1 + \mathcal{C}_2$ of $\mathcal{C}_1$ and $\mathcal{C}_2$ is $25/2$, that is, $\mathrm{vol}_2(\mathcal{C}_1 + \mathcal{C}_2) = 25/2$. Then, using Theorem 3.3.3, one has

$$\mathsf{MV}(\mathcal{C}_1, \mathcal{C}_2) = -\mathrm{vol}_2(\mathcal{C}_1) - \mathrm{vol}_2(\mathcal{C}_2) + \mathrm{vol}_2(\mathcal{C}_1 + \mathcal{C}_2) = 8.$$

3.3.1 Initial forms

Let

$$p = \sum_{\boldsymbol{q}=(q_1,\ldots,q_n)\in S} c_{\boldsymbol{q}}\, x_1^{q_1} \cdots x_n^{q_n}$$

be a Laurent polynomial with support $S = \mathrm{supp}(p)$. The field of definition may be our field $\mathbb{K}$, or, as will also happen below, a rational function field. Let $\boldsymbol{e} = (e_1, \ldots, e_n)$ be non-zero in $\mathbb{Q}^n$ and define

$$m(\boldsymbol{e}, p) = \min(\langle \boldsymbol{e}, \boldsymbol{q}\rangle \,:\, \boldsymbol{q} \in S) \quad \text{and} \quad S_{\boldsymbol{e},p} = \{\boldsymbol{q} \in S \,:\, \langle \boldsymbol{e}, \boldsymbol{q}\rangle = m(\boldsymbol{e}, p)\},$$

where $\langle\ ,\ \rangle$ is the usual dot-product in $\mathbb{R}^n$. Thus, $S_{\boldsymbol{e},p}$ is the intersection of S with its "support hyperplane" in the direction $\boldsymbol{e}$.

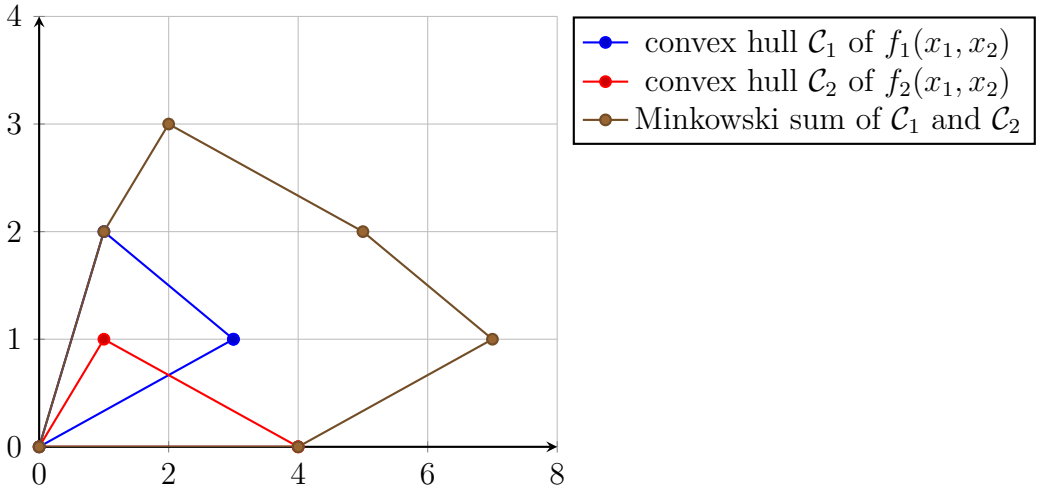


Figure 3.3: Minkowski sum of polytopes

Definition 3.3.4. *The* initial form *of p with respect to $\boldsymbol{e}$ is defined to be*

$$\mathrm{init}_{\boldsymbol{e}}(p) = \sum_{\boldsymbol{q}=(q_1,\ldots,q_n)\in S_{\boldsymbol{e},p}} c_{\boldsymbol{q}}\, x_1^{q_1}\cdots x_n^{q_n}.$$

In other words, $\mathrm{init}_{\boldsymbol{e}}(p)$ is the sum over all terms $c_{\boldsymbol{q}}\, x_1^{q_1}\cdots x_n^{q_n}$ for which the inner product $\langle \boldsymbol{e}, \boldsymbol{q}\rangle$ is minimized. For a vector $\boldsymbol{p} = (p_1, \ldots, p_n)$ of Laurent polynomials, we let

$$\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{p}) = (\mathrm{init}_{\boldsymbol{e}}(p_1), \ldots, \mathrm{init}_{\boldsymbol{e}}(p_n)).$$

Even though there is an infinite number of possible directions $\boldsymbol{e}$, the number of polynomial systems $\{\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{p}) : \boldsymbol{e} \text{ non-zero in } \mathbb{Q}^n\}$ obtained in this manner is finite, since the support of each p_i has finitely many support hyperplanes.

Example 3.3.2. Consider $\boldsymbol{e} = (-1, 1)$ in $\mathbb{Q}^2$. Let $\boldsymbol{f} = (f_1(x_1, x_2), f_2(x_1, x_2))$ be polynomials defined in (3.3). Then

$$m(\boldsymbol{e}, f_1) = -2, S_{\boldsymbol{e},f_1} = \{(3, 0)\};\ \text{and}\ m(\boldsymbol{e}, f_2) = -4, S_{\boldsymbol{e},f_2} = \{(4, 0)\}.$$

So, $\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{f}) = (\mathrm{init}_{\boldsymbol{e}}(f_1), \mathrm{init}_{\boldsymbol{e}}(f_2)) = (ax_1^3x_2, dx_1^4)$.

3.3.2 The BKK Theorem

Let $\boldsymbol{f} = (f_1, \ldots, f_n)$ with each $f_i \in \mathbb{K}[\boldsymbol{X}]$ with support $\mathcal{A}_i$ and associated convex hull $\mathcal{C}_i$. The following well-known relates the number of isolated solutions of a sparse polynomial system with the mixed volume. It is commonly refer to as the BKK bound (Bernstein, Khovanskii, and Kushnirenko). A geometric interpretation is given in [73] and [82] and a more refined version can be found in [152].

Theorem 3.3.5. [27, 121, 117, 46] *Let $\boldsymbol{f} = (f_1, \ldots, f_n)$ be a sequence of sparse polynomials in $\mathbb{K}[\boldsymbol{X}]$ with supports $\mathcal{A}_1, \ldots, \mathcal{A}_n$. Then the number of isolated nonzero solutions of $V(\boldsymbol{f})$ is bounded by $\mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_n)$ where each $\mathcal{C}_i$ is the convex hull of $\mathcal{A}_i$. The bound is tight for a generic polynomial system.*

Example 3.3.3. Let $f_1(x_1, x_2)$ and $f_2(x_1, x_2)$ be polynomials in (3.3). From Example 3.3.1, we have the mixed volume of the convex hulls of $f_1(x_1, x_2)$ and $f_2(x_1, x_2)$ is 8 which agrees with the number of solutions of the system $f_1(x_1, x_2) = f_2(x_1, x_2) = 0$ for generic choices of the coefficients.

The BKK theorem asserts that the system $f_1 = \cdots = f_n = 0$ has at most $\mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_n)$ isolated solutions in $\overline{\mathbb{K}}^n - \{\mathbf{0}\}$, with equality for generic choices of coefficients of $f_1, \ldots, f_n$. If the condition $\mathbf{0} \in \mathcal{C}_i$ holds for $1 \leq i \leq n$, then $\mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_n)$ bounds the number of solutions in $\overline{\mathbb{K}}^n$ (see e.g. [128, Theorem 2.4] and also in [56, 105, 151, 152, 153]).

Theorem 3.3.6. *The mixed volume $\mathsf{MV}(\mathcal{C}_1 \cup \{\mathbf{0}\}, \ldots, \mathcal{C}_n \cup \{\mathbf{0}\})$ is an upper bound for the number of isolated zeroes, counting multiplicities, of the system $f_1 = \cdots = f_n = 0$ in $\overline{\mathbb{K}}^n$.*

We conclude this section with some remarks on how the BKK bound plays a critical role in polynomial system solving. Recall that for system (3.3), Bézout's theorem gives an upper bound of 16 for the number of isolated solutions, while the BKK bound of 8 is smaller and gives the exact number generically. To compute all solutions of (3.3) (or polynomial systems, in general), the better bound is useful information, since one has to find 8 solutions and so no more, which is important when we want to use homotopy continuation methods. We will discuss this in more details in Section 3.7.

3.4 Weighted polynomial domains

Let $\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{N}^n$ be a sequence of integers. We consider polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ where each variable x_k has weight $w_k \geq 1$ (denoted by $\mathrm{wdeg}(x_k) = w_k$).

The *weighted degree* of a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is $w_1\alpha_1 + \cdots + w_n\alpha_n$, and the *weighted degree* of a polynomial, denoted by wdeg, is the maximum of the weighted degree of its terms with non-zero coefficients. For a polynomial g, the *leading weighted homogeneous component* of g, denoted by $lw(g)$, is the sum of terms which have weighted degrees equal the weighted degree of g.

Note that weighted polynomial domains are particular cases of sparse polynomial rings. For example, consider a polynomial ring $\mathbb{K}[x_1, x_2, x_3]$ with $\mathrm{wdeg}(x_k) = k$. The polynomial

$$g = 3x_1^3 + x_1x_2 + 5x_3 + 97x_1^2 - 10x_2 + 2x_1 + 1$$

in $\mathbb{K}[x_1, x_2, x_3]$ which has weighted degree 3 with $lw(g) = 3x_1^3 + x_1x_2 + 5x_3$ is a sparse polynomial supported by

$$\mathcal{A} = (3,0,0), (1,1,0), (0,0,1), (2,0,0), (0,1,0), (1,0,0), (0,0,0).$$

3.4.1 Weighted Bézout Theorem

Bézout's theorem bounds the number of isolated solutions to polynomial systems of equations by the product of their degrees. With polynomial systems lying in a weighted polynomial domain, one obtains better bounds by using the weighted Bézout theorem (see e.g. [108]). Similar to the discussion at the end of Subsection 3.3.2, this is important information in polynomial system solving.

Theorem 3.4.1. [108] *Let $\mathbb{K}[x_1, \ldots, x_n]$ be a polynomial ring of weights $(w_1, \ldots, w_n)$. Let $\boldsymbol{f} = (f_1, \ldots, f_n)$ be a sequence of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Then the number of isolated points of $V(\boldsymbol{f}) \subset \overline{\mathbb{K}}^n$ is bounded by*

$$\frac{\operatorname{wdeg}(f_1) \cdots \operatorname{wdeg}(f_n)}{w_1 \cdots w_n}.$$

This bound is exact if and only if the system $(lw(f_1), \ldots, lw(f_n))$ have no common solution other than $(0, \ldots, 0)$.

3.4.2 Combinatorics of monomials

Counting the number of monomials in the total degree case is a classic combinatorial problem. Let n, d be positive integers. The number of monomials in n variables having total degree d is $N_{n,d} = \binom{n+d-1}{d}$. The number of monomials in n variables having total degree at most d is $N_{n,\leq d} = \binom{n+d}{d}$. In the more general case, this number is called a denumerant.

Definition 3.4.2. *Let $\boldsymbol{w} = (w_1, \ldots, w_n)$ be a sequence of integers in $\mathbb{N}$. The* denumerant *$N_{\boldsymbol{w},d}$ is the number of non-negative integer solutions $(\alpha_1, \ldots, \alpha_n)$ to the equation*

$$w_1\alpha_1 + \cdots + w_n\alpha_n = d.$$

We define $N_{\boldsymbol{w},\leq d} = \sum_{k=0}^{d} N_{\boldsymbol{w},k}$.

The formulas given in [42, Section 2.6] express the denumerants for some specific weights. However, in general, there is no known formula to express $N_{\boldsymbol{w},d}$ as a function of $\boldsymbol{w}$ and d. The asymptotic behavior of these denumerants is well-known.

Proposition 3.4.3. [70, Proposition IV.2] *If $\boldsymbol{w}$ is fixed and d goes to infinity, then*

$$N_{\boldsymbol{w},d} = \frac{\gcd(w_1, \ldots, w_n)}{w_1 \cdots w_n} N_{n,d},$$

where $\gcd(w_1, \ldots, w_n)$ denotes the greatest common divisor of the integers $(w_1, \ldots, w_n)$.

In addition, results in [1, Theorem 3.4], [3] and [177, Theorem 1.1] give upper bounds for $N_{\boldsymbol{w},d}$ and $N_{\boldsymbol{w},\leq d}$.

Proposition 3.4.4. [1, 3, 177] *We have the following bounds:*

- $N_{\boldsymbol{w},d} \leq \frac{\gcd(w_1,\ldots,w_n)}{w_1\cdots w_n} N_{n,d+\delta-n+1}$, *where* $\delta = \sum_{i=2}^{n} w_i \frac{\gcd(w_1,\ldots,w_i)}{\gcd(w_1,\ldots,w_{i-1})}$;
- $N_{\boldsymbol{w},\leq d} \leq \frac{(d+w_1+\cdots+w_n)^n}{n!w_1\cdots w_n}$;
- *If* $n \geq 3$, *then* $N_{\boldsymbol{w},\leq d} \leq \frac{(d-w_1)\cdots(d-w_n)}{n!w_1\cdots w_n}$.

3.5 The ring of symmetric polynomials

Consider the ring $\mathbb{K}[\boldsymbol{X}]$ of polynomials in n variables $\boldsymbol{X} = (x_1, \ldots, x_n)$. The symmetric group $\mathcal{S}_n$ acts on this ring by permuting the variables. That is, for any $\sigma \in \mathcal{S}_n$ and $f \in \mathbb{K}[\boldsymbol{X}]$, $\sigma(f(\boldsymbol{X})) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

Definition 3.5.1. *A polynomial is* symmetric (*or* $\mathcal{S}_n$-invariant) *if it is invariant under the action of the symmetric group.*

For $k \geq 0$, let Λ_n^k be the set of homogeneous symmetric polynomials of degree k. The symmetric polynomials form a subring $\Lambda_n = \mathbb{K}[\boldsymbol{X}]^{\mathcal{S}_n}$ of $\mathbb{K}[\boldsymbol{X}]$ which is a graded ring with $\Lambda_n = \bigoplus_{k\geq 0} \Lambda_n^k$.

For an integer $k \geq 0$, the k-th *elementary symmetric function* $\eta_k(\boldsymbol{X})$ of $\boldsymbol{X}$ is the sum of all products of k distinct variables x_i, so that $\eta_0 = 1$ and

$$\eta_k(\boldsymbol{X}) = \sum_{1\leq i_1<\cdots<i_k\leq n} x_{i_1}\cdots x_{i_k}$$

for $k \geq 1$. For an integer $k \geq 0$, the k-th *complete symmetric function* $h_k(\boldsymbol{X})$ is the sum of all monomials of total degree k in the variables $\boldsymbol{X}$, so that $h_0 = 1$ and

$$h_k(\boldsymbol{X}) = \sum_{1\leq i_1\leq\cdots\leq i_k\leq n} x_{i_1}\cdots x_{i_k}$$

for $k \geq 1$. In particular, $h_1 = \eta_1$.

Theorem 3.5.2 (Fundamental theorem of symmetric functions)**.** [49, Theorem 3.10.1] *We have*

$$\Lambda_n = \mathbb{K}[\eta_1, \ldots, \eta_n]$$

and the η_k *are algebraically independent over* $\mathbb{K}$.

This theorem implies that, for any polynomial f in Λ_n, there exists a unique polynomial $\overline{f}$ in $\mathbb{K}[e_1, \ldots, e_n]$ such that

$$f(\boldsymbol{X}) = \overline{f}(\eta_1, \ldots, \eta_n),$$

where e_k are new variables corresponding to k-th elementary symmetric function η_k.

Notions and results in this section can be extended to block symmetric polynomials. Let r be a positive integer. For $1 \leq k \leq r$, let $\boldsymbol{X}_k = (x_{k,1}, \ldots, x_{k,\ell_k})$ be a sequence of ℓ_k variables with $\ell_k \geq 1$. The group $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$ acts naturally on $\mathbb{K}[\boldsymbol{X}_1, \ldots, \boldsymbol{X}_r]$. Extending Theorem 3.5.2 gives

$$\mathbb{K}[\boldsymbol{X}_1, \ldots, \boldsymbol{X}_r]^{\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}} = \mathbb{K}[\boldsymbol{\eta}_1, \ldots, \boldsymbol{\eta}_r],$$

where $\mathbb{K}[\boldsymbol{X}_1, \ldots, \boldsymbol{X}_r]^{\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}}$ denotes the $\mathbb{K}$-algebra of $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$-invariant polynomials and for $k = 1, \ldots, r$, $\boldsymbol{\eta}_k = (\eta_{k,1}, \ldots, \eta_{k,\ell_k})$ denote the vector of elementary symmetric polynomials in variables $\boldsymbol{X}_k$ with $\eta_{k,i}$ has degree i for all $i = 1, \ldots, \ell_k$. In other words, for any $f \in \mathbb{K}[\boldsymbol{X}_1, \ldots, \boldsymbol{X}_r]^{\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}}$, there exists a unique polynomial $\overline{f} \in \mathbb{K}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r]$ such that

$$f(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_r) = \overline{f}(\boldsymbol{\eta}_1, \ldots, \boldsymbol{\eta}_r), \tag{3.4}$$

where $\boldsymbol{e}_k = (e_{k,1}, \ldots, e_{k,\ell_k})$ is a vector of new variables corresponding to elementary symmetric functions $\boldsymbol{\eta}_k$.

3.6 Computational model and complexity estimates

We devote this section to the description some basic algebraic tasks. Our computation model is a RAM over a field $\mathbb{K}$.

3.6.1 Straight-line programs

Let f be a polynomial of degree d in n variable. The usual encoding to represent f is an array of the $\binom{n+d}{n}$ coefficients. In contrast, the sparse encoding only represents the non-zero coefficient-exponent tuples. Such an encoding allows one to store bigger sets of polynomials, especially when the degree d of f is very high.

In this thesis we use another way of representing a polynomial f, which is called the straight-line program encoding. This encoding covers both dense and sparse encoding and has additional advantages for our work.

The idea of using straight-line programs first appeared in the probabilistic testing of polynomial identities. In computer algebraic applications, this encoding was first used with the elimination of one variable problems [98, 113, 114] and later on, these were extended to multivariate elimination problems (see e.g. [85, 84] and references therein).

Definition 3.6.1. *Given a polynomial f, a* straight-line program *encoding* (SLP *for short*) *of f is a circuit $\gamma = (\gamma_{-n+1}, \ldots, \gamma_0, \gamma_1, \ldots, \gamma_L)$ where $\gamma_L = f, \gamma_{-n+1} := x_1, \cdots, \gamma_0 := x_n$ and for $k > 0$, γ_k is of one of the following forms:*

- $\gamma_k = a * \gamma_i$ *or*
- $\gamma_k = \gamma_i * \gamma_j$,

where $* \in \{+, -, \times\}$, $a \in \mathbb{K}$, *and* $i, j < k$.

The length *of a SLP* γ *is* L *and the length* $L(f)$ *of* f *is the minimum of the lengths of straight-line programs encoding* f.

Example 3.6.1. The dense encoding of the polynomial x^{2^k} (here, the number n of variables is 1 and the degree d of the polynomial is 2^k) is $(1, 0, \ldots, 0)$ with 2^k zeroes, its sparse encoding is $(2^d; 1)$, and a SLP encoding, for instance, is

$$\gamma_0 = x, \gamma_1 = \gamma_0 \cdot \gamma_0 = x^2, \ldots, \gamma_d = \gamma_{d-1} \cdot \gamma_{d-1} = x^{2^k}. \tag{3.5}$$

As a result, the length of the dense encoding of x^{2^k} is $2^k + 1$, the length of its sparse encoding is 2, and the length of its SLP encoding is bounded by d.

We remark that, under a linear change of variables sparse encodings do not behave well, while straight-line programs do not change very much. For example, by adding $\gamma'_1 = \gamma'_{-1} + \gamma_0$, where $\gamma'_{-1} = y$, before γ_1 in the SLP in (3.5), one can deduce that the length $L((x+y)^{2^d})$ is bounded by $d+1$, while both dense and sparse encodings have length $\binom{2^d}{2} = O(2^{2d})$.

In addition, the notion of SLP encoding covers both dense and sparse encoding notions. More precisely, if d is the degree of $f \in \mathbb{K}[x_1, \ldots, x_n]$, then $L(f) \leq 3\binom{n+d}{n}$. This can be seen as follows: the number of monomials of degrees at most d in $\mathbb{K}[x_1, \ldots, x_n]$ is $\binom{n+d}{n}$, taking the multiplication of all monomials of f with their coefficients and adding them up requires $2\binom{n+d}{n}$ operations. Also, it is clear that if a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ has degree d with N nonzero coefficients, then $L(f) = O(Nd)$.

3.6.2 The probabilistic aspects

Our algorithms are randomized (or probabilistic) in the sense that they make random choices of points which leads to a correct computations; those points are not in certain Zariski closed sets of suitable affine spaces. In this sense, our algorithms are of Monte Carlo type (see e.g. [8, 80]), that is, they returns the correct output with high probability, at least a fixed value greater than 1/2. Note that the error probability can be made to arbitrarily small by repeating the algorithms.

Although we will not estimate the probabilities that our algorithms are correct, these probabilities can be controlled by using the Schwartz-Zippel lemma (see e.g. [163] or [80, Lemma 6.44]). More precisely, we define sufficiently large finite sets of integers whose cardinalities depend on the degrees of polynomials defining the mentioned Zariski closed set previously and then make the needed random choices uniformly within these sets.

Lemma 3.6.2. [80, Lemma 6.44] *Let R be an integral domain and S be a finite subset of R. Let r be a polynomial in $R[x_1, \ldots, x_n]$ of degree at most d. Then, if r is not the zero polynomial, then r has at most $d\,(\sharp S)^{n-1}$ zeroes in S^n.*

Example 3.6.2. Let S be a set of complex numbers of cardinality 100 and let us consider the generic quadratic polynomial $f = ax^2 + bx^2 + c$. The polynomial f has two distinct roots when $\Delta(a, b, c) = a(b^2 - 4ac) \neq 0$.

Marking a uniform random choice (α, β, γ) for (a, b, c) in S, the probability that (α, β, γ) is a solution of $\Delta(a, b, c)$ is at most $\frac{1}{\deg(\Delta)(\sharp S)^2}$, using the Schwartz-Zippel lemma, which is at most $1/30000$. Therefore, by taking random values of a, b, c in S, the probability that $ax^2 + bx^2 + c$ has two different roots is at least $1 - 1/30000$.

3.6.3 Basic complexity estimates

In the whole thesis, we will use the standard O notation: for functions $f(x), g(x)$, we say $f(x) = O(g(x))$ if there exists a positive number m such that $|f(x)| \leq m\,|g(x)|$. In addition, we use $O^{\tilde{}}$ to indicate that polylogarithmic factors are omitted, that is, $f(x) = O^{\tilde{}}(g(x))$ if $f(x) = O(g(x)\ \log^k(g(x)))$[1] for some k.

We denote by ω the exponent in the complexity estimate $O(n^\omega)$ for the multiplication of two matrices of size $n \times n$ with coefficients in $\mathbb{Q}$. The current state of the art for ω is $2 \leq \omega \leq 2.3737$ [44, 122, 168, 176].

3.7 Symbolic homotopy continuation methods

The aim of this section is to introduce the basic ideas of symbolic homotopy methods as well as their application to polynomial system solving. Homotopy techniques play an important role in this thesis, so for completeness, we include background details in this section for the benefit of the reader. The objects in this section are square polynomial systems. We will see in the next part of the thesis that homotopy continuation can be extended to overdetermined systems (systems with more equations than unknowns).

Recall that homotopy continuation is a technique which deforms the solutions of a simpler system (called *start system*) into the solutions of the system that we want to solve (called *target system*). More precisely, suppose we seek the isolated solutions of a system $\boldsymbol{f} = (f_1, \ldots, f_n)$, where $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ for $i = 1, \ldots, n$. A start system is $\boldsymbol{g} = (g_1, \ldots, g_n)$ which is in $\mathbb{K}[x_1, \ldots, x_n]$. Consider a deformation $\boldsymbol{h} = (h_1, \ldots, h_n)$ which is defined as

$$h_i = t \cdot f_i + (1 - t) \cdot g_i \in \mathbb{K}[t, x_1, \ldots, x_n],$$

[1] log denotes logarithm to base 2.

where t is a new indeterminate. The system $(h_1, \ldots, h_n)$ is sometimes called the *homotopy system* or *continuation system*. For $\tau \in \overline{\mathbb{K}}$, we write $\boldsymbol{h}_{t=\tau} = (h_1(\tau, \boldsymbol{X}), \cdots, h_n(\tau, \boldsymbol{X}))$; in particular, we have $\boldsymbol{h}_{t=0} = \boldsymbol{g}$ and $\boldsymbol{h}_{t=1} = \boldsymbol{f}$. Note that the system $\boldsymbol{h} \in \mathbb{K}[t, \boldsymbol{X}]^n$ may not define a curve in $\overline{\mathbb{K}}^{n+1}$, for example, if $\boldsymbol{f} = -\boldsymbol{g}$, the fiber above $t = 1/2$ has dimension n.

In what follows, for $n \in \mathbb{N}$ and an algebraically closed field $\mathcal{K}$, we denote by $\mathbb{A}^n(\mathcal{K})$ the n-dimensional affine space over $\mathcal{K}$.

3.7.1 The homotopy curve $\mathcal{W}$

Let $W = V(\boldsymbol{h}) \subset \overline{\mathbb{K}}^{n+1}$ and $\pi : W \to \mathbb{A}^1$ be the projection map defined by $\pi(\tau, \boldsymbol{x}) = \tau$. The degree of π is defined as the number

$$c = \max(\sharp\pi^{-1}(\tau) \,:\, \tau \in \mathbb{A}^1 \text{ and } \pi^{-1}(\tau) \text{ is finite}).$$

Suppose further that $\pi^{-1}(0)$ is a zero-dimensional variety of degree c and that the Jacobian matrix $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})$ with respect to $\boldsymbol{X}$ is invertible for any point $(0, \boldsymbol{x}) \in \pi^{-1}(0)$; the former means $\pi^{-1}(0)$ has maximal cardinality while the latter implies that the ideal $\langle \boldsymbol{h}_{t=0} \rangle \subset \overline{\mathbb{K}}[\boldsymbol{X}]$ is radical.

Let $J = Q_1 \cap \cdots \cap Q_\ell$ be an irredundant primary decomposition of $J = \langle \boldsymbol{h} \rangle \subset \mathbb{K}[t, \boldsymbol{X}]$, and let $P_1, \ldots, P_\ell$ be the associated primes. For some $s \leq \ell$, we assume that $P_1, \ldots, P_s$ are the minimal primes so that $V(P_1), \ldots, V(P_s)$ are the irreducible components of $W = V(J) \subset \overline{\mathbb{K}}^{n+1}$. That is, if we write $W_i = V(P_i)$, for $1 \leq i \leq s$, then $W = W_1 \cup \cdots \cup W_s$ is the irreducible decomposition of W. For a positive integer $r \leq s$, let $W_1, \ldots, W_r$ be the irreducible components of W such that the restriction $\pi|_{W_i} : W_i \to \mathbb{A}^1$ is dominant, that is, the image $\pi(W_i)$ is Zariski dense, for $1 \leq i \leq r$. We write $\mathcal{W} := \cup_{1 \leq i \leq r} W_i$. The set $\mathcal{W}$ is indeed a nonempty equidimensional variety of dimension one; the algebraic set $\mathcal{W}$ is then called the *homotopy curve* and its degree is denoted by δ.

Lemma 3.7.1. *The union $\mathcal{W} = \cup_{1 \leq i \leq r} W_i$ is equidimensional variety of dimension one. In addition, for any $\tau \in \overline{\mathbb{K}}$ and any isolated solution $\boldsymbol{x} \in \overline{\mathbb{K}}^n$ of $\boldsymbol{h}_{t=\tau}(\boldsymbol{X})$, there exists $i \in \{1, \ldots, r\}$ such that $(\tau, \boldsymbol{x}) \in W_i$.*

Proof. Since W is defined by n polynomials $\boldsymbol{h}$ in $n+1$ variables $(t, \boldsymbol{X})$, then by Krull's Theorem, any irreducible component of W has dimension at least one, which implies that $\dim(\mathcal{W}) \geq 1$.

It remains to show that $\dim(\mathcal{W}) \leq 1$. For $X \in \{W_1, \ldots, W_r\}$, let $Y = \pi(X)$ be the image of X and λ be the minimum value of $\dim(\pi^{-1}(p))$ on Y. Then by Fiber Dimension Theorem (see e.g [93, Corollary 11.13]), we have

$$\dim(X) = \dim(Y) + \lambda.$$

Moreover, we claim that $\lambda \leq 0$. Indeed, if $\pi^{-1}(0) \cap X = \emptyset$, then since $\pi^{-1}(0)$ is zero-dimensional and $\lambda \leq \dim(\pi^{-1}(0))$, one has $\lambda \leq 0$; otherwise λ is equal to 0. Therefore, $\dim(X) \leq 1$, and then $\dim(\mathcal{W}) \leq 1$.

For $\tau \in \overline{\mathbb{K}}$ and $\boldsymbol{x} \in \overline{\mathbb{K}}^n$ is an isolated zero of $\boldsymbol{h}_{t=\tau}$, $(\tau, \boldsymbol{x})$ lies in an irreducible component Z of W of dimension at least one. Furthermore, since $(\tau, \boldsymbol{x})$ is an isolated point of $Z \cap V(t-\tau)$, the dimension of Z is one and $\overline{\pi(Z)} = \overline{\mathbb{K}}$. □

Lemma 3.7.2. *The set $\mathcal{W}$ is the union of all irreducible components of W having non-empty intersections with $\pi^{-1}(0)$.*

Proof. First we will show that $\pi^{-1}(0) \cap W_i$ is nonempty for all $i = 1, \ldots, r$. Assume a contradiction that there exists an irreducible component $X \in \{W_1, \ldots, W_r\}$ such that $\pi^{-1}(0) \cap X = \emptyset$. Then there is a point $\tau \in \overline{\mathbb{K}}$ such that $\pi^{-1}(\tau)$ is finite and both $\pi|_X^{-1}(\tau)$ and $\pi|_Y^{-1}(\tau)$ have maximal cardinality for all $Y \in \{W_1, \ldots, W_i\}$ with $\pi^{-1}(0) \cap Y \neq 0$. This implies that $\sharp\pi^{-1}(0) < \sharp\pi^{-1}(\tau)$, which contradicts with the fact that $\pi^{-1}(0)$ have maximal cardinality. Thus, $\pi^{-1}(0) \cap W_i \neq \emptyset$ for all $i = 1, \ldots, r$.

Conversely, let X be any irreducible components of W such that $\pi^{-1}(0) \cap X \neq \emptyset$. Then there exists a points $\boldsymbol{x} \in \overline{\mathbb{K}}^n$ such that $\boldsymbol{x}$ is isolated in $V(\boldsymbol{h}_{t=0})$; and so, by Lemma 3.7.1, X is one of $\{W_1, \ldots, W_r\}$. □

Let us denote by $\mathscr{D}$ the determinant of the Jacobian matrix $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})$ of $\boldsymbol{h}(t, \boldsymbol{X})$ with respect to $\boldsymbol{X}$. Then $\mathcal{W}$ is indeed the Zariski closure of $V(J) \setminus V(\mathscr{D})$.

Lemma 3.7.3. *The equality $\mathcal{W} = V(J : \mathscr{D}^\infty)$ holds.*

Proof. Since the irreducible components of $V(J : \mathscr{D}^\infty)$ are all irreducible components of $\mathcal{W}$ so that the Jacobian matrix $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})$ does not vanish identically, so $\mathcal{W} \subset V(J : \mathscr{D}^\infty)$. The converse holds by using the so-called Lazard Lemma [141, Proposition 3.4]. This lemma implies that $V(J : \mathscr{D}^\infty)$ is one-dimensional and for any irreducible component $\mathcal{C}$ of $V(J : \mathscr{D}^\infty)$, the image by π of $\mathcal{C}$ is dense. □

Let us write $J = J' \cap J''$, with $J' = Q_1 \cap \cdots \cap Q_r$ and $J'' = Q_{r+1} \cap \cdots \cap Q_s$. Let $\mathfrak{J}'$ be the extension of J' in $\mathbb{K}(t)[\boldsymbol{X}]$. The Jacobian criterion implies that $\mathfrak{J}'$ is radical and the variety $V(\mathfrak{J}') \subset \overline{\mathbb{K}(t)}^n$ is zero-dimensional of degree c.

With the above conditions, any point in $V(\mathfrak{J}')$ can be considered as a vector of power series in $\mathbb{K}[[t]]$. Indeed, the implicit function theorem implies that for any point $\boldsymbol{\alpha} \in V(\boldsymbol{h}_{t=0})$, since $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h}_{t=0})(\boldsymbol{x})$ has full-rank, there exists a unique vector $\boldsymbol{e}_{\boldsymbol{\alpha}}$ of power series in $\mathbb{K}[[t]]$ such that

$$\boldsymbol{e}_{\boldsymbol{\alpha}}(0) = \boldsymbol{\alpha} \text{ and } h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}) = 0 \text{ for all } 1 \leq i \leq n.$$

These vectors can be found by means of the Newton operator. Moreover, Lemma 3.7.2 implies that the correspondence $V(\boldsymbol{h}_{\tau=0}) \to V(\mathfrak{J}')$ given by $\boldsymbol{\alpha} \mapsto \boldsymbol{e}_{\boldsymbol{\alpha}}$ is one-to-one.

To summarize, by Lemma 3.7.1, for every isolated solution $\boldsymbol{x}$ of $\boldsymbol{h}_{t=1}$ (recall that $\boldsymbol{h}_{t=1}$ is our target system), there exists a one-dimensional irreducible component $\mathcal{C}$ of $V(\boldsymbol{h}) \subset \overline{\mathbb{K}}^{n+1}$ such that $(1, \boldsymbol{x}) \in \mathcal{C}$ and $\overline{\pi(\mathcal{C})} = \overline{\mathbb{K}}$. These one-dimensional irreducible components corresponds to isolated points of $V(\boldsymbol{h}) \subset \overline{\mathbb{K}(t)}^n$ by considering $\boldsymbol{h} \in \mathbb{K}[t][\boldsymbol{X}]^n$. Therefore, to find the isolated points in $V(\boldsymbol{h}_{t=1})$, we deal with the isolated solutions of $V(\boldsymbol{h}) \subset \overline{\mathbb{K}(t)}^n$; the latter class of isolated points can be found by means of the Newton operator.

Let $\mathscr{R} = ((q, v_1, \ldots, v_n), \lambda)$ be a zero-dimensional parametrization of $\mathcal{W}$ with all polynomials having coefficients in $\mathbb{K}(t)$. Theorem 1 in [162] gives a bound on the number of performed Newton iterations.

Lemma 3.7.4. *The degrees of numerators and denominators of all coefficients of* $(q, v_1, \ldots, v_n)$ *are bounded by* δ*, where* δ *is the degree of the homotopy curve* $\mathcal{W}$*.*

3.7.2 Newton-Hensel Lifting

Let $\boldsymbol{h} = (h_1(t, \boldsymbol{X}), \ldots, h_n(t, \boldsymbol{X}))$ be polynomials in $\mathbb{K}[t, \boldsymbol{X}]$, where $\boldsymbol{X} = (x_1, \ldots, x_n)$. For any $\tau \in \overline{\mathbb{K}}$, we write $\boldsymbol{h}_{t=\tau} = \boldsymbol{h}(\tau, \boldsymbol{X})$ in $\mathbb{K}[\boldsymbol{X}]$. Assume that $V(\boldsymbol{h}_{t=0}) \subset \overline{\mathbb{K}}^n$ is finite and the ideal $\langle \boldsymbol{h}_{t=0} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be a point in $V(\boldsymbol{h}_{t=0})$. We will see that there exists a unique vector of formal power series $\boldsymbol{e}_{\boldsymbol{\alpha}} = (e_{\boldsymbol{\alpha},1}, \ldots, e_{\boldsymbol{\alpha},n})$ in $\overline{\mathbb{K}}[[t]]^n$ such that

$$\boldsymbol{e}_{\boldsymbol{\alpha}}(0) := (e_{\boldsymbol{\alpha},1}(0), \ldots, e_{\boldsymbol{\alpha},n}(0)) = \boldsymbol{\alpha} \quad \text{and} \quad h_1(t, \boldsymbol{e}_{\boldsymbol{\alpha}}) = \cdots = h_n(t, \boldsymbol{e}_{\boldsymbol{\alpha}}) = 0. \tag{3.6}$$

The procedure of finding such vector of formal power series from a given point is called *Newton-Hensel lifting*. We will follow arguments of [96, 87, 162, 109] (see also references therein).

Since the ideal $\langle \boldsymbol{h}_{t=0} \rangle$ is radical in $\mathbb{K}[\boldsymbol{X}]$, the Jacobian matrix $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h}_{t=0})$ of $\boldsymbol{h}_{t=0}$ with respect to $\boldsymbol{X}$ is unimodular over $\overline{\mathbb{K}}$-algebra, which implies that the Jacobian matrix $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})$ of $\boldsymbol{h}(t, \boldsymbol{X})$ with respect to $\boldsymbol{X}$ is also unimodular over the localization

$$\left(\overline{\mathbb{K}}[t, \boldsymbol{X}]/\langle \boldsymbol{h} \rangle\right)_{\langle t \rangle} = \overline{\mathbb{K}}[t]_{\langle t \rangle}[\boldsymbol{X}]/\langle \boldsymbol{h} \rangle.$$

The *Newton operator* $N_{\boldsymbol{h}}(\boldsymbol{X})$ associated to $\boldsymbol{h}(t, \boldsymbol{X})$ is defined as

$$N_{\boldsymbol{h}}(\boldsymbol{X})^T := \boldsymbol{X}^T - \mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})^{-1} \cdot \boldsymbol{h}(\boldsymbol{X})^T \in \mathbb{K}(\boldsymbol{X})^{n \times 1}, \tag{3.7}$$

where the superscript ^{T} denotes the transpose of a vector.

Given a point $\boldsymbol{\alpha}$ in $V(\boldsymbol{h}_{t=0})$, we define a recursive construction as follows:

- $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(0)} = \boldsymbol{\alpha}$, and
- for $k \in \mathbb{Z}_{\geq 1}$, $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)} = N_{\boldsymbol{h}}(\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k-1)})$.

In other words, for $k \in \mathbb{Z}_{\geq 0}$, if $N_{\boldsymbol{h}}^k$ denotes the operator obtained by applying the Newton operator k times recursively, then we can define $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)} = N_{\boldsymbol{h}}^k(\boldsymbol{\alpha})$. We claim that the sequence $(\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)})_{k\geq 0}$ is well-defined. To do it, we prove the following claim.

Lemma 3.7.5. *For an integer $k \in \mathbb{Z}_{\geq 0}$,*

(a) *the determinant of $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})$ at $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}$ is invertible in $\mathbb{K}[t]/\langle t\rangle$ and*

(b) *$h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}) = 0 \mod t^{2^k}$ for all $i = 1, \ldots, n$.*

Proof. We prove this lemma by induction on k. For $k = 0$, the claim follows from assumption that $\pi^{-1}(0)$ is unramified and the fact that $\boldsymbol{\alpha}$ is in $V(\boldsymbol{h}_{t=0})$.

Let us assume that both (**a**) and (**b**) hold for $k \geq 0$. We will show that (**a**) and (**b**) also hold for $k+1$. Since $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} = N_{\boldsymbol{h}}(\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)})$, where $N_{\boldsymbol{h}}$ is defined as in (3.7), we have

$$\left(\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}\right)^T = -\left(\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})(e_{\boldsymbol{\alpha}}^{(k)})\right)^{-1} \begin{pmatrix} h_1(t, e_{\boldsymbol{\alpha}}^{(k)}) \\ \vdots \\ h_n(t, e_{\boldsymbol{\alpha}}^{(k)}) \end{pmatrix}; \tag{3.8}$$

together with the induction hypothesis (**b**) for k, one can deduce that

$$\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)} = 0 \mod t^{2^k}. \tag{3.9}$$

Let us denote by F the determinant of the Jacobian matrix $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})$ with respect to variables $\boldsymbol{X}$. Using the Taylor expansion of F between the points $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)}$ and $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}$ gives

$$F(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)}) = F(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}) + \sum_{j=1}^{n} \frac{\partial F}{\partial x_j}(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)})(\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}) \mod \langle \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}\rangle^2,$$

where $\langle \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}\rangle = \langle e_{\boldsymbol{\alpha},1}^{(k+1)} - e_{\boldsymbol{\alpha},1}^{(k)}, \ldots, e_{\boldsymbol{\alpha},n}^{(k+1)} - e_{\boldsymbol{\alpha},n}^{(k)}\rangle$ an ideal in $\overline{\mathbb{K}}(t)$. Moreover, from the induction hypothesis (**a**), $F(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}) \neq 0 \mod t$ and by (3.8), $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)} = 0 \mod t$. Therefore, $F(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)})$ is nonzero modulo t, which gives our claim (**a**) for $k+1$.

To prove part (**b**) holds for $k+1$, multiplying $\left(\frac{\partial h_i}{\partial x_1}, \ldots, \frac{\partial h_i}{\partial x_n}\right)$, for $1 \leq i \leq n$, to both sides of (3.8) gives

$$\left(\frac{\partial h_i}{\partial x_1}, \ldots, \frac{\partial h_i}{\partial x_n}\right)\left(\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}\right)^T = -h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)})$$

and by Taylor expansion of h_i between the points $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)}$ and $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}$,

$$h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)}) = h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}) + \sum_{j=1}^{n} \frac{\partial h_i}{\partial x_j}(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)})(\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}) \mod \langle \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}\rangle^2.$$

This implies that $h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)}) = 0 \mod \langle \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}\rangle^2$. Hence, together with (3.9), we can conclude that $h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)}) = 0 \mod t^{2^{k+1}}$, which is our claim (**b**) for $k+1$. □

We now conclude the existence of the power series $\boldsymbol{e}_{\boldsymbol{\alpha}} = (e_{\boldsymbol{\alpha},1}, \ldots, e_{\boldsymbol{\alpha},n})$ in $\overline{\mathbb{K}}[[t]]^n$ satisfying (3.6). As in (3.8), the equality $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k+1)} - \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)} = 0 \mod t^{2^k}$ holds for any $k \in \mathbb{Z}_{\geq 0}$, then for any $1 \leq i \leq n$, the sequence of rational functions $(e_{\boldsymbol{\alpha},i}^{(k)})_{k\geq 0}$ converges to a power series $e_{\boldsymbol{\alpha},i}$ of $\overline{\mathbb{K}}[[t]]$. By Lemma 3.7.5(**b**), for $1 \leq i \leq n$, $h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)}) = 0$ in $\langle t \rangle^{2^{k+1}}$ for all $k \in \mathbb{Z}_{\geq 0}$, then the equality $h_i(t, \boldsymbol{e}_{\boldsymbol{\alpha}}) = 0$ holds in $\overline{\mathbb{K}}[[t]]$ for any $1 \leq i \leq n$. Finally, the relation in (3.8) gives us $\boldsymbol{e}_{\boldsymbol{\alpha}}(0) = \boldsymbol{\alpha}$.

Algorithm 1 Newton-HenselLifting$(\boldsymbol{h}, \boldsymbol{\alpha}, \delta)$

Input: $\boldsymbol{h} = (h_1, \ldots, h_n)$ in $\mathbb{K}[t, \boldsymbol{X}]^n$ s.t $V(\boldsymbol{h}_{t=0}) \subset \overline{\mathbb{K}}^n$ is finite and $\langle \boldsymbol{h}_{t=0} \rangle$ is radical
a point $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ in $V(\boldsymbol{h}_{t=0})$
a positive integer δ (to stop the algorithm at the precision δ)
Output: the vector approximates $\boldsymbol{\alpha}$ with precision δ in $\overline{\mathbb{K}}[[t]]$.

1. $k \leftarrow 0$ and $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(0)} = \boldsymbol{\alpha}$
2. $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h}) \leftarrow$ the Jacobian matrix of $\boldsymbol{h}$ with respect to $\boldsymbol{X}$
3. while $1 \leq k < \lceil \log(\delta) \rceil$:
   (a) compute $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k)} = N_{\boldsymbol{h}}(\boldsymbol{e}_{\boldsymbol{\alpha}}^{(k-1)})$, where $N_{\boldsymbol{h}}^T := \boldsymbol{X}^T - \mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})^{-1} \cdot \boldsymbol{h}(\boldsymbol{X})^T$
   (b) $k \leftarrow k + 1$
4. return $\boldsymbol{e}_{\boldsymbol{\alpha}}^{(\lceil \log(\delta) \rceil)}$

Lemma 3.7.6. *Suppose polynomials $\boldsymbol{h} = (h_1(t, \boldsymbol{X}), \ldots, h_n(t, \boldsymbol{X}))$ in $\mathbb{K}[t, \boldsymbol{X}]$ are given by a straight-line program of length L. Assume further that $V(\boldsymbol{h}_{t=0})$ is finite and the ideal $\langle \boldsymbol{h}_{t=0} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical. Let $\boldsymbol{\alpha}$ be a point in $V(\boldsymbol{h}_{t=0})$ and δ be a positive integer.*

Then there exists an algorithm, called Newton-HenselLifting*, which takes $\boldsymbol{h}, \boldsymbol{\alpha}$ and δ as input and outputs the approximation of $\boldsymbol{\alpha}$ with precision s in $\overline{\mathbb{K}}[[t]]$ in $O(n(L + n^2)\delta)$ operations in $\mathbb{K}$.*

Proof. Previous result, for example, in [24, Theorem 1] or [84, Lemma 25], implies that computing all partial derivatives $\left(\frac{\partial h_1}{\partial x_j}\right)_{1\leq i,j\leq n}$ requires $O(nL)$ operations in $\mathbb{K}$; therefore, the same cost is needed in order to obtain the matrix $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})$. At the core of the algorithm, we need $O(n^3)$ operations to find the inverse of the Jacobian matrix in $\overline{\mathbb{K}}$ and $O(n^2)$ operations to update vector $\boldsymbol{e}_{\alpha}^{(k)}$. Therefore, at the step k of the loop, $O(nL + n^3)$ operations are performed. In total, the complexity of the algorithm is

$$\sum_{k=0}^{\lceil \log(\delta) \rceil} O((nL + n^3)) = O(n(L + n^2)\delta),$$

which finishes our proof. □

We remark that Newton-Hensel lifting appears in other important constructions in symbolic computation, including factoring and gcd for multivariate polynomials (see e.g. [81]).

3.7.3 Recover a zero-dimensional parametrization $\mathscr{R}$ of $\mathcal{W}$

Let $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_c$ be solutions of $V(\boldsymbol{h}_{t=0})$. For $i = 1, \ldots, c$, we apply Newton-Hensel lifting to the system $\boldsymbol{h}$ to lift $\boldsymbol{\alpha}_i$ into a point $\boldsymbol{e}_{\boldsymbol{\alpha}_i}$ in $\mathbb{K}[[t]]/\langle t^{2\delta}\rangle$, where δ is the degree of the homotopy curve $\mathcal{W}$. These power series are all the solutions of the extension of $\mathfrak{J}'$ to $\overline{\mathbb{K}}((t))[\boldsymbol{X}]$, where $\mathbb{K}((t))$ is the field of fractions of the ring $\mathbb{K}[[t]]$.

Let λ be a linear form in $\mathbb{K}[\boldsymbol{X}]$ separating $(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_c)$. Then the following interpolation formulas

$$q = \prod_{i=1}^{c} (y - \lambda(e_{\boldsymbol{\alpha}_i})) \text{ and } v_i = \sum_{\substack{\boldsymbol{e}=(e_1,\ldots,e_n) \\ \boldsymbol{e}\in\{\boldsymbol{e}_{\boldsymbol{\alpha}_1},\ldots,\boldsymbol{e}_{\boldsymbol{\alpha}_c}\}}} e_i \prod_{\boldsymbol{e}'\in\{\boldsymbol{e}_{\boldsymbol{\alpha}_1},\ldots,\boldsymbol{e}_{\boldsymbol{\alpha}_c}\},\boldsymbol{e}'\neq\boldsymbol{e}} (y - \lambda(\boldsymbol{e}')) \text{ for } i = 1, \ldots, n$$

define a zero-dimensional parametrization $\mathscr{R} = ((q, v_1, \ldots, v_n), \lambda)$ of $\mathcal{W}$; clearly, λ is separating for $\mathcal{W}$ as well. In addition, all polynomials $(q, v_1, \ldots, v_n)$ have non-negative valuation at $t = 0$; then, specializing the parametrization $\mathscr{R}$ at $t = 0$ gives a zero-dimensional parametrization of the solution set $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_c\}$ of $V(\boldsymbol{h}_{t=0})$.

We remark that, in general, given a family of zero-dimensional parametrizations $(\mathscr{R}_i)_{i\in I} = ((q_i, v_{i,1}, \ldots, v_{i,n}), \lambda)_{i\in I}$, where $(q_i, v_{i,1}, \ldots, v_{i,n})$ are polynomials with coefficients in $\mathbb{K}(t)[y]$ for all $i \in I$, we can combine all $(\mathscr{R}_i)_{i\in I}$ into a single zero-dimensional $\mathscr{R}$ consisting polynomials in $\mathbb{K}(t)[y]$ such that $Z(\mathscr{R}) = \cup_{i\in I} Z(\mathscr{R}_i)$ by using Chinese Remainder Theorem. If $((q_1, v_{1,1}, \ldots, v_{1,n}), \lambda)$ and $((q_1, v_{2,1}, \ldots, v_{2,n}), \lambda)$ are zero-dimensional parametrizations of disjoint set with q_1 and q_2 relatively prime polynomials, then $((q_1q_2, v_{1,1}q_2 + v_{2,1}q_1, \ldots, v_{1,n}q_2 + v_{2,n}q_1), \lambda)$ is a zero-dimensional parametrization of their union.

3.7.4 Rational reconstruction

A zero-dimensional parametrization $\mathscr{R} = ((q, v_1, \ldots, v_n), \lambda)$ of $\mathcal{W}$ consists of univariate polynomials with coefficients lying in $\mathbb{K}[[t]]/\langle t^{2\delta}\rangle$. Since the degree of $\mathcal{W}$ is δ, knowing $\mathscr{R}$ at precision 2δ allows us to recover a zero-dimensional parametrization $\mathscr{S} = ((w, w_1, \ldots, w_n), \lambda)$ with coefficients in $\mathbb{K}(t)$ such that $Z(\mathscr{S}) = \mathcal{W}$, with all coefficients having numerators and denominators bounded by δ [162, Theorem 1]. This can be done by performing Padé approximation (see e.g. [26, 80]) up to sufficient precision in order to recover numerators and denominators in $\mathbb{K}[t]$ for the coefficients of the polynomials in the parametrization $\mathscr{S}$.

Lemma 3.7.7. [26, 80] *Let $\psi = p/q \in \mathbb{K}(t)$ be a rational function such that p and q are relatively prime polynomial in $\mathbb{K}[t]$ with $\deg(p), \deg(q) \leq \delta$. Assume $q(\tau)$ is nonzero for some $\tau \in \mathbb{K}$ and let $\sum_{i=0}^{2d} \psi_i t^i$ be the Taylor expansion of ψ of order 2δ centered at τ, where*

ψ is a polynomial of degree i in $(t-\tau)$. Then one can compute p and q by using $\tilde{O}(\delta)$ operations in $\mathbb{K}$.

3.7.5 Specializing at $t = 1$

Recall that $\boldsymbol{h}_{t=1}$ is our target system. The study at $t = 1$ is more complicated than the situation at $t = 0$ since the number of roots of $\boldsymbol{h}_{t=1}$ may be fewer than c. For this purpose, we consider the Puiseux series field $\overline{\mathbb{K}}\langle\langle t\rangle\rangle$ in t with coefficients in $\overline{\mathbb{K}}$.

Any non-zero series ϕ in $\overline{\mathbb{K}}\langle\langle t\rangle\rangle$ admits a well-defined *valuation* $\nu(\phi)$, which is smallest exponent that appears in its expansion support, with $\nu(\infty) = 0$. For a vector $\Phi = (\phi_1, \ldots, \phi_n)$ of Puiseux series, its valuation is defined as

$$\nu(\Phi) = \min_{1\leq i\leq n} \nu(\phi_i).$$

A vector of Puiseux series is called *bounded* if its valuation is non-negative. For a vector $\Phi = (\phi_1, \ldots, \phi_n)$ with entries in $\overline{\mathbb{K}}\langle\langle t\rangle\rangle$, $\lim_0(\Phi)$ is the vector $(\lim_0(\phi_1), \ldots, \lim_0(\phi_n)) \in \overline{\mathbb{K}}^n$, with $\lim_0(\phi_i)$ being the coefficient of t^0 in ϕ_i.

Let $\mathcal{J}'$ be the extension of $\mathfrak{J}'$ in $\overline{\mathbb{K}}\langle\langle t\rangle\rangle$. Let $\Phi_1, \ldots, \Phi_c$ be the solutions of $\mathcal{J}'$ in the field of generalized power series in t' with coefficients in $\overline{\mathbb{K}}$ at $t = 1$, with $t' = t - 1$. Without loss of generality, we assume that $\Phi_1, \ldots, \Phi_{c'}$ are bounded and others are not, for some c' in $\{1, \ldots, c\}$. We define $\varphi_1, \ldots, \varphi_{c'}$ by $\varphi_i = \lim_0(\Phi_i)$ for $i = 1, \ldots, c'$. Lemma 5.2.8 implies that

$$V(J' + \langle t - 1\rangle) = \{\varphi_1, \ldots, \varphi_{c'}\}.$$

Following [155] and [159], we need some requirements on the linear form λ to become a separating element.

Definition 3.7.8. *A linear form λ in variables $\boldsymbol{X}$ with coefficients in $\mathbb{K}$ is a* well-separating element *if the following conditions hold.*

1. *λ is separating for $V(\mathcal{J}') = \{\Phi_1, \ldots, \Phi_c\}$;*
2. *λ is separating for $V(J' + \langle t - 1\rangle) = \{\varphi_1, \ldots, \varphi_{c'}\}$;*
3. *$\nu(\lambda(\Phi_i)) = \nu(\varphi_i)$ for all $i = 1, \ldots, c$, where ν denotes the t'-adic valuation.*

Note that the first condition and the discussion from Subsection 3.7.3 implies that λ is separating $V(\boldsymbol{h}_{t=1})$ as well. Applying Lemma 14 in [159, Section 3], we see that these conditions are satisfied for a generic choice of λ. When this is the case, Lemma 4.4 in [155] shows how to recover a zero-dimensional parametrization $\mathscr{Z} = ((r, r_1, \ldots, r_n), \lambda)$ with coefficients in $\mathbb{K}$ for the limit set $V(J' + \langle t - 1\rangle) = \{\varphi'_i : i = 1, \ldots, c'\}$ starting from the previously computed rational parametrization $\mathscr{S} = ((w, w_1, \ldots, w_n), \lambda)$. We use a slight modification from [159, Lemma 12].

Lemma 3.7.9. [159, Lemma 12] *Suppose λ be a well-separating element. Let $\mathscr{S} = ((w, w_1, \ldots, w_n), \lambda)$ be the corresponding zero-dimensional parametrization of $\mathcal{W}$ over $\mathbb{K}((t'))$, and let $e = -\nu(w)$. Then the polynomials $w^\star = t'^e w$ and $w_k^\star = t'^e w_k$ for all $k = 1, \ldots, n$ are in $\mathbb{K}[[t']][y]$.*

Further, let r_0 be the leading coefficient of $w^\star(0, y)$. We define

$$r = \frac{1}{r_0} w^\star(0, y) \quad \text{and} \quad r_k = \frac{1}{r_0} w_k^\star(0, y) \bmod r \quad (1 \le k \le n).$$

Then the polynomials $(r, r_1, \ldots, r_n)$ are such that

$$r = \prod_{i=1}^{c'} (t - \lambda(\varphi_i)) \text{ and } r_i = \sum_{1 \le i \le c} \Phi_{i,k} \prod_{1 \le i' \le c,\, i' \ne i} (y - \lambda(\Phi_{i'})).$$

3.7.6 Cleaning non-isolated points

We have seen that for any isolated points $\boldsymbol{x} \in V(\boldsymbol{h}_{t=1})$, $(1, \boldsymbol{x})$ is in $V(J' + \langle t - 1 \rangle)$, so we need to discard from $V(J' + \langle t - 1 \rangle)$ those points that do not correspond to isolated points of $V(\boldsymbol{h}_{t=1})$. This can be done by our algorithm of Section 5.1-Chapter 5.

Algorithm 2 HomotopySquare$(\boldsymbol{h}, \mathscr{R}_0, \delta)$

Input: $\boldsymbol{h} = (h_1, \ldots, h_n)$ in $\mathbb{K}[t, \boldsymbol{X}]$ such that $\langle \boldsymbol{h}_{t=0} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
the set V_0 containing all isolated points of $V(\boldsymbol{h}_{t=0})$
an upper bound δ on the degree of the homotopy curve

Output: a zero-dimensional parametrization $\mathscr{R}_1$ of the isolated points of $V(\boldsymbol{h}_{t=1})$

1. for all $\boldsymbol{\alpha} \in \mathsf{V}_0$, apply a Newton-Hensel lifting (in parameter t) to the system $\boldsymbol{h}$ to lift $\boldsymbol{\alpha}$ upto precision 2δ to $\boldsymbol{e}_{\boldsymbol{\alpha}} \in \mathbb{K}[[t]]/\langle t^{2\delta} \rangle$
2. combine $(\boldsymbol{e}_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathsf{V}_0}$ into a zero-dimensional parametrization $\mathscr{R}$ with coefficients in $\mathbb{K}[[t]]/\langle t^{2\delta} \rangle$ as in Subsection 3.7.3
3. find a zero-dimensional parametrization $\mathscr{S}$ with coefficients in $\mathbb{K}(t)$ as in Subsection 3.7.4
4. compute a zero-dimensional parametrization $\mathscr{Z}$ with coefficients in $\mathbb{K}$ as in Subsection 3.7.5
5. remove non-isolated points in $V(\boldsymbol{h}_{t=1})$ from $Z(\mathscr{Z})$ to get $\mathscr{R}_1$

3.7.7 Degree bounds and start systems

Let $\boldsymbol{f} = (f_1, \ldots, f_n)$ be the target system with $\deg(f_i) = d_i$. As mentioned above, the complexity of symbolic homotopy continuation methods is dependent on c, the number of paths to be followed in the continuation. This number is also known as the number of isolated solutions of $\boldsymbol{f}$. Therefore, better bounds for c give better algorithms, in complexity, to solve the target system.

When homotopy continuation methods were first developed, the best commonly-known bound for c was the Bézout theorem bound, that is, $c \leq d_1 \cdots d_n$. A common choice for a start system $\boldsymbol{g} = (g_1, \ldots, g_n)$ was a random dense system with polynomials have the same degrees as the target system. Bézout theorem implies that, generically, this start system has exact $d_1 \cdots d_n$ isolated solutions. Another choice for the start system is

$$g_i = \alpha_i x_i^{d_i} - \beta_i \text{ for } i = 1, \ldots, n, \tag{3.10}$$

which also has $d_1 \cdots d_n$ solutions. Recently, some authors use the products of generic linear forms as a start system. More precisely, for $i = 1, \ldots, n$, define

$$g_i = \prod_{k=1}^{d_i} \left(\alpha_{i,0,k} + \alpha_{i,1,k} x_1 + \cdots + \alpha_{i,n,k} x_n\right), \tag{3.11}$$

where $\{\alpha_{i,j,k}\}_{1 \leq i,j \leq n, 1 \leq k \leq d_i}$ are generically chosen in $\mathbb{K}$. The number of isolated solutions of this system is exactly $d_1 \cdots d_n$. Furthermore, both systems of equations in (3.10) and (3.11) are easy to solve: for system (3.10), values of x_i are the d_i-th roots of β_i/α_i while for system from (3.11) one only need to solve $d_1 \cdots d_n$ linear systems by using, for example, Gaussian elimination.

However, many polynomial systems have fewer solutions than general dense systems of total degrees. For instance, system of equations from (3.3) has 8 solutions while the total degree bound of 16. Another known example is the eigenvalue problem. Consider

$$A\boldsymbol{X} = \lambda \boldsymbol{X}, \text{ where } A = (a_{i,j}) \in \mathbb{C}^{n \times n}. \tag{3.12}$$

We might consider (3.12) as the following $n+1$ polynomial equations with $n+1$ unknowns $(\lambda, x_1, \ldots, x_n)$

$$\begin{aligned} &\lambda x_1 - (a_{1,1} x_1 + \cdots + a_{1,n} x_n) = 0 \\ &\quad \vdots \\ &\lambda x_n - (a_{n,1} x_1 + \cdots + a_{n,n} x_n) = 0 \\ &b_1 x_1 + \cdots + b_n x_n - 1 = 0 \end{aligned} \tag{3.13}$$

where $(b_1, \cdots b_n) \in \mathbb{C}^n$ are chosen at random. If $(\lambda, \boldsymbol{x})$ is an eigenvalue-eigenvector pair of (3.12), then $(\lambda, k\boldsymbol{x})$ also satisfies (3.12); so, the last equation in (3.13) is used to normalize

the eigenvectors. The number isolated solutions of (3.13) is n while the Bézout theorem bound is 2^n.

As a result, better bounds on the number of expected solutions and suitable start systems reduce time in solving polynomial system by using homotopy continuation methods. For sparse systems, the BKK bound is used to bound the number of isolated solutions and instead of building start systems as in dense cases, a much better choice is a generic start system $\boldsymbol{g} = (g_1, \ldots, g_n)$ for which the g_i have the same Newton polytope as the polynomials f_i for $i = 1, \ldots, n$. Of course, the solutions of $\boldsymbol{g} = 0$ must be found before apply the homotopy continuation methods. For this purpose, authors of [110] propose a deformation, which combines Huber and Sturmfels homotopic procedures in [104] with symbolic homotopy techniques, for solving sparse zero-dimensional polynomial systems.

Part I

Determinantal systems

Chapter 4

An overview

Consider a sequence of polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[\boldsymbol{X}]$ and a matrix $\boldsymbol{F}$ in $\mathbb{K}[\boldsymbol{X}]^{p\times q}$, where $\boldsymbol{X} = (x_1, \ldots, x_n)$. In this part of the thesis, we study the problem of computing the set of points in $\overline{\mathbb{K}}^n$ at which $\boldsymbol{G}$ vanishes and $\boldsymbol{F}$ has rank deficient.

4.1 Problem statements

Let $\boldsymbol{G} = (g_1, \ldots, g_s)$ be a sequence of polynomials in $\mathbb{K}[\boldsymbol{X}]$ and $\boldsymbol{F}$ be a matrix in $\mathbb{K}[\boldsymbol{X}]^{p\times q}$ such that $p \leq q$ and $n = q - p + s + 1$. The central question that we are interested in is to describe the set

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = \{\boldsymbol{x} \in \overline{\mathbb{K}}^n \,|\, \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p \text{ and } g_1(\boldsymbol{x}) = \cdots = g_s(\boldsymbol{x}) = 0\}.$$

A natural algebraic representation for the problem above gives rise to a determinantal ideal which is generated by $\boldsymbol{G}$ and all p-minors of $\boldsymbol{F}$. For any matrix $\boldsymbol{F}$, polynomials $\boldsymbol{G}$, and an integer r, we denote by $M_r(\boldsymbol{F})$ the set of r-minors of $\boldsymbol{F}$ and by

$$I_r(\boldsymbol{F}, \boldsymbol{G}) = \langle g_1, \ldots, g_s\rangle + \langle M_r(\boldsymbol{F})\rangle,$$

the ideal generated by $\boldsymbol{G}$ and $M_r(\boldsymbol{F})$. Then $V_p(\boldsymbol{F}, \boldsymbol{G})$ is an algebraic set with

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = V(I_p(\boldsymbol{F}, \boldsymbol{G})).$$

Remark 4.1.1. *It is natural to assume that $n = q - p + s + 1$. Indeed, results due to Macaulay [131] and Eagon and Northcott [52] imply that all irreducible components of $V(M_p(\boldsymbol{F}))$ have codimension at most $q - p + 1$. Hence, the irreducible components of $V_p(\boldsymbol{F}, \boldsymbol{G})$ have codimension at most $q - p + s + 1$ by Krull's theorem. This implies that the irreducible components of $V_p(\boldsymbol{F}, \boldsymbol{G})$ in $\overline{\mathbb{K}}^n$ have dimension at least $n - (q - p + s + 1)$, which is positive when $n > q - p + s + 1$. In such cases, there are no isolated points in $V_p(\boldsymbol{F}, \boldsymbol{G})$.*

In addition, in the case $n = q - p + 1$ (that is when $s = 0$), it is proved, for instance, in [167], that $V(M_r(\boldsymbol{F}))$ has dimension zero for a generic choice of the entries of $\boldsymbol{F}$.

Note that for systems coming from optimization, this condition is satisfied since in this case, when $\boldsymbol{F}$ is the Jacobian matrix of $\boldsymbol{G}$ together the gradient of a function that we want to optimize on $V(\boldsymbol{G})$, we have $p = s + 1$ and $q = n$.

Even under this assumption, $V_p(\boldsymbol{F}, \boldsymbol{G})$ may have positive dimensional components, so we will be interested in describing only isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

Problem 1. *For $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p\times q}$ and $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that $p \leq q$ and $n = q - p + s + 1$, compute the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.*

In several of these situations, we are only interested in the solutions of the system made of minors $M_p(\boldsymbol{F})$ and $\boldsymbol{G} = (g_1, \ldots, g_s)$ at which the associated Jacobian matrix has full rank; these are simple points in $V_p(\boldsymbol{F}, \boldsymbol{G})$. Hence, it also makes sense to look at the following slight variant of Problem (1).

Problem 2. *For $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p\times q}$ and $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$, with $p \leq q$ and $n = q - p + s + 1$, compute the simple points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.*

It is often the case that the polynomials making up $\boldsymbol{G}$ and entries of $\boldsymbol{F}$ are in fact sparse. For instance, in optimization problems, when the object function ϕ and polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ are sparse, then so are entries of $\boldsymbol{F}$. A second example occurs when both ϕ and $\boldsymbol{G}$ are invariant under the action of the symmetric group, a situation which we make more precise in Part II of the thesis. Therefore, we also study the following problem.

Problem 3. *Consider sparse polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ and $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p\times q}$ with sparse entries such that $p \leq q$ and $n = q - p + s + 1$, compute the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.*

The tools used to create our sparse column support homotopy also allow us to build a column homotopy algorithm for determinantal systems for weighted polynomials. These are important when all our input polynomials (including those in the input matrix) are invariant under the action of the group of permutations on n letters. In that case, one can perform an algebraic change of coordinates to express all entries with respect to elementary symmetric functions which are naturally weighted (the k-th elementary symmetric function then has weighted degree k). This procedure will be made more precise in Part II. As such we look at the following slight variant of Problem (3).

Problem 4. *Let $\mathbb{K}[x_1, \ldots, x_n]$ be a polynomial ring of weights $(w_1, \ldots, w_n)$. For $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p\times q}$ and $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that $p \leq q$ and $n = q-p+s+1$, compute the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.*

4.2 Main results

Our first result gives bounds on the number of solutions of $V_p(\boldsymbol{F}, \boldsymbol{G})$, counted with multiplicities. We will consider two degree measures for the matrix $\boldsymbol{F}$ which have been used

before in [144, 136]. For $i = 1, \ldots, p$, we will write $\mathrm{rdeg}(\boldsymbol{F}, i)$ for the degree of the i-th row of $\boldsymbol{F}$, that is, $\mathrm{rdeg}(\boldsymbol{F}, i) = \max(\deg(f_{i,j}))_{1 \le j \le q}$. Similarly, for $j = 1, \ldots, q$, we write $\mathrm{cdeg}(\boldsymbol{F}, j)$ for the degree of the j-th column of $\boldsymbol{F}$, that is, $\mathrm{cdeg}(\boldsymbol{F}, j) = \max(\deg(f_{i,j}))_{1 \le i \le p}$.

Theorem 4.2.1. *Let $\boldsymbol{F}$ be in $\mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ and let $\boldsymbol{G} = (g_1, \ldots, g_s)$ be in $\mathbb{K}[x_1, \ldots, x_n]$, with $p \le q$ and $n = q - p + s + 1$. Then, the sum of the multiplicities of the isolated points of the ideal generated by the p-minors of $\boldsymbol{F}$ and $g_1, \ldots, g_s$ is at most $\min(c, c')$ with*

$$c = \deg(g_1) \cdots \deg(g_s) \cdot \eta_{n-s}(\mathrm{cdeg}(\boldsymbol{F}, 1), \ldots, \mathrm{cdeg}(\boldsymbol{F}, q))$$

and

$$c' = \deg(g_1) \cdots \deg(g_s) \cdot h_{n-s}(\mathrm{rdeg}(\boldsymbol{F}, 1), \ldots, \mathrm{rdeg}(\boldsymbol{F}, p)),$$

where $\eta_k(\cdot)$ is the k-th elementary symmetric function and $h_k(\cdot)$ is the k-th complete symmetric function.

When $\mathrm{rdeg}(\boldsymbol{F}, i) = \mathrm{cdeg}(\boldsymbol{F}, j) = d$ for all i, j, the c and c' coincide with the common value $\deg(g_1) \cdots \deg(g_s)\binom{q}{p-1}$. Otherwise, one can take the minimum between $\eta_{n-s}(\mathrm{cdeg}(\boldsymbol{F}, 1), \ldots, \mathrm{cdeg}(\boldsymbol{F}, q))$ and $h_{n-s}(\mathrm{rdeg}(\boldsymbol{F}, 1), \ldots, \mathrm{rdeg}(\boldsymbol{F}, p))$.

Example 4.2.1. Consider the case there are no equations $\boldsymbol{G}$ and the degrees of the entries of $\boldsymbol{F}$ are

$$\begin{bmatrix} 2 & 1 & 5 & 7 \\ 2 & 1 & 5 & 7 \\ 2 & 1 & 5 & 7 \end{bmatrix}.$$

Here, $s = 0, p = q = 3$, and $n = 2$. Then

$$c = \eta_2(2, 1, 5, 7) = 73 \text{ and } c' = h_2(7, 7, 7) = 294,$$

and so the number of isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$ is at most 73.

On the other hand, if the degrees of the entries of $\boldsymbol{F}$ are

$$\begin{bmatrix} 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \\ 5 & 5 & 5 & 5 \end{bmatrix},$$

then $c = \eta_2(5, 5, 5, 5) = 100$ and $c' = h_2(2, 1, 5) = 47$. In this case, the number of isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$ is bounded by 47.

For systems coming from optimization, where $\boldsymbol{F}$ is a Jacobian matrix, we are in a situation similar to our second example. That is the i-th row degree of $\boldsymbol{F}$ is simply the degree of the corresponding equation, minus one.

Our second result gives bounds on the cost of computing a zero-dimensional parametrization of the isolated solutions of $V_p(\boldsymbol{F}, G)$ and so gives an answer for Problem (1).

Theorem 4.2.2. *Suppose that matrix* $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ *and polynomials* $\boldsymbol{G} = (g_1, \ldots, g_s)$ *in* $\mathbb{K}[x_1, \ldots, x_n]$ *are given by a straight-line program of length* σ*. Assume that* $(\deg(g_i))_{1 \le i \le s}$*, as well as* $\operatorname{cdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{cdeg}(\boldsymbol{F}, q)$ *and* $\operatorname{rdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{rdeg}(\boldsymbol{F}, p)$ *are all at least equal to* 1*.*

Then, there exist randomized algorithms that solve Problem (1) *in either*

$$O^{\sim}\left(\binom{q}{p} c(e + c^5)\big(\sigma + q\delta + \gamma\big)\right)$$

operations in $\mathbb{K}$*, with*

$$\begin{aligned}
c &= \deg(g_1) \cdots \deg(g_s)\ \eta_{n-s}(\operatorname{cdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{cdeg}(\boldsymbol{F}, q)),\\
e &= (\deg(g_1) + 1) \cdots (\deg(g_s) + 1)\ \eta_{n-s}(\operatorname{cdeg}(\boldsymbol{F}, 1) + 1, \ldots, \operatorname{cdeg}(\boldsymbol{F}, q) + 1),\\
\gamma &= \max(\deg(g_1), \ldots, \deg(g_s)),\\
\delta &= \max(\operatorname{cdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{cdeg}(\boldsymbol{F}, q))
\end{aligned}$$

or

$$O^{\sim}\left(\binom{q}{p} c'(e' + c'^5)\big(\sigma + p\alpha + \gamma\big)\right)$$

operations in $\mathbb{K}$*, with*

$$\begin{aligned}
c' &= \deg(g_1) \cdots \deg(g_s)\ h_{n-s}(\operatorname{rdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{rdeg}(\boldsymbol{F}, p)),\\
e' &= (\deg(g_1) + 1) \cdots (\deg(g_s) + 1)\ h_{n-s}(\operatorname{rdeg}(\boldsymbol{F}, 1) + 1, \ldots, \operatorname{rdeg}(\boldsymbol{F}, p) + 1),\\
\gamma &= \max(\deg(g_1), \ldots, \deg(g_s)),\\
\alpha &= \max(\operatorname{rdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{rdeg}(\boldsymbol{F}, p)).
\end{aligned}$$

The assumption that all degrees are at least 1 is not a strong restriction. If $\deg(g_i) = 0$ for some i, then g_i is constant. So, either the system is inconsistent (if $g_i \neq 0$) or g_i can be discarded from the system. If the latter holds, then s decreases and so n is strictly less than $q - p + s + 1$ after this update which implies that there is no isolated point in $V_p(\boldsymbol{F}, \boldsymbol{G})$, by Remark 4.1.1. Similarly, if say $\operatorname{cdeg}(\boldsymbol{F}, i) = 0$, then the i-th column of $\boldsymbol{F}$ consists of constants. After applying linear combinations with coefficients in $\mathbb{K}$ to the rows of $\boldsymbol{F}$, we may assume that all entries in the i-th column, except at most one, are non-zero without changing the column degrees. The i-th column of $\boldsymbol{F}$ (and the row of the non-zero entry, if there is one) can then be discarded. In other words, both p and q decrease by 1, so we still have $n = q - p + s + 1$.

Note that in the common situation where all measures $(\deg(g_i))_{1 \le i \le s}$, $(\operatorname{rdeg}(\boldsymbol{F}, i))_{1 \le i \le p}$, and $(\operatorname{cdeg}(\boldsymbol{F}, j))_{1 \le j \le q}$ involved in the formulas above are at least equal to 2, we have the inequalities $e \le c^2$, $e' \le c'^2$, and $\binom{q}{p} \le c'$. As a result, the runtimes become polynomial in either c, σ and c', σ with $O^{\sim}(c^8\sigma)$ and $O^{\sim}(c'^8\sigma)$, respectively. This is to be compared with Theorem 4.2.1, which shows that $\min(c, c')$ is a natural upper bound for the output size of such algorithms.

For solving Problem (2), we obtain slightly better complexity estimates.

Theorem 4.2.3. *Suppose that the matrix* $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ *and polynomials* $\boldsymbol{G} = (g_1, \ldots, g_s)$ *in* $\mathbb{K}[x_1, \ldots, x_n]$ *are given by a straight-line program of length* σ*. Assume that* $\deg(g_1), \ldots, \deg(g_s)$*, as well as* $\operatorname{cdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{cdeg}(\boldsymbol{F}, q)$ *and* $\operatorname{rdeg}(\boldsymbol{F}, 1), \ldots, \operatorname{rdeg}(\boldsymbol{F}, p)$ *are all at least equal to* 1*.*

Then, there exist randomized algorithms that solve Problem (2) *in either*

$$O^{\sim}\left(\binom{q}{p} ce\big(\sigma + q\delta + \gamma\big)\right)$$

or

$$O^{\sim}\left(\binom{q}{p} c'e'\big(\sigma + p\alpha + \gamma\big)\right)$$

operations in $\mathbb{K}$*, all notations being as in Theorem* 4.2.2*.*

The difference in the runtimes for Problem (1) and Problem (2) comes from the fact that we need an algorithm which takes as input a system and a point in the zero-set of this system, and decides whether this point is isolated. The detailed description of this algorithm is given in Section 5.1.

In Problems (1) and (2) we consider the row-degree and column-degree cases. However when the polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ and entries of $\boldsymbol{F}$ are sparse, we study only the column-support case. The row-support case is left for future work.

For $1 \leq i \leq s$, let $\mathcal{A}_i \subset \mathbb{N}^n$ denote the support of g_i, to which we add the origin $\mathbf{0} \in \mathbb{N}^n$. For $1 \leq j \leq q$, let $\mathcal{B}_j \subset \mathbb{N}^n$ be the union of the supports of the polynomials in the j-th column of $\boldsymbol{F}$, to which we add $\mathbf{0}$ as well. For $1 \leq i \leq s$ and $1 \leq j \leq q$, we let $\mathcal{C}_i$ and $\mathcal{D}_j$ be the convex hulls of respectively $\mathcal{A}_i$ and $\mathcal{B}_j$. Our next result gives the complexity to solve Problem (3) as follows (see Theorem 7.1.10 below for a precise statement).

Theorem 4.2.4. *Let* $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ *be a matrix with entries being sparse polynomials and* $\boldsymbol{G} = (g_1, \ldots, g_s)$ *in* $\mathbb{K}[x_1, \ldots, x_n]$ *be a sequence of sparse polynomials.*

Then, there exist a randomized algorithm that solves Problem (3)*, with the runtime is polynomial in* χ *and the degree of the homotopy curve, where*

$$\chi = \sum_{\boldsymbol{i} \subset \{1, \ldots, q\}^{n-s}} \mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_s, \mathcal{D}_{i_1}, \ldots, \mathcal{D}_{i_{n-s}}).$$

Moreover, there are at most χ *isolated points, counted with multiplicities, in* $V_p(\boldsymbol{F}, \boldsymbol{G})$*.*

Example 4.2.2. Consider the case when $s = 1, p = 2, q = 3$, and $n = 3$. Let $\boldsymbol{F} \in \mathbb{Q}[x_1, x_2, x_3]^{2 \times 3}$ be

$$\begin{pmatrix} 76x_1^3 + 123x_1^2 + 8x_1x_2 + 140x_1 - 193x_2 - 163x_3 - 1 & 4x_1^2 - 193x_1 - 64x_2 - 111 & -163x_1 + 251 \\ -92x_1^3 + 30x_1^2 + 310x_1x_2 + 90x_1 - 62x_3 + 60 & 155x_1^2 - 346x_2 - 78 & -62x_1 - 86 \end{pmatrix}.$$

and $\boldsymbol{G} = (-23x_1^4 + 10x_1^3 + 155x_1^2x_2 + 45x_1^2 - 62x_1x_3 - 173x_2^2 + 60x_1 - 78x_2 - 86x_3 - 93)$ in $\mathbb{Q}[x_1, x_2, x_3]$. Then

$$\begin{aligned}
\mathcal{A}_1 &= \{(4,0,0),(3,0,0),(2,1,0),(2,0,0),(1,0,1),(0,2,0),(1,0,0),(0,1,0),(0,0,1),(0,0,0)\},\\
\mathcal{B}_1 &= \{(3,0,0),(2,0,0),(1,1,0),(1,0,0),(0,1,0),(0,0,1),(0,0,0)\},\\
\mathcal{B}_2 &= \{(2,0,0),(1,0,0),(0,1,0),(0,0,0)\},\\
\mathcal{B}_3 &= \{(1,0,0),(0,0,0)\}.
\end{aligned}$$

The convex hulls of $\mathcal{A}_1$ and $(\mathcal{B}_i)_{1\le i\le 3}$ are respectively $\mathcal{C}_1 = \{(4,0,0),(2,1,0),(0,2,0),(0,0,1),(1,0,1),(0,0,0)\}$, $\mathcal{D}_1 = \{(3,0,0),(1,1,0),(0,1,0),(0,0,1),(0,0,0)\}$, $\mathcal{D}_2 = \{(2,0,0),(0,1,0),(0,0,0)\}$, and $\mathcal{D}_3 = \mathcal{B}_3$. Then

$$\mathsf{MV}(\mathcal{C}_1,\mathcal{D}_1,\mathcal{D}_2) = 4,\ \mathsf{MV}(\mathcal{C}_1,\mathcal{D}_1,\mathcal{D}_3) = 2,\ \text{and } \mathsf{MV}(\mathcal{C}_1,\mathcal{D}_2,\mathcal{D}_3) = 1,$$

and so the number of isolated points of $V_3(\boldsymbol{F},\boldsymbol{G})$ is at most $\chi = 7$.

On the other hand, if we use our result from Theorem 4.2.1, we get a bound $\min(c,c') = 44$ for the number of isolated points of $V_2(\boldsymbol{F},\boldsymbol{G})$ with

$$c = 4\cdot\eta_2(3,2,1) = 44 \text{ and } c' = 4\cdot h_2(3,3) = 108.$$

Therefore, using χ gives a sharp bound for the number of isolated points of $V_2(\boldsymbol{F},\boldsymbol{G})$ in this example.

Finally, our last result is to give the complexity to describe the isolated points of $V_p(\boldsymbol{F},\boldsymbol{G})$ when polynomials $\boldsymbol{G}$ and all entries of $\boldsymbol{F}$ are in some weighted polynomial rings. As in the sparse case, we study only weighted column-degree case and weighted row-degree case is left for future work. For this purpose, for $1 \le i \le q$, we define $\mathrm{wcdeg}(\boldsymbol{F}, j)$ for the weighted degree of the j-th column of $\boldsymbol{F}$, that is, $\mathrm{wcdeg}(\boldsymbol{F}, j) = \max(\mathrm{wdeg}(f_{i,j}))_{1\le i\le p}$. Our result is stated as follows (see Theorem 7.2.2 for a precise statement).

Theorem 4.2.5. *Let $\boldsymbol{w} = (w_1,\ldots,w_n)$ in $\mathbb{N}_{\ge 1}$ and $\mathbb{K}[x_1,\ldots,x_n]$ be a polynomial ring of weights $\boldsymbol{w}$. Suppose that the matrix $\boldsymbol{F} \in \mathbb{K}[x_1,\ldots,x_n]^{p\times q}$ of weighted column degrees $(\delta_1,\ldots,\delta_q)$ and polynomials $\boldsymbol{G} = (g_1,\ldots,g_s)$ of weighted degrees $(\gamma_1,\ldots,\gamma_s)$.*

Then, there exists a randomized algorithm that solves Problem (4) with the runtime is polynomial in $\tilde{c}$ and the degree of the homotopy curve $\tilde{e}$, where

$$\begin{aligned}
\tilde{c} &= \frac{\gamma_1\cdots\gamma_s\cdot\eta_{n-s}(\delta_1,\ldots\delta_q)}{\prod_{i=1}^n w_i} \text{ and}\\
\tilde{e} &= \max(w_1,\ldots,w_n)\cdot\frac{(\gamma_1+1)\cdots(\gamma_s+1)\cdot\eta_{n-s}(\delta_1+1,\ldots\delta_q+1)}{\prod_{i=1}^n w_i}.
\end{aligned}$$

Moreover, the sum of the multiplicities of the isolated points in $V_p(\boldsymbol{F},\boldsymbol{G})$ is at most $\tilde{c}$.

Example 4.2.3. Consider the case when $s = 1, p = 2, q = 3$, and $n = 3$. $\boldsymbol{F} \in \mathbb{Q}[x_1, x_2, x_3]^{2\times 3}$ and $\boldsymbol{G}$ in $\mathbb{Q}[x_1, x_2, x_3]$ be defined as in Example 4.2.2 with $\mathrm{wdeg}(x_1) = 1$, $\mathrm{wdeg}(x_2) = 2$, and $\mathrm{wdeg}(x_3) = 3$. Then $\mathrm{wdeg}(\boldsymbol{G}) = (4)$ and the weighted column degrees of $\boldsymbol{F}$ are

$$\mathrm{wcdeg}(\boldsymbol{F}, i) = i \text{ for } 1 \leq i \leq 3.$$

Then $\tilde{c} = \frac{4\cdot\eta_2(3,2,1)}{3.2.1} = 22/3$ and so the number of isolated points of $V_2(\boldsymbol{F}, \boldsymbol{G})$ is at most 7, which is coincident with the bound χ in Example 4.2.2.

Again, if we use the bounds from Theorem 4.2.1, we obtain a bound $\min(c, c') = 44$ for the number of isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$, which is not considered as a sharp bound. We remark that, in general, $\tilde{c}$ and χ are not coincident.

4.3 Roadmap of algorithms

To this end, we fix an ordering $\succ$ on the p-minors of $p \times q$ matrices and set $m = s + \binom{q}{p}$. We start with $\boldsymbol{F}$ and $\boldsymbol{G}$ as above and build the equations $\boldsymbol{C} = (c_1, \ldots, c_s, \ldots c_m)$ where $(c_1, \ldots, c_s) = (g_1, \ldots, g_s)$ and $(c_{s+1}, \ldots, c_m)$ are the p-minors of $\boldsymbol{F}$, following the order $\succ$.

Example 4.3.1. Throughout the part, we will consider the following example, with $\mathbb{K} = \mathbb{Q}$, $n = 2$, $s = 0$, $p = 2$ and $q = 3$ (so $n = q - p + s + 1$), and we let $\boldsymbol{F} \in \mathbb{K}[x_1, x_2]^{2\times 3}$ be given by

$$\boldsymbol{F} = \begin{bmatrix} x_1 + x_2 - 1 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix}.$$

The maximal minors $\boldsymbol{C} = M_2(\boldsymbol{F})$ are

$$\begin{aligned} c_1 &= -7x_1^3 - 38x_1^2x_2 - 7x_1^2 - 20x_1x_2^2 - 6x_1x_2 + 20x_1 + 5x_2^3 + 2x_2^2 + 16x_2 + 5, \\ c_2 &= x_1^3 - 3x_1^2x_2 - 11x_1^2 - 13x_1x_2^2 - 97x_1x_2 - 26x_1 - 10x_2^2 + 10x_2, \text{ and} \\ c_3 &= x_1^3 + 4x_1^2x_2 - 3x_1^2 - 37x_1x_2 - 13x_1 - 5x_2^3 - 52x_2^2 - 36x_2 - 5. \end{aligned}$$

As a preliminary, we will need an algorithm which takes as input polynomials $\boldsymbol{C}$ and a point $\boldsymbol{x}$ in the zero-set of $\boldsymbol{C}$, and which decides whether $\boldsymbol{x}$ is an isolated point of $V(\boldsymbol{C})$ (this will be used to solve Problem (1)). When a bound μ is known on the multiplicity of $\boldsymbol{x}$ as a root of $\boldsymbol{C}$, it becomes possible to solve this problem in time polynomial in the number of equations m, the number of variables n, the bound μ, and the complexity of evaluation σ of $\boldsymbol{C}$. This is detailed in Section 5.1, where we explain how to modify an algorithm by Mourrain [142] and adapt it to our context.

Example 4.3.2. In Example 4.3.1, the maximal minors $\boldsymbol{C} = M_2(\boldsymbol{F})$ generate a radical ideal of dimension zero, so Problems (1) and (2) admit the same answer. There are 7

solutions, which are described by means of the univariate representation $\mathscr{R} = ((q, v_1, v_2), \lambda)$, with

$$q = y^7 + \frac{5249}{285}y^6 + \frac{5899}{76}y^5 - \frac{32593}{950}y^4 - \frac{719401}{5700}y^3 - \frac{302473}{5700}y^2 - \frac{1243}{475}y + \frac{379}{1140},$$
$$v_1 = -\frac{461}{114}y^6 - \frac{39047}{380}y^5 - \frac{2431807}{2850}y^4 - \frac{87697}{76}y^3 - \frac{560363}{1900}y^2 + \frac{64121}{570}y + \frac{1341}{76},$$
$$v_2 = -\frac{5249}{285}y^6 - \frac{5899}{38}y^5 + \frac{97779}{950}y^4 + \frac{719401}{1425}y^3 + \frac{302473}{1140}y^2 + \frac{7458}{475}y - \frac{2653}{1140},$$

and $\lambda = x_2$. The coordinates of the solutions are the values taken by $(v_1/q', v_2/q')$ at the roots of q.

In our example, we have no polynomials $\boldsymbol{G}$. The column and row degrees of $\boldsymbol{F}$ are

$$(\mathrm{cdeg}(\boldsymbol{F}, 1), \mathrm{cdeg}(\boldsymbol{F}, 2), \mathrm{cdeg}(\boldsymbol{F}, 3)) = (2, 2, 2) \text{ and } (\mathrm{rdeg}(\boldsymbol{F}, 1), \mathrm{rdeg}(\boldsymbol{F}, 2)) = (1, 2).$$

Using Theorem 4.2.1, the column degree bound is $c = \eta_2(2, 2, 2) = 12$, the row degree bound is $c' = h_2(1, 2) = 7$. The latter is sharp and it can be used for the bound μ we mentioned above.

In order to compute the isolated points, or the simple points, of $V(\boldsymbol{C})$, we work with a deformation of these equations. We let t be a new variable, and we define polynomials $\boldsymbol{V} = (v_1, \ldots, v_s)$ of the form

$$\boldsymbol{V} = (1 - t) \cdot \boldsymbol{M} + t \cdot \boldsymbol{G} \in \mathbb{K}[t, x_1, \ldots, x_n]^s, \tag{4.1}$$

that connect certain polynomials $\boldsymbol{M} = (m_1, \ldots, m_s)$ to the target system $\boldsymbol{G}$, together with the matrix

$$\boldsymbol{U} = (1 - t) \cdot \boldsymbol{L} + t \cdot \boldsymbol{F} \in \mathbb{K}[t, x_1, \ldots, x_n]^{p \times q} \tag{4.2}$$

that connects a suitable start matrix $\boldsymbol{L}$ to the target matrix $\boldsymbol{F}$.

- The start system $\boldsymbol{A} = (a_1, \ldots, a_s, \ldots, a_m)$ in $\mathbb{K}[x_1, \ldots, x_n]$ will be defined by taking $(a_1, \ldots, a_s) = (m_1, \ldots, m_s)$, and by letting $(a_{s+1}, \ldots, a_m)$ be the p-minors of $\boldsymbol{L}$ following the ordering $\succ$.
- The parametric system $\boldsymbol{B} = (b_1, \ldots, b_s, \ldots, b_m)$ in $\mathbb{K}[t, x_1, \ldots, x_n]$ will be defined by taking $(b_1, \ldots, b_s) = (v_1, \ldots, v_s)$, and by letting $(b_{s+1}, \ldots, b_m)$ be the p-minors of $\boldsymbol{U}$ following the ordering $\succ$.

In particular, setting $t = 0$ in $\boldsymbol{B}$ gives us $\boldsymbol{A}$, and setting $t = 1$ in $\boldsymbol{B}$ recovers $\boldsymbol{C}$.

In Chapter 5, we first prove some properties of the ideal generated by $\boldsymbol{B}$, independent of the choices of $\boldsymbol{L}$ and $\boldsymbol{M}$. We then give symbolic homotopy algorithms which take as input the sequence of polynomials $\boldsymbol{B}$, together with a description of $V(\boldsymbol{A})$ (under certain regularity assumptions), and computes a zero-dimensional parametrization of either the

isolated solutions, or the simple solutions of $\boldsymbol{C}$. The complexity of these algorithms depend on the degree of the ideal $\boldsymbol{C}$ and the degree of the homotopy curve $\boldsymbol{B}$ (the number of steps we perform).

As we have seen in Section 3.7, start systems play an important role in symbolic homotopy algorithms with these systems being easy to solve. We will specify how to define polynomials $\boldsymbol{M}$ and matrix $\boldsymbol{L}$, and then how to find the solutions of $\boldsymbol{A} = 0$. The main difficulty lies in the definition of a matrix $\boldsymbol{L}$ that will respect either the column-degree or the row-degree of $\boldsymbol{F}$, while satisfying all assumptions needed for the algorithm of Chapter 5 and allowing us to solve the start system $\boldsymbol{A} = 0$ easily.

In the case of column-support, we will have to study how to build polynomials $\boldsymbol{M}$ and matrix $\boldsymbol{L}$ which exploits the sparsity of the input $(\boldsymbol{F}, \boldsymbol{G})$ and such that all assumptions needed for the algorithm of Chapter 5 are still satisfied. Note that weighted polynomial rings are particular cases of sparse domains. The only difference between column-support homotopy algorithms and weighted column-degree homotopy algorithm is in the latter, we use the weighted degree structure of the target system to build $\boldsymbol{M}$ and $\boldsymbol{L}$. We do not need to verify again all assumptions for the algorithm of Chapter 5. That is why we consider our weighted column-degree homotopy algorithm is an application of our column-support homotopy algorithm. Note also that we will use different algorithms to solve start systems in these two domains.

Chapter 5

Determinantal homotopy algorithm

In this chapter, we give symbolic homotopy algorithms for computing the isolated points or the simple points of the target system $\boldsymbol{C} = (c_1, \ldots, c_m)$ in $\mathbb{K}[\boldsymbol{X}]$ with $\boldsymbol{X} = (x_1, \ldots, x_n)$. Recall that $\boldsymbol{B} = (b_1, \ldots, b_m) \in \mathbb{K}[t, \boldsymbol{X}]$ is the homotopy system and $\boldsymbol{A} = (a_1, \ldots, a_m)$ in $\mathbb{K}[\boldsymbol{X}]$ is a start system with $\boldsymbol{B}(0, \boldsymbol{X}) = \boldsymbol{A}$ and $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$. We first need an algorithm to determine whether a point $\boldsymbol{x}$ in $V(\boldsymbol{C})$ is isolated.

5.1 A local dimension test

Let $\mathbb{L}$ be a field containing the field $\mathbb{K}$ with $\overline{\mathbb{L}}$ the algebraic closure of $\mathbb{L}$. Let $\boldsymbol{C}$ be a system of polynomials in $\mathbb{K}[\boldsymbol{X}]$ and $\boldsymbol{x}$ a point in $V(\boldsymbol{C}) \subset \overline{\mathbb{L}}^n$. In this section, we discuss how to decide if $\boldsymbol{x}$ is an isolated point of $V(\boldsymbol{C})$. The main result of this section is the following proposition.

Proposition 5.1.1. *Suppose that $\boldsymbol{C}$ is given by a straight-line program of length σ, and that we are given an integer μ such that either $\boldsymbol{x}$ is isolated in $V(\boldsymbol{C})$, with multiplicity at most μ with respect to the ideal $\langle \boldsymbol{C} \rangle$, or $\boldsymbol{x}$ belongs to a positive-dimensional component of $V(\boldsymbol{C})$. Then, we can decide whether $\boldsymbol{x}$ is an isolated point of $V(\boldsymbol{C})$ using*

$$O(n^4\mu^4 + n^2 m\mu^3 + n\sigma\mu^4) \subset (\mu\,\sigma\,m)^{O(1)}$$

operations in $\mathbb{L}$.

Bates et al. [23] give an algorithm to compute the dimension of $V(\boldsymbol{C})$ at $\boldsymbol{x}$, but its complexity is not known to us, as this algorithm relies on linear algebra with matrices of potentially large size which is not necessarily polynomial in μ, σ, and m. Indeed, we use an adaptation of a prior result by Mourrain [142], which allows us to control the size of matrices we handle. We only give detailed proofs for new ingredients that are specific to our context, a key difference being the cost analysis in the straight-line program model.

Mourrain's original result depends on the number of monomials appearing when we expand the polynomials $\boldsymbol{C}$, which would be too high for the applications we will make of this result. We remark that the assumption that $\mathbb{K}$, and then $\mathbb{L}$, have characteristic zero is needed for Mourrain's algorithm.

The rest of this section is devoted to prove Proposition 5.1.1. We assume henceforth that $\boldsymbol{x} = 0$. More generally, if $\boldsymbol{x} = (\alpha_1, \ldots, \alpha_n)$, we can replace $\boldsymbol{C}$ by the polynomials $\boldsymbol{C}' = \boldsymbol{C}(\boldsymbol{X} + \boldsymbol{x})$, which have complexity of evaluation $\sigma' = \sigma + n$ with n extra operations for computing $(x_i + \alpha_i)_{1 \leq i \leq n}$. We first need the following remark.

Lemma 5.1.2. *Let I be the zero-dimensional ideal $\langle I \rangle + \mathfrak{m}^{\mu+1}$, where $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$ is the maximal ideal at the origin. Then, 0 is isolated in $V(\boldsymbol{C})$ if and only if the multiplicity of I at the origin is at most μ.*

Proof. For a positive integer k, let $I_k = \langle I \rangle + \mathfrak{m}^k$ be a zero-dimensional ideal in $\mathbb{K}[\boldsymbol{X}]$, and let ν_k be the multiplicity of this ideal at the origin. The result in [23, Theorem 1] implies that the sequence $(\nu_k)_{k \geq 1}$ is non-decreasing, and that 0 is an isolated point in $V(\boldsymbol{C})$ if and only if there exists a positive integer k such that $\nu_k = \nu_{k+i}$ for all $i \geq 0$.

If 0 is isolated in $\boldsymbol{C}$, then by our assumption in Proposition 5.1.1, the multiplicity of 0 with respect to $\langle \boldsymbol{C} \rangle$ is at most μ, that is, the multiplicity of the origin with respect to I can not be larger than μ. Otherwise, by the result above, the inequality $\nu_{k+1} > \nu_k$ holds for all $k \geq 1$. This implies that $\nu_k \geq k$, for all $k \geq 1$, since $\nu_1 = 1$. In particular, the multiplicity of I at the origin, which is ν_{k+1}, is at least $\mu + 1$. □

Lemma 5.1.2 implies that we are left with deciding whether the multiplicity of I at the origin is at most μ; we remark that, since I is $\mathfrak{m}$-primary, this multiplicity equals the dimension of $\mathbb{L}[\boldsymbol{X}]/I$. Let $I^\perp$ be the diagonal of I, that is,

$$I^\perp = \{\beta : \mathbb{L}[\boldsymbol{X}] \to \mathbb{L} \text{ such that } \beta(f) = 0 \text{ for all } f \in I\},$$

the set of all $\mathbb{L}$-linear forms $\mathbb{L}[\boldsymbol{X}] \to \mathbb{L}$ that vanish on I. The $\mathbb{L}$-vector space $I^\perp$ is naturally identified with the dual of $\mathbb{L}[\boldsymbol{X}]/I$, so, its dimension is equal the multiplicity of I at the origin. Therefore, it is sufficient to do the computation of the orthogonal $I^\perp$; we do this by following and slightly modifying Mourrain's algorithm. We do not need to give all details of the algorithm, let alone proof of correctness; we just mention the key ingredients for the cost analysis in our straight-line program setting.

Mourrain's algorithm represents the elements in $I^\perp$ by means of *matrices multiplication*. An important feature of $I^\perp$ is that it admits the structure of an $\mathbb{L}[\boldsymbol{X}]$-module. For $k = 1, \ldots, n$ and β in $I^\perp$, the $\mathbb{L}$-linear form $x_k \cdot \beta : f \mapsto \beta(x_k f)$ is still in $I^\perp$. In particular, if $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_d)$ is an $\mathbb{L}$-basis of $I^\perp$, then for $k = 1, \ldots, n$ and all $i \in \{1, \ldots, d\}$, $x_k \cdot \beta_i$ is a linear combination of $\boldsymbol{\beta}$. Mourrain's algorithm computes a basis $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_d)$ with the following features:

- for $1 \leq i \leq d$ and $1 \leq k \leq n$, we have $x_k \cdot \beta_i = \sum_{1 \leq j < i} \lambda_{i,j}^{(k)} \beta_j$ (hence $\lambda_{i,j}^{(k)}$ may be non-zero only for $j < i$);
- β_1 is the evaluation at 0, $\beta_1(f) = f(0)$ for all f in I;
- for $2 \leq i \leq d$, $\beta_i(1) = 0$.

The following lemma shows that the coefficients $(\lambda_{i,j}^{(k)})$ are sufficient to evaluate the linear forms β_i at any polynomial f in $\mathbb{L}[\boldsymbol{X}]$. More precisely, for any $1 \leq s \leq d$, knowing only values of $(\lambda_{i,j}^{(k)})$ for $j < i \leq s$ allows us compute the evaluations of $\beta_1, \ldots, \beta_s$ at any polynomial f in $\mathbb{L}[\boldsymbol{X}]$. The following lemma follows the description of the matrices $\boldsymbol{M}_{k,s}$; the (rather straightforward) complexity analysis in the straight-line program model is new.

Lemma 5.1.3. *Let s be in $\{1, \ldots, d\}$, and suppose that the coefficients $(\lambda_{i,j}^{(k)})_{1 \leq i \leq s, 1 \leq j < i}$ are known for $k = 1, \ldots, n$. Given a straight-line program Γ of length σ that computes polynomials $\boldsymbol{h} = (h_1, \ldots, h_r)$ in $\mathbb{L}[\boldsymbol{X}]$, one can compute $\beta_i(h_u)$, for all $i = 1, \ldots, s$ and $u = 1, \ldots, r$, using $O(s^3\sigma)$ operations in $\mathbb{L}$.*

Proof. For h in $\mathbb{L}[\boldsymbol{X}]$ and $k = 1, \ldots, n$, we have

$$\begin{bmatrix} \beta_1(x_k h) \\ \vdots \\ \beta_s(x_k h) \end{bmatrix} = \boldsymbol{M}_{k,s} \begin{bmatrix} \beta_1(h) \\ \vdots \\ \beta_s(h) \end{bmatrix}, \text{ with } \boldsymbol{M}_{k,s} = \begin{bmatrix} \lambda_{1,1}^{(k)} & \cdots & \lambda_{s,1}^{(k)} \\ \vdots & & \vdots \\ \lambda_{1,s}^{(k)} & \cdots & \lambda_{s,s}^{(k)} \end{bmatrix}.$$

We remark that the matrices $\boldsymbol{M}_{k,s}$ all commute with each others. Indeed, for k, k' in $\{1, \ldots, n\}$, by using basic linear algebra computations, one can verify that

$$\boldsymbol{M}_{k',s} \begin{bmatrix} \beta_1(x_k h) \\ \vdots \\ \beta_s(x_k h) \end{bmatrix} = \boldsymbol{M}_{k,s} \begin{bmatrix} \beta_1(x_{k'} h) \\ \vdots \\ \beta_s(x_{k'} h) \end{bmatrix};$$

together with the relation above, we can deduce that

$$(\boldsymbol{M}_{k,s}\boldsymbol{M}_{k',s} - \boldsymbol{M}_{k',s}\boldsymbol{M}_{k,s}) \begin{bmatrix} \beta_1(h) \\ \vdots \\ \beta_s(h) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Moreover, since the linear forms $\beta_1, \ldots, \beta_s$ are linearly independent, then all rows of $\Delta_{k,k',s} := \boldsymbol{M}_{k,s}\boldsymbol{M}_{k',s} - \boldsymbol{M}_{k',s}\boldsymbol{M}_{k,s}$ must be zero, which means $\boldsymbol{M}_{k,s}\boldsymbol{M}_{k',s} = \boldsymbol{M}_{k',s}\boldsymbol{M}_{k,s}$ for any k, k'.

Then, for any polynomial h in $\mathbb{L}[X]$, the following equality holds:

$$\begin{bmatrix} \beta_1(h) \\ \vdots \\ \beta_s(h) \end{bmatrix} = h(\boldsymbol{M}_{1,s}, \ldots, \boldsymbol{M}_{n,s}) \begin{bmatrix} \beta_1(1) \\ \vdots \\ \beta_s(1) \end{bmatrix}.$$

On the other hand, our assumptions imply that $(\beta_1(1), \ldots, \beta_s(1))$ is $(1, 0, \ldots, 0)$. Therefore, to conclude, we use the fact that the evaluations of $(h_1, \ldots, h_r)$ at $(\boldsymbol{M}_{1,s}, \ldots, \boldsymbol{M}_{n,s})$ can be computed using a straight-line program performing $O(s^3\sigma)$ operations in $\mathbb{K}$. □

Mourrain's algorithm proceeds in an iterative manner, starting from $\boldsymbol{\beta}^{(1)} = (\beta_1)$ (and setting $e_1 = 1$), and computing successively $\boldsymbol{\beta}^{(2)} = (\beta_{e_1+1}, \ldots, \beta_{e_2})$, $\boldsymbol{\beta}^{(3)} = (\beta_{e_2+1}, \ldots, \beta_{e_3})$, $\ldots$, for some integers $e_1 \leq e_2 \leq e_3 \leq \cdots$. The algorithm stops when $e_{\ell+1} = e_\ell$, in which case $\beta_1, \ldots, \beta_{e_\ell}$ is an $\mathbb{L}$-basis of $I^\perp$, and $e_\ell = d$. In our case, we are not interested in computing this multiplicity, but only in deciding whether it is less than or equal to the parameter μ; we do it as the follows.

Assume that we have computed $\boldsymbol{\beta}^{(1)}, \boldsymbol{\beta}^{(2)}, \ldots, \boldsymbol{\beta}^{(\ell)}$, together with the corresponding integers $e_1, e_2, \ldots, e_\ell$, with $e_1 < \cdots < e_\ell \leq \mu$. We compute $\boldsymbol{\beta}^{(\ell+1)}$ and $e_{\ell+1}$, and continue according to the following:

- if $e_{\ell+1} = e_\ell$, we conclude that the multiplicity d of I at the origin is $e_\ell \leq \mu$; we stop the algorithm;
- if $e_{\ell+1} > \mu$, we conclude that this multiplicity is greater than μ; we stop the algorithm;
- else, when $e_\ell < e_{\ell+1} \leq \mu$, we do $(\ell + 2)$-th loop.

Since the sequence $(e_\ell)_{\ell \geq 1}$ is increasing with $e_1 = 1$, then it satisfies $e_\ell \geq \ell$. Then, whenever we enter the loop ℓ, we have $\ell \leq \mu$. It remains to explain how to compute $\boldsymbol{\beta}^{(\ell+1)}$ from $(\boldsymbol{\beta}^{(1)}, \boldsymbol{\beta}^{(2)}, \ldots, \boldsymbol{\beta}^{(\ell)}) = (\beta_1, \ldots, \beta_{e_\ell})$.

As per our description above, at any step of the algorithm, $\beta_1, \ldots, \beta_{e_\ell}$ are represented by means of the coefficients $\lambda_{i,j}^{(k)}$, for $0 \leq j < i \leq e_\ell$ and $1 \leq k \leq n$. At step ℓ, Mourrain's algorithm solves a homogeneous linear system T_ℓ with $n(n-1)e_\ell/2 + m'$ equations and ne_ℓ unknowns, where m' is the number of generators of the ideal $I = \langle \boldsymbol{C} \rangle + \mathfrak{m}^{\mu+1}$. Remark that m' is not polynomial in μ and n, so the size of T_ℓ is *a prior* too large to fit our cost bound; we will explain below how to resolve this issue in the straight-line program model.

The null dimension of this linear system gives us the cardinality $e_{\ell+1} - e_\ell$ of $\boldsymbol{\beta}^{(\ell+1)}$. The coordinates of the $e_{\ell+1} - e_\ell$ vectors in a nullspace basis are precisely the coefficients $(\lambda_{i,j}^{(k)})_{e_\ell+1 \leq i \leq e_{\ell+1}, 1 \leq j \leq e_\ell}$ for $k = 1, \ldots, n$. Note that $\lambda_{i,j}^{(k)} = 0$ for $j = e_\ell + 1, \ldots, i - 1$. For all $\ell \geq 2$, all linear forms β in $\boldsymbol{\beta}^{(\ell)}$ are such that for all k in $\{1, \ldots, n\}$, $x_k \cdot \beta$ belongs to the span of $\boldsymbol{\beta}^{(1)}, \ldots, \boldsymbol{\beta}^{(\ell-1)}$. In particular, a quick induction shows that all linear forms in $\boldsymbol{\beta}^{(1)}, \ldots, \boldsymbol{\beta}^{(\ell)}$ vanish on all monomials of degree at least ℓ.

There remains the question of setting up the system T_ℓ. For k in $\{1, \ldots, n\}$ and an $\mathbb{L}$-linear form β, we denote by $x_k^{-1} \cdot \beta$ the $\mathbb{L}$-linear form defined by $\mathbb{L}$-linearity as follows:

- $(x_k^{-1} \cdot \beta)(x_k f) = \beta(f)$ for any monomial f in $\mathbb{L}[\boldsymbol{X}]$,
- $(x_k^{-1} \cdot \beta)(f) = 0$ if $f \in \mathbb{L}[\boldsymbol{X}]$ is a monomial which does not depend on x_k.

In other words, $(x_k^{-1} \cdot \beta)(f) = \beta(\delta_k(f))$ holds for all f, where $\delta_k : \mathbb{L}[\boldsymbol{X}] \to \mathbb{L}[\boldsymbol{X}]$ is the k-th divided difference operator

$$f \mapsto \frac{f(x_1, \ldots, x_n) - f(x_1, \ldots, x_{k-1}, 0, x_{k+1}, \ldots, x_n)}{x_k}.$$

One can verify that, $x_k \cdot (x_k^{-1} \cdot \beta)$ is equal to β. This being said, we can then describe what the entries of T_ℓ are:

- the first $n(n-1)e_\ell/2$ equations involve only the coefficients $\lambda_{i,j}^{(k)}$ previously computed (we refer to [142, Section 4.4] for details of how exactly these entries are distributed in T_ℓ, as we do not need such details here).
- each of the other m' equations has coefficient vector

  $$v_f = \Big((x_k^{-1} \cdot \beta_1)(f(x_1, \ldots, x_k, 0, \ldots, 0)), \ldots, (x_k^{-1} \cdot \beta_{e_\ell})(f(x_1, \ldots, x_k, 0, \ldots, 0)) \Big)_{1 \le k \le n},$$

  where f is a generator of $I = \langle \boldsymbol{C} \rangle + \mathfrak{m}^{\mu+1}$.

We claim that only those equations corresponding to generators $c_1, \ldots, c_m$ of the input system $\boldsymbol{C}$ are useful, as all others are identically zero.

Indeed, we pointed out above that any linear form β_i in $\beta_1, \ldots, \beta_{e_\ell}$ vanishes on all monomials of degree at least ℓ; in addition, as we saw that $\ell \le \mu$, all of these β_i vanish on monomials of degree μ. This implies that $x_k^{-1} \cdot \beta$ vanishes on monomials of degree $\mu + 1$. The generators f of $\mathfrak{m}^{\mu+1}$ have degree $\mu + 1$, and for any such f, $f(x_1, \ldots, x_k, 0, \ldots, 0)$ is either zero, or of degree $\mu + 1$ as well. Hence, for any k, β_i in $\beta_1, \ldots, \beta_{e_\ell}$ and f as above, $(x_k^{-1} \cdot \beta_i)(f(x_1, \ldots, x_k, 0, \ldots, 0))$ vanishes. This implies that the vector v_f is identically zero for such an f, and that the corresponding equation can be discarded.

In summary, we have to compute the values

$$(x_k^{-1} \cdot \beta_i)(c_j(x_1, \ldots, x_k, 0, \ldots, 0)),$$

for $k = 1, \ldots, n$, $i = 1, \ldots, e_\ell$ and $j = 1, \ldots, m$. Fixing k in $\{1, \ldots, n\}$, we let $\boldsymbol{C}_k = (c_{j,k})_{1 \le j \le m}$, where $c_{j,k}$ is the polynomial $c_j(x_1, \ldots, x_k, 0, \ldots, 0)$; note that the system $\boldsymbol{C}_k$ can be computed by a straight-line program of length $\sigma' = \sigma + n$. Then, applying the following lemma with $s = e_\ell \le \mu$ and $\boldsymbol{h} = \boldsymbol{C}_k$, we deduce that the values $(x_k^{-1} \cdot \beta_i)(c_j(x_1, \ldots, x_k, 0, \ldots, 0))$, for k fixed, can be computed in time $O(\mu^3(\sigma + n))$.

Lemma 5.1.4. *Let s be in $1, \ldots, d$, and suppose that the coefficients $\lambda_{i,j}^{(k)}$ are known for $i = 1, \ldots, s$, $j = 0, \ldots, i-1$ and $k = 1, \ldots, n$. Given a straight-line program Γ of length σ that computes $\boldsymbol{h} = (h_1, \ldots, h_r)$ and given k in $\{1, \ldots, n\}$, one can compute $(x_k^{-1} \cdot \beta_i)(h_u)$, for all $i = 1, \ldots, s$ and $u = 1, \ldots, r$, using $O(s^3(\sigma + n))$ operations in $\mathbb{L}$.*

Proof. In view of the formula $(x_k^{-1} \cdot \beta)(f) = \beta(\delta_k(f))$, and of Lemma 5.1.3, it is sufficient to prove the existence of a straight-line program of length $O(\sigma + n)$ that computes $(\delta_k(h_1), \ldots, \delta_k(h_r))$.

To do this, we replace all polynomials $\gamma_{-n+1}, \ldots, \gamma_\sigma$ computed by Γ by terms $\eta_{-n+1}, \ldots, \eta_\sigma$ and $\nu_{-n+1}, \ldots, \nu_\sigma$, with

$$\eta_\ell = \gamma_\ell(x_1, \ldots, x_{k-1}, 0, x_{k+1}, \ldots, x_n)$$

and ν_ℓ in $\mathbb{L}[\boldsymbol{X}]$ such that $\gamma_\ell = \eta_\ell + x_k\nu_\ell$ holds for all ℓ. In particular, one has $\nu_\ell = \delta_k(\gamma_\ell)$ for $\ell = -n+1, \ldots, \sigma$. To compute η_ℓ and ν_ℓ, assuming all previous $\eta_{\ell'}$ and $\nu_{\ell'}$ are known, we proceed as follows:

- if $\gamma_\ell = x_k$, we set $\eta_\ell = 0$ and $\nu_\ell = 1$;
- if $\gamma_\ell = x_{k'}$, with $k' \neq k$, we set $\eta_\ell = x_{k'}$ and $\nu_\ell = 0$;
- if $\gamma_\ell = d_\ell$, with $d_\ell \in \mathbb{L}$, then we set $\eta_\ell = d_\ell$ and $\nu_\ell = 0$;
- if $\gamma_\ell = \gamma_{a_\ell} \pm \gamma_{b_\ell}$, for some indices $a_\ell, b_\ell < \ell$, then we set $\eta_\ell = \eta_{a_\ell} \pm \eta_{b_\ell}$ and $\nu_\ell = \nu_{a_\ell} \pm \nu_{b_\ell}$;
- if $\gamma_\ell = \gamma_{a_\ell}\gamma_{b_\ell}$, for some indices $a_\ell, b_\ell < \ell$, then we set $\eta_\ell = \eta_{a_\ell}\eta_{b_\ell}$ and

$$\nu_\ell = \eta_{a_\ell}\nu_{b_\ell} + \nu_{a_\ell}\eta_{b_\ell} + x_k\nu_{a_\ell}\nu_{b_\ell}.$$

One verifies that in all cases, the relation $\gamma_\ell = \eta_\ell + x_k\nu_\ell$ still holds. Since the previous construction allows us to compute η_ℓ and ν_ℓ in $O(1)$ operations from the knowledge of all previous $\eta_{\ell'}$ and $\nu_{\ell'}$, we deduce that all η_ℓ and ν_ℓ, for $\ell = -n+1, \ldots, \sigma$, can be computed by a straight-line program of length $O(\sigma + n)$. □

Taking all values of k, from 1 to n, into account, we see that we can compute all entries we need to set up the linear system T_ℓ using $O(\mu^3 n(\sigma + n))$ operations in $\mathbb{L}$. After discarding the useless equations described above, the numbers of equations and unknowns in the system T_ℓ are respectively at most $n^2\mu + m$ and $n\mu$. This implies that we can find a null space basis, for instance, by using Gaussian elimination, of this system in time $O(n^2\mu^2(n^2\mu + m))$. Altogether, the time spent to find $\boldsymbol{\beta}^{(\ell+1)}$ from $(\boldsymbol{\beta}^{(1)}, \boldsymbol{\beta}^{(2)}, \ldots, \boldsymbol{\beta}^{(\ell)}) = (\beta_1, \ldots, \beta_{e_\ell})$ is $O(n^4\mu^3 + n^2 m\mu^2 + n\sigma\mu^3)$. Finally, since we saw that we do at most μ such loops, the cumulative time is $O(n^4\mu^4 + n^2 m\mu^3 + n\sigma\mu^4)$, and Proposition 5.1.1 is proved.

We close this section by discussing how to apply such a result in Proposition 5.1.1. The easiest way is to do so is when $\mathbb{L} = \mathbb{K}$ with $\boldsymbol{x}$ a point in the zero-set of a polynomial system in $\mathbb{K}[x_1, \ldots, x_n]$. In Subsection 5.2.3, we will apply it when $\mathbb{L}$ the fraction field of the integral ring $\mathbb{K}[y]/\langle w \rangle$, where y is a variable and $w \in \mathbb{K}[y]$ is an irreducible polynomial. In this setting, the coordinates of $\boldsymbol{x}$ are expressed through the evaluation of a polynomial in $\mathbb{K}[y]$ at one root of w. Classical arithmetic operation such as addition, subtraction and multiplication are performed modulo w; inverting a non-zero element in $\mathbb{K}[y]/\langle w \rangle$ boils down to applying the Extended Euclidean Algorithm (see e.g. [80]).

5.2 Symbolic homotopy algorithms

Let $\boldsymbol{C} = (c_1, \ldots, c_m)$ in $\mathbb{K}[\boldsymbol{X}]$ with $\boldsymbol{X} = (x_1, \ldots, x_n)$. In this section, we give algorithms to compute a zero-dimensional parametrization of the isolated/simple points of $V(\boldsymbol{C})$, assuming the existence of a suitable homotopy deformation $\boldsymbol{B}$ of $\boldsymbol{C}$. We can assume $m \geq n$, since otherwise there is no isolated point in $V(\boldsymbol{C})$. This assumption is trivial for determinantal systems since $m = s + \binom{q}{p}$ and $n = q - p + s + 1$ with $q \geq p$.

Let t be a new variable and consider polynomials $\boldsymbol{B} = (b_1, \ldots, b_m)$ in $\mathbb{K}[t, \boldsymbol{X}]$. For $\tau \in \overline{\mathbb{K}}$, we write $\boldsymbol{B}_{t=\tau} = \boldsymbol{B}(\tau, \boldsymbol{X}) \in \overline{\mathbb{K}}[\boldsymbol{X}]$. In particular, we assume that $\boldsymbol{B}_{t=1} = \boldsymbol{C}$ and $\boldsymbol{B}_{t=0} = \boldsymbol{A}$, a start system. We define the ideal $J = \langle \boldsymbol{B} \rangle \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]$.

5.2.1 Bounds on the number of isolated points

Our first result in this section is to give a precise description on the number of isolated solutions of $\boldsymbol{B}_{t=\tau} = 0$ for any τ in $\overline{\mathbb{K}}$.

Proposition 5.2.1. *Suppose that the following two conditions hold:*

B_1. *Any irreducible component of $V(J) \subset \overline{\mathbb{K}}^{n+1}$ has dimension at least one.*

B_2. *For any maximal ideal $\mathfrak{m} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]$, if the localization $J_{\mathfrak{m}} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$ has height n, then it is unmixed (that is, all associated primes have height n).*

Then there exists an integer c such that for all τ in $\overline{\mathbb{K}}$, the sum of the multiplicities of the isolated solutions of $\boldsymbol{B}_{t=\tau}$ is at most c.

An obvious example where B_1 and B_2 hold is when $m = n$. Then B_1 is Krull's theorem, and B_2 is Macaulay's unmixedness theorem in the Cohen-Macaulay ring $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$ [53, Corollary 18.14]. More generally, these properties hold when $\boldsymbol{B}$ is the sequence of p-minors of a $p \times q$ matrix with entries in $\mathbb{K}[t, \boldsymbol{X}]$, with $p \leq q$ and $n = q - p + 1$; we discuss this, and a slightly more general situation, in Section 5.3.

The rest of the section is dedicated to proving this proposition. In the core of the proof, we will give a precise characterization of the integer c mentioned in the proposition, although the statement given in the proposition will actually be enough for our later purposes.

Consider $J = Q_1 \cap \cdots \cap Q_r$ an irredundant primary decomposition of the ideal $J = \langle \boldsymbol{B} \rangle \subset \mathbb{K}[t, \boldsymbol{X}]$, and let $P_1, \ldots, P_r$ be the associated primes, that is, the respective radicals of $Q_1, \ldots, Q_r$. We assume that $P_1, \ldots, P_\ell$ are the minimal primes, for some $\ell \leq r$, so that $V(P_1), \ldots, V(P_\ell)$ are the (absolutely) irreducible components of $V(J) \subset \overline{\mathbb{K}}^{n+1}$. By B_1, these irreducible components have dimension at least one. Refining further, we assume that

$u \leq \ell$ is such that $V(P_1), \ldots, V(P_u)$ are the irreducible components of $V(J)$ of dimension one whose image by $\pi_t : (\tau, x_1, \ldots, x_n) \mapsto \tau$ is Zariski dense in $\overline{\mathbb{K}}$ (i.e. π_t is dominant).

Let us write $J = J' \cap J''$, with $J' = Q_1 \cap \cdots \cap Q_u$ and $J'' = Q_{u+1} \cap \cdots \cap Q_r$. We consider the Puiseux series field $\mathbf{S} = \overline{\mathbb{K}}\langle\langle t \rangle\rangle$ in t with coefficients in $\overline{\mathbb{K}}$. Since $\overline{\mathbb{K}}$ is algebraically closed and of characteristic zero, $\mathbf{S}$ is algebraically closed (actually, it is an algebraic closure of $\overline{\mathbb{K}}(t)$) and hence a perfect field. We consider the extension $\mathfrak{J}$ of J in $\mathbf{S}[\boldsymbol{X}]$, and similarly let $\mathfrak{J}'$ and $\mathfrak{J}''$ denote the extensions of J' and J'' in $\mathbf{S}[\boldsymbol{X}]$. Let us define

$$c = \dim_{\mathbf{S}}(\mathbf{S}[\boldsymbol{X}]/\mathfrak{J}').$$

Lemma 5.2.2. *Let τ be in $\overline{\mathbb{K}}$ and let $\boldsymbol{x} \in \overline{\mathbb{K}}^n$ be an isolated solution of the system $\boldsymbol{B}_{t=\tau}$. Then, $(\tau, \boldsymbol{x})$ belongs to $V(P_i)$ for at least one index i in $\{1, \ldots, u\}$, and does not belong to $V(P_i)$ for any index i in $\{u+1, \ldots, r\}$.*

Proof. Since $(\tau, \boldsymbol{x})$ is a solution of $\boldsymbol{B} = 0$, it belongs to at least one of $V(P_1), \ldots, V(P_r)$. It remains to show that $(\tau, \boldsymbol{x})$ does not belong to $V(P_i)$ for some index i in $\{u+1, \ldots, r\}$.

For indices $i \in \{u+1, \ldots, \ell\}$, these are those primary components with minimal associated primes P_i that either have dimension at least two, or have dimension one but whose image by π_t is a single point. In both cases, all irreducible components of the intersection $V(P_i) \cap V(t - \tau)$, for $u+1 \leq i \leq \ell$, have dimension at least one. On the other hand, since $\boldsymbol{x}$ is an isolated point in $V(\boldsymbol{B}_\tau)$, $(\tau, \boldsymbol{x})$ is isolated in $V(P_i) \cap V(t - \tau)$. Therefore, $(\tau, \boldsymbol{x})$ cannot belong to $V(P_i) \cap V(t - \tau)$ for any $i \in \{u+1, \ldots, \ell\}$.

It remains to show that $(\tau, \boldsymbol{x})$ does not belong to $V(P_i)$, for any of the embedded primes $P_{\ell+1}, \ldots, P_r$. We prove this by contradiction by assuming that $(\tau, \boldsymbol{x})$ is in $V(P_{i_1}), \ldots, V(P_{i_k})$ for some $\ell+1 \leq i_1 < \cdots < i_k \leq r$. Since $P_{i_1}, \ldots, P_{i_k}$ are embedded primes, $V(P_{i_1}), \ldots, V(P_{i_k})$ are contained in one of $V(P_1), \ldots, V(P_\ell)$. Further, all $V(P_1), \ldots, V(P_\ell)$ have dimension one, so $V(P_{i_1}), \ldots, V(P_{i_k})$ are zero-dimensional; then they are the point $\{(\tau, \boldsymbol{x})\}$. As a result, $V(P_{i_1}), \ldots, V(P_{i_k})$ equal $V(P_{i_1})$ which contradicts the irredundancy of our decomposition. Therefore, if $(\tau, \boldsymbol{x})$ belongs to $V(P_{\ell+1}), \ldots, V(P_r)$, it has to belong to at most one of those sets. Without loss of generality, let us assume $(\tau, \boldsymbol{x}) \in V(P_{\ell+1})$ and $(\tau, \boldsymbol{x}) \notin V(P_i)$ for $\ell + 1 < i \leq r$.

To summarize, $(\tau, \boldsymbol{x})$ belongs to $V(P_{\ell+1})$, together with $V(P_i)$ for some indices i $\{1, \ldots, u\}$, say $P_1, \ldots, P_\rho$, up to reordering, for some $\rho \geq 1$, and avoids all other associated primes. Let us localize the decomposition $J = Q_1 \cap \cdots \cap Q_r$ at $P_{\ell+1}$. By Proposition 3.1.12,

$$J_{P_{\ell+1}} = Q_{1P_{\ell+1}} \cap \cdots \cap Q_{\rho P_{\ell+1}} \cap Q_{\ell+1 P_{\ell+1}}$$

is an irredundant primary decomposition of the ideal $J_{P_{\ell+1}}$ in $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{P_{\ell+1}}$ with the minimal primes being $P_{1P_{\ell+1}}, \ldots, P_{\rho P_{\ell+1}}, P_{\ell+1 P_{\ell+1}}$.

By Corollary 4 p.24 in [135], for any prime $P_{iP_{\ell+1}}$ with $i = 1, \ldots, \rho$ or $i = \ell + 1$, the localization of $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{P_{\ell+1}}$ at $P_{iP_{\ell+1}}$ is $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{P_i}$. In particular, the height of $P_{iP_{\ell+1}}$ in

$\overline{\mathbb{K}}[t, \boldsymbol{X}]_{P_{\ell+1}}$ is equal to that of P_i in $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{P_i}$. Moreover, $\dim(V(P_i)) = 1$ for $i = 1, \ldots, \rho$ and $\dim(V(P_{\ell+1})) = 0$. Therefore, by Theorem 3.1.1, for $i = 1, \ldots, \rho$,

$$\text{height}(P_i) = (n+1) - \dim(V(P_i)) = n,$$

and

$$\text{height}(P_{\ell+1}) = (n+1) - \dim(V(P_{\ell+1})) = n+1.$$

This implies $\text{height}(P_{i\,P_{\ell+1}}) = n$ for $i = 1, \ldots, \rho$ and $\text{height}(P_{\ell+1\,P_{\ell+1}}) = n+1$. Since $\rho \geq 1$, then $J_{P_{\ell+1}}$ has height n. As a result, B_2 implies that $J_{P_{\ell+1}}$ is unmixed which is a contradiction. □

Remark 5.2.3. *The zero-set $V(J')$ is the union of all one-dimensional irreducible components of $V(J) = V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$ whose projection on the t-axis is dense. As a consequence, we will call it the* homotopy curve.

For τ in $\overline{\mathbb{K}}$, we denote by $J_{t=\tau} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]$ the ideal $J + \langle t - \tau \rangle$, and similarly for $J'_{t=\tau}$ and $J''_{t=\tau}$.

Lemma 5.2.4. *Let τ and $\boldsymbol{x}$ be as in Lemma 5.2.2. Then, the multiplicities of the ideals $J_{t=\tau}$ and $J'_{t=\tau}$ at $(\tau, \boldsymbol{x})$ are the same.*

Proof. Without loss of generality, assume that $\tau = 0 \in \overline{\mathbb{K}}$ and $\boldsymbol{x} = \boldsymbol{0} \in \overline{\mathbb{K}}^n$. We will see the equality $J = J' \cap J''$ which holds in $\overline{\mathbb{K}}[t, \boldsymbol{X}]$ in the formal power series $\overline{\mathbb{K}}[[t, \boldsymbol{X}]]$. Lemma 5.2.2 implies that there exists a polynomial in J'' that does not vanish at $(\tau, \boldsymbol{x})$. Then this polynomial is a unit in $\overline{\mathbb{K}}[[t, \boldsymbol{X}]]$, which implies that the extension of J'' in $\overline{\mathbb{K}}[[t, \boldsymbol{X}]]$ is the trivial ideal $\langle 1 \rangle$. This means the equality $J = J'$ holds in $\overline{\mathbb{K}}[[t, \boldsymbol{X}]]$, which gives the equality $J + \langle t - \tau \rangle = J' + \langle t - \tau \rangle$ in $\overline{\mathbb{K}}[[t, \boldsymbol{X}]]$. Consequently, our conclusion holds. □

We now can give a bound on the sum of the multiplicities of $\boldsymbol{B}_{t=\tau}$ at all its isolated roots, for any τ in $\overline{\mathbb{K}}$.

Lemma 5.2.5. *The ideal $\mathfrak{J}'$ has dimension zero and $V(\mathfrak{J}') \subset \mathbf{S}^n$ is the set of isolated solutions of $V(\mathfrak{J}) \subset \mathbf{S}^n$.*

Proof. Since $J = J' \cap J''$, we have $\mathfrak{J} = \mathfrak{J}' \cap \mathfrak{J}''$ by Corollary 3.4 in [6]. Moreover, the irreducible components of $V(J')$ are precisely those irreducible components of $V(J)$ that have dimension one and with a dense image by π_t, our claim holds. □

Recall that $c = \dim_{\mathbf{S}}(\mathbf{S}[\boldsymbol{X}]/\mathfrak{J}')$. Let $\tilde{J}'$ is the extension of J' in $\overline{\mathbb{K}}(t)[\boldsymbol{X}]$. Since $\mathbf{S}$ is an algebraic closure of $\overline{\mathbb{K}}(t)$, one has $\dim_{\overline{\mathbb{K}}(t)}(\overline{\mathbb{K}}(t)[\boldsymbol{X}]/\tilde{J}') = c$. The following lemma relates this quantity to the multiplicities of the solutions in any fiber $\boldsymbol{B}_{t=\tau}$. This gives our proof for Proposition 5.2.1.

Lemma 5.2.6. *Let τ be in $\overline{\mathbb{K}}$. The sum of the multiplicities of the isolated solutions of $\boldsymbol{B}_{t=\tau}$ is at most equal to c.*

Proof. The sum in this lemma is also the sum of the multiplicities of the ideal J_τ at all $(\tau, \boldsymbol{x})$, for $\boldsymbol{x}$ an isolated solution of $\boldsymbol{B}_{t=\tau} = 0$. By Lemma 5.2.4, this is also the sum of the multiplicities of $J'_{t=\tau}$ at all $(\tau, \boldsymbol{x})$, for $\boldsymbol{x}$ an isolated solution of $\boldsymbol{B}_{t=\tau} = 0$. Therefore, it is sufficient to show that the sum of the multiplicities of $J'_{t=\tau}$ at all $(\tau, \boldsymbol{x})$, for $\boldsymbol{x}$ such that $(\tau, \boldsymbol{x})$ cancels $J'_{t=\tau}$, is at most c. Note that this sum is equal to the dimension k of the $\overline{\mathbb{K}}$-vector space $\overline{\mathbb{K}}[t, \boldsymbol{X}]/J'_{t=\tau}$. We also remark that for any isolated solution $\boldsymbol{x}$ of $\boldsymbol{B}_\tau$, $(\tau, \boldsymbol{x})$ is an isolated root of J'_τ, though the converse may not be true.

Let $m_1, \ldots, m_k$ be monomials that forms a $\overline{\mathbb{K}}$-basis of $\overline{\mathbb{K}}[t, \boldsymbol{X}]/J'_{t=\tau}$. Since $T - \tau \in J'_\tau$, these monomials are monomials in only $\boldsymbol{X}$ variables. We will prove that $m_1, \ldots, m_k$ are still $\overline{\mathbb{K}}(t)$-linearly independent in $\overline{\mathbb{K}}(t)[\boldsymbol{X}]/\tilde{J}'$. This will imply $k \leq c$, and our conclusion follows.

Suppose that there exists a linear combination $a_1 m_1 + \cdots + a_k m_k$ in $\tilde{J}'$, with all a_i's in $\overline{\mathbb{K}}(t)$ and not all of them zero. This means we have an equality

$$\frac{a'_1}{d_1} m_1 + \cdots + \frac{a'_k}{d_k} m_k = \frac{a}{d}, \tag{5.1}$$

with all a'_i's, d, and all d_i's are in $\mathbb{K}[t]$; and a is in J'. Cleaning denominators in (5.1) gives us a combination of the form

$$e_1 m_1 + \cdots + e_k m_k \in J', \tag{5.2}$$

with not all e_i's zero. Let m be the highest non-negative integer such that the relation in (5.2) can be written as

$$(t - \tau)^m \left(f_1 m_1 + \cdots + f_k m_k\right) \in J', \tag{5.3}$$

with $f_i = e_i/(t-\tau)^m \in \mathbb{K}[t]$ for all $i = 1, \ldots, k$. In particular, $f_i(\tau)$ are not zero for all $i = 1, \ldots, k$. Note that the number m is well-defined since not all e_i's vanish.

Recall that the ideal J' has the form $J' = Q_1 \cap \cdots \cap Q_u$. For $i = 1, \ldots, u$, since Q_i is primary, the relation in (5.3) implies that either $f_1 m_1 + \cdots + f_k m_k \in Q_i$ or $(t-\tau)^{mn} \in Q_i$ for some $n > 0$. Since Q_i does not contain any non-zero polynomial in $\mathbb{K}[t]$, $f_1 m_1 + \cdots + f_k m_k$ must belong to all Q_i's. This means $f_1 m_1 + \cdots + f_k m_k$ is in J'. We can then evaluate this relation at $t = \tau$. We saw that the values $f_i(\tau)$ do not all vanish on the left, which is a contradiction with the independence of the monomials $m_1, \ldots, m_k$ modulo $J'_{t=\tau}$. □

5.2.2 Properties of the start system

With notation being as in Subsection 5.2.1, in this subsection we discuss the geometry of $V(J)$ at a neighborhood of $t = 0$. Note that $\boldsymbol{B}_{t=0} = \boldsymbol{A}$ is our start system. We will see

below that if some properties of the start system hold, we have that the number of isolated solutions, counting with multiplicities, of $\boldsymbol{A} = 0$ is equal to c.

We have already mentioned that the field $\mathbf{S} = \overline{\mathbb{K}}\langle\langle t\rangle\rangle$ is an algebraic closure of $\overline{\mathbb{K}}(t)$. Thus we can let $\Phi_1, \ldots, \Phi_{c'}$ be the points of $V(\mathfrak{J}')$, with coordinates taken in $\mathbf{S}$; in particular, we can see that $c' \leq c$. Any non-zero series φ in $\mathbf{S}$ admits a well-defined *valuation* $\nu(\varphi)$, which is the smallest exponent that appears in its expansion with a non-zero coefficient; we also set $\nu(0) = \infty$. The valuation $\nu(\Phi)$, for a vector $\Phi = (\phi_1, \ldots, \phi_s)$ with entries in $\mathbf{S}$, is the minimum of the valuations of its exponents. We say that Φ is *bounded* if it has non-negative valuation; in this case, $\lim_0(\Phi)$ is defined as the vector $(\lim_0(\phi_1), \ldots, \lim_0(\phi_s))$, with $\lim_0(\phi_i) = \mathrm{coeff}(\phi_i, t^0)$ for all $i = 1, \ldots, s$.

Proposition 5.2.7. *With conditions in Proposition 5.2.1 and suppose further that the following conditions hold:*

C_1. *All points $\Phi_1, \ldots, \Phi_{c'}$ are bounded.*

C_2. *The ideal $\langle \boldsymbol{A} \rangle$ is radical and of dimension zero in $\overline{\mathbb{K}}[\boldsymbol{X}]$.*

Then, $\boldsymbol{A}$ has exactly c solutions, all of them having multiplicity one.

The rest of this subsection is devoted to prove this proposition. We define $\varphi_1, \ldots, \varphi_{c'}$ by $\varphi_i = \lim_0(\Phi_i) \in \overline{\mathbb{K}}^n$ for $i = 1, \ldots, c'$.

Lemma 5.2.8. *The variety $V(J' + \langle t\rangle) = \{\varphi_i \mid i = 1, \ldots, c'\}$.*

Proof. We first prove that φ_i is in $V(J' + \langle t\rangle)$ for $i \leq c'$. Let $g_1, \ldots, g_\ell$ be generators of the ideal J' in $\overline{\mathbb{K}}[t, \boldsymbol{X}]$; they also generate $\mathfrak{J}'$ in $\overline{\mathbb{K}}(t)[X]$. Then

$$J' + \langle t\rangle = \langle g_{1,0}, \cdots, g_{\ell,0}\rangle,$$

where $g_{k,0} = g_k(0, \boldsymbol{X}) \in \overline{\mathbb{K}}[\boldsymbol{X}]$ for $k = 1, \ldots, \ell$. For $i \leq c'$, consider the vector of series Φ_i, then $g_k(\Phi_i) = 0$ for $k = 1, \ldots, \ell$. Since Φ_i is bounded, that is all elements involved in Φ_i have non-negative valuation, we can take the coefficient of t^0 which gives us $g_{k,0}(\varphi_i) = 0$ for $k = 1, \ldots, \ell$. This gives our claim.

Conversely, let $t_1, \ldots, t_n$ be new indeterminates and $\mathbb{L}$ be the algebraic closure of the field $\overline{\mathbb{K}}(t_1, \ldots, t_n)$. Let $\mathcal{C} \subset \mathbb{L}^{n+1}$ be the zero-set of the ideal $J' \cdot \mathbb{L}[t, \boldsymbol{X}]$ and consider the projection $\mathcal{C} \to \mathbb{L}^2$ defined by $(\tau, \alpha_1, \ldots, \alpha_n) \mapsto (\tau, t_1\alpha_1 + \cdots + t_n\alpha_n)$. The Zariski closure $\mathcal{S}$ of the image of this map is a hypersurface.

Since the ideal J' is generated by polynomials with coefficients in $\overline{\mathbb{K}}$, we can deduce that $\mathcal{S}$ admits a squarefree defining equation $\mathcal{H}$ in $\mathbb{K}(t_1, \ldots, t_n)[t, t_0]$. Without loss of generality, we can assume that $\mathcal{H}$ is in $\mathbb{K}[t_1, \ldots, t_n][t, t_0]$. Since $\mathcal{H}$ admits no irreducible component lying above $t = \tau$, for any $\tau \in \mathbb{K}$, the polynomial $\mathcal{H}$ admits no factor in $\overline{\mathbb{K}}[t]$. Thus, $\mathcal{H}(0, t_0, \ldots, t_n)$ is non-zero.

Let h be the leading coefficient of $\mathcal{H}$ with respect to t_0. Result in [162, Proposition 1] proves that $\mathcal{H}/h$, seen in $\overline{\mathbb{K}}(t_1,\ldots,t_n,t)[t_0] \subset \mathbb{L}(t)[t_0]$, is the minimal polynomial of $t_1x_1 + \cdots + t_nx_n$ in $\mathbb{L}(t)[\boldsymbol{X}]/\sqrt{J'}\cdot\mathbb{L}(t)[\boldsymbol{X}]$. The latter ideal is also the extension of $\sqrt{\mathfrak{J}'}$ to $\mathbb{L}(t)[\boldsymbol{X}]$, so $\mathcal{H}/h$ factors as

$$\frac{\mathcal{H}}{h} = \prod_{1\leq i\leq c'} (t_0 - t_1\Phi_{i,1} - \cdots - t_n\Phi_{i,n})$$

in $\mathbb{L}'[t_0]$, where $\mathbb{L}' = \mathbb{L}[[t]]$ is the generalized power series of ring in t with coefficients in $\mathbb{L}$. This give the equality

$$\mathcal{H} = h\cdot \prod_{1\leq i\leq c'} (t_0 - t_1\Phi_{i,1} - \cdots - t_n\Phi_{i,n})$$

over $\mathbf{S}[t_1,\ldots,t_n,t_0]$.

Since h and $(t_0 - t_1\Phi_{i,1} - \cdots - t_n\Phi_{i,n})$, for $1\leq i\leq c'$, are primitive in $\mathbb{K}[t_0,\ldots,t_n][t]$, then Gauss' Lemma implies that $\mathcal{H}$ is primitive as well (recall that a polynomial $h = \sum_{0\leq k\leq m} h_k t^k$ in $\mathbb{K}[t_0,\ldots,t_n][t]$ is called *primitive* if the only common factor of $(h_k)_{0\leq k\leq m}$ is 1). As a result, we can take the coefficient of t^0 term-wise, and obtain

$$\mathcal{H}(0,t_0,\ldots,t_n) = h_0\prod(t_0 - t_1\varphi_{i,1} - \cdots - t_n\varphi_{i,n}),$$

where h_0 is in $\mathbb{K}[t_1,\ldots,t_n]$. Note that h_0 is non-zero because $\mathcal{H}(0,t_0,\ldots,t_n)$ is non-zero as above. By the construction of $\mathcal{H}$, for any $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n)$ in $V(J' + \langle t\rangle)$, $(t_1\alpha_1 + \cdots t_n\alpha_n)$ cancels $\mathcal{H}(0,t_0,\alpha_1,\ldots,\alpha_n)$, so $\boldsymbol{\alpha}$ must be one of $(\varphi_i)_{1\leq i\leq c'}$. □

Lemma 5.2.9. *The ideal $\mathfrak{J}'$ is radical. Equivalently, $c' = c$.*

Proof. From Lemma 5.2.5, $\mathfrak{J}'$ has dimension zero, so it is sufficient to prove that for $i = 1,\ldots,c'$, the localization of $\mathbf{S}[\boldsymbol{X}]/\mathfrak{J}'$ at the maximal ideal $\mathfrak{m}_{\Phi_i}$ is a field, or equivalently that the localization of $\mathbf{S}[\boldsymbol{X}]/\mathfrak{J}$ at $\mathfrak{m}_{\Phi_i}$ is a field. Since $\mathbf{S} = \overline{\mathbb{K}}\langle\langle t\rangle\rangle$ is algebraically closed, it is a perfect field. By the Jacobian criterion [53, Theorem 16.19.b], our claim holds if and only if the Jacobian matrix of $\boldsymbol{B}$ with respect to $\boldsymbol{X}$ has full rank n at Φ_i.

By Lemma 5.2.8, we know that $\varphi_i = \lim_0(\Phi_i)$ is a root of $\boldsymbol{B}_{\tau=0}$. Since the ideal $\langle \boldsymbol{B}_{\tau=0}\rangle$ is radical and zero-dimensional (by C_2), then the Jacobian matrix of $\boldsymbol{B}_{\tau=0} = \boldsymbol{B}(0,\boldsymbol{X})$ with respect to variables $\boldsymbol{X}$ has full rank n at φ_i by Lemma 3.1.8. Since this matrix is the limit at zero of the Jacobian matrix of $\boldsymbol{B}$ with respect to $\boldsymbol{X}$, taken at Φ_i, the latter must have full rank n, and our claim that $\mathfrak{J}'$ is radical is proved. □

We can now finish our proof of Proposition 5.2.7. To do this, we have to show that $V(\boldsymbol{B}_{t=0})$ consists of exactly c solutions, all with multiplicity one. First, since $\boldsymbol{B}_{t=0}$ is finite (from C_2), Lemma 5.2.2 implies that $\boldsymbol{x}$ is in $V(\boldsymbol{B}_{t=0})$ if and only if $(0,\boldsymbol{x})$ is in $V(J' + \langle t\rangle)$ (recall that $P_1,\ldots,P_u$ are associated primes of $Q_1,\ldots,Q_u$ and $J' = Q_1\cap\cdots\cap Q_u$). Next, taking C_1 and Lemma 5.2.9 implies that $c = c'$. Thus, in view of Lemma 5.2.8, it suffices to show that for i, i' in $\{1,\ldots,c\}$ with $i\neq i'$, we have $\varphi_i \neq \varphi_{i'}$.

Lemma 5.2.10. *For i, i' in $\{1, \ldots, c\}$ with $i \neq i'$, we have $\varphi_i \neq \varphi_{i'}$.*

Proof. Suppose on the contrary that $\varphi_i = \varphi_{i'}$ for some $i \neq i'$. Since the Jacobian matrix of $\boldsymbol{B}_{t=0}$ has full rank n at φ_i, there exists a corresponding maximal non-zero minor in $\boldsymbol{B}$. Without loss of generality, we can assume that $\boldsymbol{B}' = (b_1, \ldots, b_n)$ gives this maximal non-zero minor.

Let $z = \nu(\Phi_i - \Phi_{i'})$. Since $\varphi_i = \varphi_{i'}$, then $z > 0$; and z is finite since otherwise we would have $\Phi_i = \Phi_{i'}$ which contradicts with $i \neq i'$. Let us write $\Phi_i = \phi + t^z \delta_i$ and $\Phi_i = \phi + t^z \delta_{i'}$, for some vectors of bounded series $\phi, \delta_i, \delta_{i'}$ such that all terms in ϕ have valuation less than z. In addition, $\lim_0(\delta_i) \neq \lim_0(\delta_{i'})$.

Consider the Taylor expansion of $\boldsymbol{B}'$ at ϕ

$$\boldsymbol{B}'(\Phi_i) = B'(\phi) + \mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{B}')(\phi)\, t^z \delta_i + t^{2z} r_i = 0 \tag{5.4}$$

and

$$\boldsymbol{B}'(\Phi_{i'}) = B'(\phi) + \mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{B}')(\phi)\, t^z \delta_{i'} + t^{2z} r_{i'} = 0, \tag{5.5}$$

for some vectors of bounded series $r_i, r_{i'}$. By subtracting equations (5.4) and (5.5) and dividing by t^z, we obtain

$$\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{B}')(\phi)(\delta_i - \delta_{i'}) = t^z r,$$

for some vectors of bounded series r. Furthermore, $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{B}')(\phi)$ is invertible, so one can deduce

$$\delta_i - \delta_{i'} = t^z r', \tag{5.6}$$

where $r' = r/\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{B}')(\phi)$ is a vector of bounded series. However, while $(\delta_i - \delta_{i'})$ has zero-valuation, $t^z r$ has positive valuation since $z > 0$ and r' is bounded. This is a contradiction. □

5.2.3 Homotopy algorithms

With all notation being as in the previous subsections, we now describe our algorithmic framework for computing either the isolated solutions, or the simple solutions, of the system $\boldsymbol{C} = (c_1, \ldots, c_m)$, assuming that conditions in both Proposition 5.2.1 and Proposition 5.2.7 are satisfied. The main result in this subsection is the following proposition.

Proposition 5.2.11. *Suppose that assumptions* B_1, B_2, C_1, *and* C_2 *hold and that we are given*

- *a straight-line program Γ of length σ that computes $\boldsymbol{B}$;*
- *a zero-dimensional parametrization $\mathscr{R}_0 = ((w_0, v_{0,1}, \ldots, v_{0,n}), \lambda)$ with coefficients in $\mathbb{K}$ of $V(\boldsymbol{A}) = V(\boldsymbol{B}_{t=0})$; the linear form λ needs to satisfy some genericity requirements, that are described below. Note that w_0 has degree c, where c is defined in Proposition 5.2.1;*

- *an upper bound e on the degree of the homotopy curve $V(J') \subset \overline{\mathbb{K}}^{n+1}$ (see Remark 5.2.3).*

Then there exists a randomized algorithm Homotopy *which computes a zero-dimensional parametrization of the isolated points of $V(\boldsymbol{C})$ using*

$$O^{\sim}(c^5 mn^2 + c(e + c^5)n(\sigma + n^3)) \subset (e\,\sigma\,m)^{O(1)}$$

operations in $\mathbb{K}$.

The variant below focuses on the computation of simple points.

Proposition 5.2.12. *Under the assumptions of Proposition 5.2.11, there exists a randomized algorithm* Homotopy_simple *which computes a zero-dimensional parametrization of the simple points of $V(\boldsymbol{C})$ using*

$$O^{\sim}(c^2\,m\,n^2 + \,c\,e\,n(\sigma + n^2)) \subset (e\,\sigma\,m)^{O(1)}$$

operations in $\mathbb{K}$.

Our goal in this subsection is to prove these propositions. Once this is done, in order to obtain complete algorithms for Problems (1) to (4), we will still have to specify how to define $\boldsymbol{B}$ and how to solve the start system $\boldsymbol{A} = \boldsymbol{B}_{t=0}$; this is the purpose of the next chapters. In Section 5.3, we will show determinantal systems $\boldsymbol{B}$ satisfy assumptions B_1 and B_2, while in the next chapters, depending on the context, we will construct systems which satisfy assumptions C_1 and C_2 for the start systems $\boldsymbol{A}$.

Decomposing $\mathscr{R}_0$.

Let $\mathscr{R}_0 = ((w_0, v_{0,1}, \ldots, v_{0,n}), \lambda)$ be a zero-dimensional parametrization of the start system $V(\boldsymbol{B}_{t=0})$, with w_0 and all $v_{0,j}$ in $\mathbb{K}[y]$. Note that the degree of w_0 equals the degree of the variety $V(\boldsymbol{B}_{t=0})$, which is the integer c defined previously.

At the core of the algorithms, we need to use Newton-Hensel iterations to lift $\mathscr{R}_0$. Therefore, we first need to decompose $\mathscr{R}_0$ into finitely many zero-dimensional parametrizations $\mathscr{R}_{0,j} = ((w_{0,j}, v_{0,j,1}, \ldots, v_{0,j,n}), \lambda)_{1 \le j \le t}$, all with coefficients in $\mathbb{K}$, such that for j in $\{1, \ldots, t\}$, we know indices $\boldsymbol{i}_j = (i_{j,1}, \ldots, i_{j,n})$ such that the Jacobian matrix of $(b_{0,i})_{i \in \boldsymbol{i}_j}$ has full rank n at $\boldsymbol{x}$, for all $\boldsymbol{x}$ in $Z(\mathscr{R}_{0,j})$.

If w_0 were irreducible, we would simply evaluate the Jacobian matrix of $\boldsymbol{B}_{t=0}$ at the point $(v_{0,1}/w_0', \ldots, v_{0,n}/w_0')$, which has coordinates in the field $\mathbb{L} = \mathbb{K}[y]/\langle w_0 \rangle$, and find a non-zero minor of size n in this matrix. Computing this Jacobian matrix takes $O(n\sigma)$ operations in $\mathbb{L}$ (see e.g. [84, Lemma 25]) and finding an invertible minor requires $O(mn^2)$ operations in $\mathbb{L}$ by using, for example, Gaussian elimination. The total time, under the

assumption that w_0 is irreducible, is thus $O(mn^2+n\sigma)$ operations in $\mathbb{L}$, that is, $O^{\sim}(c(mn^2+n\sigma))$ operations in $\mathbb{K}$.

When w_0 is not irreducible, $\mathbb{L} = \mathbb{K}[y]/\langle w_0\rangle$ is a product of fields. We can still apply the same process as in the irreducible case by factoring w_0. However, we do not want our runtime to depend on the cost of factoring polynomials (else our analysis would depend on the bit size of the data when $\mathbb{K} = \mathbb{Q}$). Hence, we will use *dynamic evaluation techniques*, as in [48] which is also known as the *D5 principle*. Indeed, the only issue that may arise is that we attempt to invert a zero-divisor in $\mathbb{L}$. If this is the case, following the D5 principle, the computation splits into branches and we find a non-zero factor r_0 of w_0.

We then replace $\mathscr{R}_0$ by two new zero-dimensional parametrizations $\mathscr{R}_0' = ((r_0, (v_{0,1}/s_0) \bmod r_0, \ldots, (v_{0,n}/s_0) \bmod r_0), \lambda)$ and $\mathscr{R}_0'' = ((s_0, (v_{0,1}/r_0) \bmod s_0, \ldots, (v_{0,n}/r_0) \bmod s_0), \lambda)$, with $s_0 = w_0/r_0$, such that $Z(\mathscr{R}_0) = Z(\mathscr{R}_0') \cup Z(\mathscr{R}_0'')$, where r_0 vanishes and is non-zero on $Z(\mathscr{R}_0')$ and $Z(\mathscr{R}_0'')$, respectively. Then, we can restart from $Z(\mathscr{R}_0')$ and $Z(\mathscr{R}_0'')$ independently. Overall, in the worst case, we arrive to c branches, that is, the splitting process induces an extra factor of $O(c)$ in the runtime compared to the case when w_0 is irreducible. Therefore, one needs $O^{\sim}(c^2(mn^2 + n\sigma))$ operations in $\mathbb{K}$.

Lifting power series and rational reconstructions.

For $j = 1, \ldots, t$, we can then apply Newton-Hensel iteration to the system $(b_i)_{i\in \boldsymbol{i}_j}$ to lift $\mathscr{R}_{0,j} = ((w_{0,j}, v_{0,j,1}, \ldots, v_{0,j,n}), \lambda)$ into a zero-dimensional parametrization $\mathscr{R}_j$ with coefficients in $\mathbb{K}[[t]]/\langle t^{2e}\rangle$, where e is the degree of the homotopy curve $\boldsymbol{B}$ and which is given as input to the algorithm. By Lemma 3.7.6, this can be done using $O^{\sim}(c\,e(\sigma + n^2)n)$ operations in $\mathbb{K}$. Using the Chinese Remainder Theorem, we can combine all $\mathscr{R}_j$ into a single zero-dimensional parametrization $\mathscr{R}$ with coefficients in $\mathbb{K}[[t]]/\langle t^{2e}\rangle$, since for $j \neq j'$, $w_{0,j}$ and $w_{0,j'}$ generate the unit ideal in $\mathbb{K}[[t]]/\langle t^{2e}\rangle$; this takes time $O^{\sim}(c\,e\,n)$.

Using the notation of the previous subsection, as we have discussed in Subsection 3.7, the zeros of $\mathscr{R}$ in $\overline{\mathbb{K}}[[t]]/\langle t^{2e}\rangle$ are the truncation of the power series roots $\Phi_1, \ldots, \Phi_c$ of $\mathfrak{J}'$. Since the degree of $V(J')$ is at most e, knowing $\mathscr{R}$ at precision $2e$ allows us to reconstruct a zero-dimensional parametrization $\mathscr{S}$ with coefficients in $\mathbb{K}(t)$ such that $Z(\mathscr{S}) = V(\mathfrak{J}')$, with all coefficients having numerator and denominator of degree at most e. This can be done by applying rational function reconstruction to all coefficients of $\mathscr{R}$. There are n coordinates $(x_1, \ldots, x_n)$ each has $O(c)$ coefficients with each of coefficients having numerator and denominator of degree $O(e)$. Thus computing $\mathscr{S}$ from $\mathscr{R}$ takes $O^{\sim}(c\,e\,n)$ operations in $\mathbb{K}$. Therefore the total cost of this step is $O^{\sim}(c\,e\,n(\sigma + n^2))$.

A finite set containing the isolated points of $V(\boldsymbol{C})$.

Similar to what we did in the previous section for $t = 0$, we let $\Phi_1', \ldots, \Phi_c'$ be the roots of $\mathfrak{J}'$ in the field of generalized power series in t' with coefficients in $\overline{\mathbb{K}}$ at $t = 1$, where $t' = t - 1$. Without loss of generality, we assume that $\Phi_1', \ldots, \Phi_{\kappa'}'$ are bounded, and $\Phi_{\kappa'+1}', \ldots, \Phi_c'$ are

unbounded, for some κ' in $\{0,\ldots,c\}$, and we define $\varphi'_1,\ldots,\varphi'_{\kappa'}$ by $\varphi'_i = \lim_0(\Phi'_i) \in \overline{\mathbb{K}}^n$ for $i = 1,\ldots,\kappa'$. By Lemma 5.2.8, $V(J' + \langle t-1\rangle) = \{\varphi'_i \mid i = 1,\ldots,\kappa'\}$.

We can now specify our requirements on the linear form λ which are already given in Definition 3.7.8. We restate those conditions here. We ask that λ be a well-separating element, that is:

1. λ is separating for $V(\mathfrak{J}') = \{\Phi'_1,\ldots,\Phi'_c\}$, that is, all values $\lambda(\Phi'_1),\ldots,\lambda(\Phi'_c)$ are pairwise distinct;
2. λ is separating for $V(J' + \langle t-1\rangle) = \{\varphi'_1,\ldots,\varphi'_{\kappa'}\}$;
3. for all $i = 1,\ldots,c$, $\nu(\lambda(\Phi_i)) = \nu(\Phi_i)$, where ν denotes the t'-adic valuation.

From Lemma 14 in [159, Section 3], we see that these conditions are satisfied for a generic choice of λ.

When this is the case, Lemma 4.4 in [155] shows how to recover a zero-dimensional parametrization $\mathscr{R}_1 = ((w_1, v_{1,1},\ldots,v_{1,n}),\lambda)$ with coefficients in $\mathbb{K}$ for the limit set

$$V(J' + \langle t-1\rangle) = \{\varphi'_i \mid i = 1,\ldots,\kappa'\}$$

starting from the previously computed rational parametrization $\mathscr{S}$, in time $O^{\sim}(c\,e\,n)$. We refer to Subsection 3.7.5 for the construction of $\mathscr{R}_1$ from $\mathscr{S}$ (in that subsection, we use the notion of $\mathscr{Z}$ instead of $\mathscr{R}_1$).

When the chosen linear form λ is not generic enough, the algorithm may fail, or output a parametrization of a subset of the zero-dimensional set we aim to compute. We refer to [159, Remark 14] for a discussion on probabilistic aspects.

In summary, at this stage, for the first three steps decomposition of $\mathscr{R}_0$, lifting and rational reconstruction and getting a finite set containing the isolated points of $V(\boldsymbol{C})$, we perform

$$O^{\sim}(c^2(mn^2 + n\sigma) + c\,e\,n(\sigma + n^2))$$

operations in $\mathbb{K}$.

Extract the isolated points.

We now can finish our proof for Proposition 5.2.11. From Lemma 5.2.2, any isolated solution $\boldsymbol{x}$ of $\boldsymbol{C}$, $(1,\boldsymbol{x})$ is in $V(J' + \langle t-1\rangle)$, so we discard from $V(J' + \langle t-1\rangle)$ those points that do not correspond to isolated points of $V(\boldsymbol{C})$ by using the algorithm of Section 5.1. Proposition 5.2.7 implies that we can take c as an upper bound on the multiplicity of isolated solutions.

We reuse the idea from dynamic evaluation techniques. If w_1 is irreducible, we can use the algorithm of Section 5.1, with an overhead $O^{\sim}(c)$ to account for the cost of operations

in $\mathbb{K}[y]/\langle w_1\rangle$. If w_1 is reducible, splittings are performed with the number of branches is bounded by c and then the total overhead is $O^{\sim}(c^2)$.

The runtime deduced from Proposition 5.1.1 to extract isolated points in $V(\boldsymbol{C})$ is then

$$O^{\sim}(c^6n^4 + c^5mn^2 + c^6n\sigma) = O(c^5mn^2 + c^6(n^3 + \sigma)n).$$

Plugging all together gives an algorithm called Homotopy with its runtime being

$$O(c\,e(n^2 + \sigma)n + c^5mn^2 + c^6(n^3 + \sigma)n) = O(c^5mn^2 + c(e + c^5)(n^3 + \sigma)n).$$

This finishes our proof for Proposition 5.2.11.

Algorithm 3 Homotopy$(\Gamma, \mathscr{R}_0, e)$

Input: a straight-line program Γ of length σ that computes $\boldsymbol{B} \in \mathbb{K}[t, \boldsymbol{X}]^m$
a zero-dimensional parametrization $\mathscr{R}_0$ of the system $\boldsymbol{A} = \boldsymbol{B}_{t=0}$
an upper bound e on the degree of the homotopy curve

Output: a zero-dimensional parametrization of the isolated points of $V(\boldsymbol{B}_{t=1})$

1. decompose $\mathscr{R}_0$ into $(\mathscr{R}_{0,j})_{1\le j\le t}$
   cost: $O^{\sim}(c^2(mn^2 + n\sigma))$
2. lift $(\mathscr{R}_{0,j})_{1\le j\le t}$ to $(\mathscr{R}_j)_{1\le j\le t}$ with coefficients in $\mathbb{K}[[t]]/\langle t^{2e}\rangle$
   cost: $O^{\sim}(c\,e\,n(\sigma + n^2))$
3. combine $(\mathscr{R}_j)_{1\le j\le t}$ into $\mathscr{R}$ with coefficients in $\mathbb{K}[[t]]/\langle t^{2e}\rangle$
   cost: $O^{\sim}(c\,e\,n)$
4. compute a zero-dimensional parametrization $\mathscr{S}$ with coefficients in $\mathbb{K}(t)$ from $\mathscr{R}$
   cost: $O^{\sim}(c\,e\,n)$
5. deduce a zero-dimensional parametrization $\mathscr{R}_1$ with coefficients in $\mathbb{K}$ from $\mathscr{S}$
   cost: $O^{\sim}(c\,e\,n)$
6. remove from $Z(\mathscr{R}_1)$ points that are not isolated in $V(\boldsymbol{C})$
   cost: $O^{\sim}(c^6n^4 + c^5mn^2 + c^6n\sigma)$

The Homotopy_simple algorithm.

The only difference to proving Proposition 5.2.12 is that we now need to discard from $V(J' + \langle t - 1\rangle)$ those points at which the Jacobian matrix associated to $\boldsymbol{C}$ is not full rank. This process is easier than discarding those points which are isolated by doing as follows.

First, we construct a straight-line program that evaluates the Jacobian matrix associated to $\boldsymbol{C}$. As we said in the Decomposing $\mathscr{R}_0$ step, this straight-line program has

length $O(n\,\sigma)$. Next, one evaluates this matrix modulo w_1, as done previously when we were decomposing $\mathscr{R}_0$, and use Gaussian elimination modulo w_1 to identify divisors of w_1 that need to be removed. The overall cost is similar to that of decomposing $\mathscr{R}_0$, that is, $O^{\sim}(c^2(mn^2+n\sigma))$ operations in $\mathbb{K}$.

In total, the cost of the Homotopy_simple algorithm is

$$O^{\sim}(c^2(mn^2+n\sigma)+c\,e\,n(\sigma+n^2))$$

operations in $\mathbb{K}$. Taking into account the inequality $e \geq c$ (Lemma 5.2.13 below) this simplifies as

$$O^{\sim}(c^2mn^2+c\,e\,n(\sigma+n^2)),$$

which completes the proof of Proposition 5.2.12.

Algorithm 4 Homotopy_simple$(\Gamma, \mathscr{R}_0, e)$

Input: a straight-line program Γ of length σ that computes $\boldsymbol{B} \in \mathbb{K}[t, \boldsymbol{X}]^m$
a zero-dimensional parametrization $\mathscr{R}_0$ of the system $\boldsymbol{A} = \boldsymbol{B}_{t=0}$
an upper bound e on the degree of the homotopy curve

Output: a zero-dimensional parametrization of the simple points of $V(\boldsymbol{B}_{t=1})$

1. run steps 1 to 5 of Homotopy$(\Gamma, \mathscr{R}_0, e)$ to have $\mathscr{R}_1$

   cost: $O^{\sim}(c^2(mn^2+n\sigma)+c\,e\,n(\sigma+n^2))$

2. remove from $Z(\mathscr{R}_1)$ points at which the Jacobian matrix of $\boldsymbol{C}$ is not full rank

   cost: $O^{\sim}(c^2(mn^2+n\sigma))$

We end this section with the proof of inequality $e \geq c$ used above.

Lemma 5.2.13. *Under the above notations and assumptions, the inequality $e \geq c$ holds.*

Proof. By definition, e upper bounds the degree of $V(J')$, which is an algebraic curve. The degree of this curve is at least to the cardinality of any fiber $V(J'_{t=\tau})$. In particular, we have

$$\sharp V(J'_{t=0}) \leq \deg(V(J')) \leq e.$$

Proposition 5.2.7 establishes that the number of isolated points of $V(\boldsymbol{B}_{t=0})$ equals c. By Lemma 5.2.2, all these points lie in $V(J'_{t=0})$, which allows us to deduce $c \leq e$. □

5.3 Properties of determinantal ideals

We have seen in Section 5.2 that in order to apply our homotopy algorithms, the deformed system needs to satisfy assumptions B_1 and B_2. In this section, we prove that determinantal systems satisfy B_1 and B_2.

Let t and $\boldsymbol{X} = (x_1, \ldots, x_n)$ be variables, let $\boldsymbol{V} = (v_1, \ldots, v_s)$ be polynomials in $\mathbb{K}[t, \boldsymbol{X}]$ with $s \leq n$, and $\boldsymbol{U}$ be a matrix in $\mathbb{K}[t, \boldsymbol{X}]^{p \times q}$ with $p \leq q$. Let $\boldsymbol{B} = (b_1, \ldots, b_s, \ldots b_m)$ where $(b_1, \ldots, b_s) = (v_1, \ldots, v_s)$ and the polynomials $(b_{s+1}, \ldots, b_m)$ are the p-minors of $\boldsymbol{U}$. In particular, $m = s + \binom{q}{p}$. Let $J = \langle \boldsymbol{B} \rangle$ be an ideal in $\overline{\mathbb{K}}[t, \boldsymbol{X}]$.

Proposition 5.3.1. *If $n = q - p + s + 1$, the ideal J satisfies the following properties:*

- *Any irreducible component of $V(J) \subset \overline{\mathbb{K}}^{n+1}$ has dimension at least one.*
- *For any maximal ideal $\mathfrak{m} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]$, if the localization $J_{\mathfrak{m}} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$ has height n, then it is unmixed (that is, all associated primes have height n).*

We note that when $p = 1$, the ideal J is defined by $m = s + q$ polynomials in $\mathbb{K}[t, \boldsymbol{X}]$ with $n = q - p + s + 1 = q + s$ and so $m = n$. In this case, these properties are well-known with the first one being Krull's theorem, and the second being the Macaulay's unmixedness theorem in the Cohen-Macaulay ring $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$ [53, Corollary 18.14].

The rest of this section is devoted for the proof in the general case, when J contains maximal minors of a polynomial matrix with $p \geq 2$.

Let us denote by $\bar{J} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]$ the ideal generated by only the minors $(b_{s+1}, \ldots, b_m)$ of $\boldsymbol{B}$; and so $J = \langle v_1, \ldots, v_s \rangle + \bar{J}$. Let $W_1, \ldots, W_k$ be the $\overline{\mathbb{K}}$-irreducible components of $V(\bar{J}) \subset \overline{\mathbb{K}}^{n+1}$. We have the following result.

Lemma 5.3.2. *For any $1 \leq i \leq k$, $\dim(W_i) \geq (n+1) - (q - p + 1)$.*

Proof. Note first that we can assume $V(\bar{J}) \neq 0$ so that $\bar{J} \neq \overline{\mathbb{K}}[t, \boldsymbol{X}]$, since otherwise the proposition itself would be vacuously true. Recall that for a point $\boldsymbol{x}$ in $V(\bar{J}) \subset \overline{\mathbb{K}}^{n+1}$ and $\mathfrak{m} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]$ is the maximal ideal at $\boldsymbol{x}$, the height of $\bar{J}_{\mathfrak{m}} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$ is equal to

$$\operatorname{height}(\bar{J}_{\mathfrak{m}}) = (n+1) - \max\{\dim(W_i) \mid 1 \leq i \leq k, \boldsymbol{x} \in W_i\}. \tag{5.7}$$

Now for $i = 1, \ldots, k$, let $\boldsymbol{x}_i$ be a point in W_i that $\boldsymbol{x}_i \notin W_{i'}$ for all other $i' \neq i$ and let $\mathfrak{m}_i$ be the corresponding maximal ideal. Using equation (5.7) gives

$$\operatorname{height}(\bar{J}_{\mathfrak{m}_i}) = (n+1) - \dim(W_i).$$

Furthermore, Proposition 3.1.15 implies that the ring $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}_i}$ is Cohen-Macaulay. Then applying Lemma 3.2.1(i) with $R = \overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}_i}$ gives

$$(n+1) - \dim(W_i) \leq q - p + 1$$

which gives our claim. □

We now can finish our proof for the first property of Proposition 5.3.1. Since $\boldsymbol{V}$ consists of s polynomials, $J = \langle \boldsymbol{V} \rangle + \bar{J}$, and noticing that in this case $(n+1) - (q-p+1) = s+1$ then, by Krull's theorem, all irreducible components of $V(J) \subset \overline{\mathbb{K}}^{n+1}$ have dimension at least one.

For the second property, let $J_{\mathfrak{m}} = Q_1 \cap \cdots \cap Q_r$ be an irredundant primary decomposition of $J_{\mathfrak{m}}$ in $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$, and let $P_1, \ldots, P_r$ be the corresponding primes. We assume that the height of $J_{\mathfrak{m}}$ is n, so we need to show that all P_i's have height n. Let $\bar{J}_{\mathfrak{m}} \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]$ be the localization for $\bar{J}$ at $\mathfrak{m}$.

Lemma 5.3.3. *The quotient ring $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\langle \bar{J}_{\mathfrak{m}} \rangle$ is Cohen-Macaulay.*

Proof. Since $\mathfrak{m}$ is a maximal ideal in $\overline{\mathbb{K}}[t, \boldsymbol{X}]$, then $\mathfrak{m}$ is the maximal ideal at a point $\boldsymbol{x} \in \overline{\mathbb{K}}^{n+1}$ with $\boldsymbol{x} \in V(J)$. Then the height of $J_{\mathfrak{m}}$ in $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$ is

$$\operatorname{height}_{\overline{\mathbb{K}}[t,\boldsymbol{X}]_{\mathfrak{m}}}(J_{\mathfrak{m}}) = n + 1 - \dim(V_{\boldsymbol{x}}),$$

where $V_{\boldsymbol{x}}$ is the union of the irreducible components of $V(J)$ that contain $\boldsymbol{x}$. Our assumption is that $\operatorname{height}_{\overline{\mathbb{K}}[t,\boldsymbol{X}]_{\mathfrak{m}}}(J_{\mathfrak{m}}) = n$, that is, that $\dim(V_{\boldsymbol{x}}) = 1$. Thus, every irreducible component of $V(J)$ containing $\boldsymbol{x}$ has dimension 1.

Let W be an irreducible component of $V(\bar{J})$ containing $\boldsymbol{x}$. We claim that $\dim(W) = s+1$. Indeed, from Lemma 5.3.2, $\dim(W) \geq n - q + p = s + 1$. If $\dim(W) > s+1$, then by Krull's theorem, all irreducible components of $W \cap V(\boldsymbol{V})$, with $\boldsymbol{V} = (v_1, \ldots, v_s)$, have dimension at least 2. As $W \cap V(\boldsymbol{V})$ is a subset of $V(J)$ and contains $\boldsymbol{x}$, we have reached a contradiction with the first paragraph. Therefore, $\dim(W) = s+1$ for any irreducible component W of $V(\bar{J})$ containing $\boldsymbol{x}$. This implies that

$$\operatorname{height}_{\overline{\mathbb{K}}[t,\boldsymbol{X}]_{\mathfrak{m}}}(\bar{J}_{\mathfrak{m}}) = (n+1) - (s+1) = n - s = q - p + 1.$$

Note that the definitions of the height and the codimension of a prime ideal of a ring are coincident. Furthermore, $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$ is Cohen-Macaulay by Proposition 3.1.15. As a result, Theorem 3.2.2 shows that $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{J}_{\mathfrak{m}}$ is Cohen-Macaulay. □

For an ideal $I \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}$, we denote by $\bar{I}$ its image modulo $\langle J_{\mathfrak{m}} \rangle$. By the remarks following [178, Theorem IV.5.9], $\bar{Q}_1 \cap \cdots \cap \bar{Q}_r$ is an irredundant primary decomposition of $\bar{J}_{\mathfrak{m}}$ in $\mathbb{K}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{J}_{\mathfrak{m}}$, with the associated primes being $\bar{P}_1, \ldots, \bar{P}_r$. In addition, if $P_1, \ldots, P_u$ are the minimal primes of $J_{\mathfrak{m}}$, for some $u \leq r$, then $\bar{P}_1, \ldots, \bar{P}_u$ are the minimal primes of $\bar{J}_{\mathfrak{m}}$. Furthermore, since the height of $J_{\mathfrak{m}}$ is n, so $P_1, \ldots, P_u$ have height n as well.

We have the ring $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\langle \bar{J}_{\mathfrak{m}} \rangle$ is local by Lemma 3.1.13, and Lemma 5.3.3 implies that this quotient ring is Cohen-Macaulay. In other words, $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\langle \bar{J}_{\mathfrak{m}} \rangle$ is a Cohen-Macaulay local ring. As a result, for $1 \leq i \leq r$, by Theorem 3.1.16, one has

$$\dim(\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{J}_{\mathfrak{m}}) = \dim((\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{J}_{\mathfrak{m}})/\bar{P}_i) + \operatorname{height}(\bar{P}_i).$$

The factor $(\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{J}_{\mathfrak{m}})/\bar{P}_i$ can be simplified as $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{P}_i$, so we have

$$s + 1 = \dim(\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{P}_i) + \text{height}(\bar{P}_i).$$

For $1 \leq i \leq u$, $\dim(\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{P}_i) = 1$, so $\text{height}(\bar{P}_i) = s$ and for $u < i \leq r$, $\text{height}(\bar{P}_i)$ equals $s + 1$. Then the height of $\bar{J}_{\mathfrak{m}}$ is s since $\bar{P}_1, \ldots, \bar{P}_u$ are the minimal primes of $\bar{J}_{\mathfrak{m}}$.

The ideal $\bar{J}_{\mathfrak{m}} = \langle v_1, \ldots, v_s \rangle \subset \overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{J}_{\mathfrak{m}}$, and $\overline{\mathbb{K}}[t, \boldsymbol{X}]_{\mathfrak{m}}/\bar{J}_{\mathfrak{m}}$ is Cohen-Macaulay by Lemma 5.3.3, so $\bar{J}_{\mathfrak{m}}$ is unmixed, that is, u equals r. This implies that $Q_1 \cap \cdots \cap Q_u$ is an irredundant primary decomposition of $J_{\mathfrak{m}}$, and $J_{\mathfrak{m}}$ is unmixed. This finishes our proof for the second property of Proposition 5.3.1.

Chapter 6

Determinantal ideals in classical polynomial rings

6.1 A property of start systems

We have seen from the previous chapter that our systems need to satisfy conditions C_1 and C_2. With our notation being as in the previous chapter, in this section, we provide an equivalent condition to C_1.

Lemma 6.1.1. *Suppose the following conditions hold:*

- *For $k = 1, \ldots, m$, $\deg_{\boldsymbol{X}}(b_k) = \deg_{\boldsymbol{X}}(a_k)$, where $\deg_{\boldsymbol{X}}$ denotes the degree of a polynomial in $\boldsymbol{X}$ variables.*
- *The only common solution to $a_1^H(0, \boldsymbol{X}) = \cdots = a_m^H(0, \boldsymbol{X}) = 0$ is $(0, \ldots, 0) \in \overline{\mathbb{K}}^n$, where for $k = 1, \ldots, m$, a_k^H is the polynomial in $\overline{\mathbb{K}}[x_0, \boldsymbol{X}]$ obtained by homogenizing a_k using a new variable x_0.*

Then, all $\Phi_1, \ldots, \Phi_{c'}$ are bounded.

Proof. Since a zero vector is bounded, without loss of generality, one can assume that Φ_i are all non-zero for $i = 1, \ldots, c'$.

For $i = 1, \ldots, c'$, we write $\Phi_i = 1/t^{e_i}(\Psi_{i,1}, \ldots, \Psi_{i,n})$, for a vector $(\Psi_{i,1}, \ldots, \Psi_{i,n})$ of power series of valuation zero. That is all $\Psi_{i,j}$ are bounded and the vector $(\psi_{i,1}, \ldots, \psi_{i,n}) = \lim_0(\Psi_{i,1}, \ldots, \Psi_{i,n})$ is non-zero. Then $e_i = -\nu(\Psi_i)$, and we have to prove that $e_i \leq 0$. By way of contradiction, let us instead assume that $e_i > 0$.

For $k = 1, \ldots, m$, let $b_k^H \in \mathbb{K}[x_0, t, \boldsymbol{X}]$ be the homogenization of b_k with respect to variables $\boldsymbol{X}$. From the inequality

$$b_k^H(t^{e_i}, \Psi_{i,1}, \cdots, \Psi_{i,n}) = t^{e_i} b_k(\Psi_i)$$

and the fact that Ψ_i cancels $b_1, \ldots, b_m$, one can deduce that, for $k = 1, \ldots, m$,

$$b_k^H(t^{e_i}, \Psi_{i,1}, \cdots, \Psi_{i,n}) = 0.$$

Furthermore, we can write $b_k = a_k + t\tilde{b}_k$, for some polynomial $\tilde{b}_k$ in $\overline{\mathbb{K}}[t, \boldsymbol{X}]$, the first assumption of this lemma implies that $\deg_{\boldsymbol{X}}(\tilde{b}_k) \leq \deg_{\boldsymbol{X}}(a_k)$. As a result, the homogenizations with respect to $\boldsymbol{X}$ of b_k, a_k and $\tilde{b}_k$ satisfy a relation of the form

$$b_k^H = a_k^H + x_0^{\delta_k}\, t\, \tilde{b}_k^H,$$

for some $\delta_k \geq 0$. This implies the equality

$$a_k^H(t^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n}) + t^{\delta_k e_i + 1}\tilde{b}_k^H(t^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n}) = 0.$$

The second term has positive valuation, so is $a_k^H(t^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n})$. Taking the coefficient of t^0, this means that $a_k^H(0, \psi_{i,1}, \ldots, \psi_{i,n}) = 0$ (since $e_i > 0$), which implies that $(\psi_{i,1}, \ldots, \psi_{i,n}) = (0, \ldots, 0)$ by the second property of the lemma. This however contradicts the definition of $(\psi_{i,1}, \ldots, \psi_{i,n})$ which is a non-zero vector. □

6.2 The column-degree homotopy

We can now prove the first halves of Theorems 4.2.1, Theorem 4.2.2, and Theorem 4.2.3 by using the homotopy algorithms and taking into account the column-degree structure of our matrices.

As input, we are given a matrix $\boldsymbol{F} = [f_{i,j}] \in \mathbb{K}[\boldsymbol{X}]^{p \times q}$ with $\boldsymbol{X} = (x_1, \ldots, x_n)$ and polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[\boldsymbol{X}]$ such that $p \leq q$ and $n = q - p + s + 1$, and we want to compute either the isolated points or the simple points of

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = \{\boldsymbol{x} \in \overline{\mathbb{K}}^n \mid \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p \text{ and } g_1(\boldsymbol{x}) = \cdots = g_s(\boldsymbol{x}) = 0\}.$$

To match the notation of the previous chapters, let us define $\boldsymbol{C} = (c_1, \ldots, c_s, \ldots, c_m)$ where $(c_1, \ldots, c_s) = (g_1, \ldots, g_s)$ and $(c_{s+1}, \ldots, c_m)$ are the p-minors of $\boldsymbol{F}$ following the fixed ordering $\succ$. In particular, $m = s + \binom{q}{p}$.

For $j = 1, \ldots, q$, let $\operatorname{cdeg}(\boldsymbol{F}, j)$ be the degree of the j-th column of $\boldsymbol{F}$, that is, $\operatorname{cdeg}(\boldsymbol{F}, j) = \max_{1 \leq i \leq p}(\deg(f_{i,j}))$. For $1 \leq i \leq s$, we write $\gamma_i = \deg(g_i)$. Recall that for $k \geq 0$, $\eta_k(\delta_1, \ldots, \delta_q)$ denotes the elementary symmetric polynomial of degree k in $(\delta_1, \ldots, \delta_q)$.

Proposition 6.2.1. *The sum of the multiplicities of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$ is at most*

$$c = \gamma_1 \cdots \gamma_s\, \eta_{n-s}(\delta_1, \ldots, \delta_q).$$

Suppose that $\boldsymbol{F}$ *and* $\boldsymbol{G}$ *are given by a straight-line program of length* σ*. Assume that all* δ_j*'s and* γ_i*'s are at least equal to 1. Then there exists a randomized algorithm which is called* ColumnDegree *that computes these isolated points using*

$$O^{\sim}\left(\binom{q}{p} c(e+c^5)(\sigma+\gamma+q\delta)\right)$$

operations in $\mathbb{K}$*, where*

$$e = (\gamma_1+1)\cdots(\gamma_s+1)\eta_{n-s}(\delta_1+1,\ldots,\delta_q+1),$$
$$\gamma = \max(\gamma_1,\ldots,\gamma_s), \text{ and } \delta = \max(\delta_1,\ldots,\delta_q).$$

When we are interested in computing the simple points of $V_p(\boldsymbol{F},\boldsymbol{G})$, we have a better complexity estimate.

Proposition 6.2.2. *Reusing the notations introduced above, there exists a randomized algorithm which is called* ColumnDegree_simple *that computes the simple points of* $V_p(\boldsymbol{F},\boldsymbol{G})$ *using*

$$O^{\sim}\left(\binom{q}{p} c\, e(\sigma+\gamma+q\delta))\right)$$

operations in $\mathbb{K}$*.*

In both cases, we use the homotopy algorithms from the previous chapter. To use these algorithms, we need to define a start system $\boldsymbol{A} \in \mathbb{K}[\boldsymbol{X}]^m$ and a deformed system $\boldsymbol{B} \in \mathbb{K}[t,\boldsymbol{X}]^m$, for a new variable t, such that all assumptions B_1, B_2, C_1, and C_2 are satisfied. Note that the assumption C_1 is equivalent to the two conditions which are stated in Lemma 6.1.1. In the case where there are no polynomials $\boldsymbol{G}$ as the input, the construction used in this section is already in the appendix of [144], where it was used to bound the number of solutions of determinantal systems $V_p(\boldsymbol{F})$.

6.2.1 Setting up systems

We first show how to construct a polynomial matrix $\boldsymbol{L}$ in $\mathbb{K}[\boldsymbol{X}]^{p\times q}$ and polynomials $\boldsymbol{M} = (m_1,\ldots,m_s)$ in $\mathbb{K}[\boldsymbol{X}]^s$ used as the starting point for the homotopy deformation. For any $1 \le j \le q$ and $1 \le k \le \delta_j$, define

$$\lambda_{j,k} = \lambda_{j,k,0} + \sum_{\ell=1}^{n} \lambda_{j,k,\ell} x_\ell,$$

where all $\lambda_{j,k,\ell}$ are random elements in $\mathbb{K}$. Then, for $j = 1,\ldots,q$, we define

$$\lambda_j = \prod_{k=1}^{\delta_j} \lambda_{j,k},$$

and we let $\boldsymbol{L}$ be the matrix

$$\boldsymbol{L} = \begin{pmatrix} \lambda_1 & 2\lambda_2 & \cdots & q\lambda_q \\ \lambda_1 & 2^2\lambda_2 & \cdots & q^2\lambda_q \\ \vdots & \vdots & & \vdots \\ \lambda_1 & 2^p\lambda_2 & \cdots & q^p\lambda_q \end{pmatrix} \in \mathbb{K}[\boldsymbol{X}]^{p\times q}. \tag{6.1}$$

In addition, for $i = 1, \ldots, s$ and $k = 1, \ldots, \gamma_i$, we define

$$\mu_{i,k} = \mu_{i,k,0} + \sum_{\ell=1}^{n} \mu_{i,k,\ell} x_\ell,$$

where all $\mu_{i,k,\ell}$ are random elements in $\mathbb{K}$. Then we let $\boldsymbol{M} = (m_1, \ldots, m_s)$, with

$$m_i = \prod_{k=1}^{\gamma_i} \mu_{i,k}, \quad i = 1, \ldots, s.$$

Finally, we define our start system $\boldsymbol{A} = (a_1, \ldots, a_s, \ldots, a_m)$ as $(a_1, \ldots, a_s) = (g_1, \ldots, g_s)$ and the polynomials $(a_{s+1}, \ldots, a_m)$ are the p-minors of $\boldsymbol{L}$, following the ordering $\succ$.

Next, we define our deformed system $\boldsymbol{B} = (b_1, \ldots, b_m)$. Let t be a new variable and define the polynomials $\boldsymbol{V} = (v_1, \ldots, v_s)$ in $\mathbb{K}[t, \boldsymbol{X}]^s$ by $v_i = (1-t)\cdot m_i + t\cdot g_i$ for $i = 1, \ldots, s$, and the matrix

$$\boldsymbol{U} = (1-t)\cdot \boldsymbol{L} + t\cdot \boldsymbol{F} \in \mathbb{K}[t, \boldsymbol{X}]^{p\times q}.$$

We let $\boldsymbol{B} = (b_1, \ldots, b_s, \ldots, b_m)$ be the polynomials in $\mathbb{K}[t, \boldsymbol{X}]$ given by $(b_1, \ldots, b_s) = (v_1, \ldots, v_s)$ and $(b_{s+1}, \ldots, b_m)$ are the p-minors of $\boldsymbol{U}$, following the ordering $\succ$. Then, $\boldsymbol{B}_{t=1} = \boldsymbol{C}$ and $\boldsymbol{B}_{t=0} = \boldsymbol{A}$. Finally, we define J as the ideal generated by $\boldsymbol{B}$ in $\overline{\mathbb{K}}[t, \boldsymbol{X}]$.

Example 6.2.1. We illustrate this construction with Example 4.3.1 from the introduction. In this case, there are no polynomials $\boldsymbol{G}$, so $s = 0$. The column degrees $\delta_1, \delta_2, \delta_3$ of $\boldsymbol{F}$ are all equal to 2, and we take

$$\begin{aligned} \lambda_1 &= (10x_1 + x_2 - 1)(x_1 + 3x_2 - 5) \\ \lambda_2 &= (2x_1 - x_2 - 2)(3x_1 + 3x_2 - 1) \\ \lambda_3 &= (-x_1 + x_2 - 9)(-3x_1 + x_2 + 5). \end{aligned}$$

Then, $\boldsymbol{L}$ is given by

$$\boldsymbol{L} = \begin{bmatrix} \lambda_1 & 2\lambda_2 & 3\lambda_3 \\ \lambda_1 & 4\lambda_2 & 9\lambda_3 \end{bmatrix}.$$

The start system $\boldsymbol{A} = (2\lambda_1\lambda_2, 6\lambda_1\lambda_3, -4\lambda_2\lambda_3)$ is the set of 2-minors of this matrix.

Keeping in mind that we want to apply Propositions 5.2.11 and 5.2.12, we now verify that all required assumptions are satisfied. From Proposition 5.3.1, the determinantal ideal $J = \langle \boldsymbol{B} \rangle \subset \mathbb{K}[t, \boldsymbol{X}]$ satisfy properties B_1 and B_2. Recall that to have C_1, it suffices to show the two properties stated in Lemma 6.1.1.

6.2.2 Degrees of the start and deformed systems

We have to prove that for $i = 1, \ldots, m$, $\deg_{\boldsymbol{X}}(a_i) = \deg_{\boldsymbol{X}}(b_i)$. For $i = 1, \ldots, s$, $a_i = v_i$ and $b_i = (1-t) \cdot a_i + t \cdot c_i$ with $\deg_{\boldsymbol{X}}(a_i) = \deg_{\boldsymbol{X}}(c_i) = \gamma_i$ (a_i and c_i are polynomials in $\mathbb{K}[\boldsymbol{X}]$); then $\deg_{\boldsymbol{X}}(b_i) \leq \deg_{\boldsymbol{X}}(a_i)$. Furthermore, we have $b_i(0, \boldsymbol{X}) = a_i(\boldsymbol{X})$, so $\deg_{\boldsymbol{X}}(b_i) = \deg_{\boldsymbol{X}}(a_i) = \gamma_i$.

For $i = s+1, \ldots, m$, let $\boldsymbol{j}_i = (j_{i_1}, \ldots, j_{i_p})$ be the corresponding sequence of column indices such that a_i and b_i are the minors built with columns indexed by $\boldsymbol{j}_i$ in $\boldsymbol{L}$ and $\boldsymbol{U}$, respectively. Then $a_i = \alpha_i \lambda_{j_{i_1}} \cdots \lambda_{j_{i_p}}$, where

$$\alpha_i = \begin{vmatrix} j_{i_1} & j_{i_2} & \cdots & j_{i_p} \\ j_{i_1}^2 & j_{i_2}^2 & \cdots & j_{i_p}^2 \\ \vdots & \vdots & & \vdots \\ j_{i_1}^p & j_{i_2}^p & \cdots & j_{i_p}^p \end{vmatrix}.$$

Since $\mathbb{K}$ has characteristic zero, so α_i is a non-zero constant in $\mathbb{K}$. Therefore,

$$\deg(a_i) = \deg(\lambda_{j_{i_1}}) + \cdots + \deg(\lambda_{j_{i_p}}) = \delta_{j_{i_1}} + \cdots + \delta_{j_{i_p}}.$$

On the other hand, since the columns $(j_{i_1}, \ldots, j_{i_p})$ of $\boldsymbol{U}$ have respective degrees at most $\delta_{j_{i_1}}, \ldots, \delta_{j_{i_p}}$, then for $i = s+1, \ldots, m$,

$$\deg_{\boldsymbol{X}}(b_i) \leq \delta_{j_{i_1}} + \cdots + \delta_{j_{i_p}}.$$

Moreover, it can be shown that $b_i = a_i + t \cdot \tilde{b_i}$, for some polynomials $\tilde{b_i}$ in $\mathbb{K}[t, \boldsymbol{X}]$, which implies that $b_i(0, \boldsymbol{X}) = a_i(\boldsymbol{X})$. This gives us

$$\deg_{\boldsymbol{X}}(b_i) = \delta_{j_{i_1}} + \cdots + \delta_{j_{i_p}}.$$

Hence, $\deg_{\boldsymbol{X}}(b_i) = \deg_{\boldsymbol{X}}(a_i)$ for all $i = 1, \ldots, m$.

6.2.3 Solutions of the homogenization of the start system

We have to prove that the homogenization of the system $\boldsymbol{A}$ has no root at infinity. Let x_0 be a new variable and let $\boldsymbol{A}^H = (a_1^H, \ldots, a_m^H)$ be the homogenization of $\boldsymbol{A}$. Then, for $i = 1, \ldots, s$, we have

$$a_i^H = \prod_{k=1}^{\gamma_i} \mu_{i,k}^H \quad \text{with} \quad \mu_{i,k}^H = (\mu_{i,k,0} x_0 + \sum_{\ell=1}^{n} \mu_{i,k,\ell} x_\ell).$$

Since a_i^H, for $i = 1, \ldots, m$, are products of linear forms, we find the solutions of $\boldsymbol{A}^H$ by setting some of these linear forms to zero. In order to cancel $a_1^H, \ldots, a_s^H$, we choose

indices $\boldsymbol{u} = (u_1, \ldots, u_s)$, with $u_1 \in \{1, \ldots, \gamma_1\}$, $\ldots$, $u_s \in \{1, \ldots, \gamma_s\}$, and we consider the equations

$$\mu^H_{i,u_i} = 0, \quad \text{that is,} \quad \mu_{i,u_i,0} x_0 + \sum_{\ell=1}^{n} \mu_{i,u_i,\ell} x_\ell = 0,$$

for $i = 1, \ldots, s$.

For $i = s+1, \ldots, m$,

$$a^H_i = \alpha_i \lambda^H_{j_{i_1}} \ldots \lambda^H_{j_{i_p}}, \quad \text{for } \boldsymbol{j}_i = (j_{i_1}, \ldots, j_{i_p}) \text{ and } \alpha_i \in \mathbb{K}_{\neq 0} \text{ as above,}$$

where for $j = 1, \ldots, q$ we set

$$\lambda^H_j = \prod_{k=1}^{\delta_j} \lambda^H_{j,k} \quad \text{with} \quad \lambda^H_{j,k} = \lambda_{j,k,0} x_0 + \sum_{\ell=1}^{n} \lambda_{j,k,\ell} x_\ell.$$

In order to cancel $a^H_{s+1}, \ldots, a^H_m$, there are $q - p + 1 = n - s$ terms $(\lambda^H_{j_1}, \ldots, \lambda^H_{j_{n-s}})$ among $(\lambda^H_1, \ldots, \lambda^H_q)$ which vanish, and we choose indices $\boldsymbol{k} = (k_1, \ldots, k_{n-s})$, with $k_1 \in \{1, \ldots, \delta_{j_1}\}$, $\ldots$, $k_{n-s} \in \{1, \ldots, \delta_{j_{n-s}}\}$ such that

$$\lambda^H_{j_1,k_1} = \cdots = \lambda^H_{j_{n-s},k_{n-s}} = 0.$$

That is, for $\rho = 1, \ldots, n-s$,

$$\lambda^H_{j_\rho,k\rho} = \lambda_{j_\rho,k_\rho,0}\, x_0 + \sum_{\ell=1}^{n} \lambda_{j_\rho,k_\rho,\ell} x_\ell.$$

To sum up, any solution of $\boldsymbol{A}^H$ vanishes at a linear system

$$\mu_{i,u_i,0} x_0 + \sum_{\ell=1}^{n} \mu_{i,u_i,\ell} x_\ell = \lambda_{j_\rho,k_\rho,0}\, x_0 + \sum_{\ell=1}^{n} \lambda_{j_\rho,k_\rho,\ell} x_\ell = 0 \tag{6.2}$$

for fixed indices $\boldsymbol{u} = (u_1, \ldots, u_s)$ and $\boldsymbol{k} = (k_1, \ldots, k_{n-s})$. This implies that the possible values of points in $\mathbb{P}^n(\overline{\mathbb{K}})$ which cancel $\boldsymbol{A}^H$ are determined as solutions of a linear system of size n. For a generic choice of the coefficients $\lambda_{j,k,\ell}$ and $\mu_{i,k,\ell}$, none of these points satisfies $x_0 = 0$, so that our claim holds.

6.2.4 Radical and zero-dimensional properties of $\langle \boldsymbol{A} \rangle$

We need to prove that the ideal $\langle \boldsymbol{A} \rangle$ is zero-dimensional and radical in $\overline{\mathbb{K}}[\boldsymbol{X}]$. From the previous subsection, we know that the projective variety defined by $\boldsymbol{A}^H$ has no point at infinity, so it is finite. As a result, the affine algebraic set defined by $\boldsymbol{A}$ is finite as well. It remains to show that the ideal generated by $\boldsymbol{A}$ is radical. Equivalently, we need to prove that at any points in $\boldsymbol{V}(\boldsymbol{A})$, the Jacobian matrix of $\boldsymbol{A}$ with respect to $x_1, \ldots, x_n$ has full rank.

We have all the affine solutions to $\boldsymbol{A}$ are obtained by setting x_0 in the projective solutions of $\boldsymbol{A}^H$. In other words, they are obtained by choosing indices $\boldsymbol{u} = (u_1, \ldots, u_s)$, with u_i in $\{1, \ldots, \gamma_i\}$ for all i, column indices $\boldsymbol{j} = (j_1, \ldots, j_{n-s})$, and $\boldsymbol{k} = (k_1, \ldots, k_{n-s})$, with k_i in $\{1, \ldots, \delta_{j_i}\}$ for all i, and solving the affine linear system

$$\mu_{1,u_1}(x_1, \ldots, x_n) = \cdots = \mu_{s,u_s}(x_1, \ldots, x_n) = \lambda_{j_1,k_1}(x_1, \ldots, x_n) = \cdots = \lambda_{j_{n-s},k_{n-s}}(x_1, \ldots, x_n).$$

Let $\boldsymbol{x} \in \overline{\mathbb{K}}^n$ be the corresponding point in $V(\boldsymbol{A})$. We consider first the equations $(a_1, \ldots, a_s)$; each such equation is a product of linear forms such as $a_i = \prod_{k=1}^{\gamma_i} \mu_{i,k}$, with $\mu_{i,u_i}(\boldsymbol{x}) = 0$. Since the coefficients $\mu_{i,k,\ell}$ are chosen generically, for $i = 1, \ldots, s$ and $k \neq u_i$, $\mu_{i,k}(\boldsymbol{x})$ is non-zero. As a result, in the local ring at $\boldsymbol{x}$, the polynomials $(a_1, \ldots, a_s)$ are equal, up to units, to the linear forms $(\mu_{1,u_1}, \ldots, \mu_{s,u_s})$.

Next we consider the p-minors of $\boldsymbol{L}$. Due to the genericity of the coefficients $\lambda_{j,k,\ell}$, since

$$\lambda_{j_1,k_1} = \cdots = \lambda_{j_{n-s},k_{n-s}} = 0,$$

together with $\mu_{i,u_i} = 0$ for $i = 1, \ldots, s$, only admits $\boldsymbol{x}$ as a solution, none of the other linear forms $\lambda_{j,k}$ vanishes at $\boldsymbol{x}$.

Recall that $n = q - p + s + 1$, so that $n - s = q - (p - 1)$. Hence, there are exactly $p - 1$ columns indexed by $\boldsymbol{j'} = (j'_1, \ldots, j'_{p-1})$ of $\boldsymbol{L}$ such that $j'_k \notin \boldsymbol{j} = (j_1, \ldots, j_{n-s})$ for all $k = 1, \ldots, p - 1$. We can then consider the products

$$\lambda_{j_1}\lambda_{j'_1} \cdots \lambda_{j'_{p-1}}, \ldots, \lambda_{j_{n-s}}\lambda_{j'_1} \cdots \lambda_{j'_{p-1}};$$

each of them (up to a non-zero constant) is a p-minor of $\boldsymbol{L}$, so they appear as elements in the sequence $(a_{s+1}, \ldots, a_m)$, say as $(a_{e_1}, \ldots, a_{e_{n-s}})$. By the remark of the previous paragraph, in the local ring at $\boldsymbol{x}$, up to non-zero constants, these polynomials are respectively equal to the linear forms $\lambda_{j_1,k_1}, \ldots, \lambda_{j_{n-s},k_{n-s}}$.

To summarize, we have found that the linear equations $(\lambda_{j_1,k_1}, \ldots, \lambda_{j_{n-s},k_{n-s}})$ and $(\mu_{1,u_1}, \ldots, \mu_{s,u_s})$ belong to the ideal $\langle \boldsymbol{A} \rangle_{\mathfrak{m}}$, where $\mathfrak{m}$ is the maximal ideal at $\boldsymbol{x}$. As a result, the Jacobian matrix of $\boldsymbol{A}$ must be invertible at $\boldsymbol{x}$, and C_2 holds.

Example 6.2.2. Let us see how the discussion above allows us to find all solutions to the system $\boldsymbol{A}$ from Example 6.2.1.

Since $s = 0$, we do not need to involve indices $\boldsymbol{u}$ in our discussion: the matrix $\boldsymbol{L}$ given in that example has rank less than 2 at $\boldsymbol{x}$ if and only if one of the conditions $\lambda_1(\boldsymbol{x}) = \lambda_2(\boldsymbol{x}) = 0$, $\lambda_1(\boldsymbol{x}) = \lambda_3(\boldsymbol{x}) = 0$, or $\lambda_2(\boldsymbol{x}) = \lambda_3(\boldsymbol{x}) = 0$ holds. Since each λ_i is a product of two linear forms, we obtain a total of $3 \cdot 4 = 12$ points in $V(\boldsymbol{A})$, namely

$$(-11/2, 7/2), (-13/3, 14/3), (-2, 7/3), (-8/11, 91/11), (2/27, 7/27),$$
$$(/4, -3/2), (6/13, -47/13), (4/3, -1), (11/7, 8/7), (2, 1), (3, 4), (11, 20).$$

At this stage, we have established all assumptions necessary to apply Proposition 5.2.1 and Proposition 5.2.7. We deduce that the sum of the multiplicities of the isolated solutions of $\boldsymbol{C} = \boldsymbol{B}_{t=1}$ is at most c, where c is the number of solutions of $\boldsymbol{A} = \boldsymbol{B}_{t=0}$.

Lemma 6.2.3. *Under the above assumptions,* $c = \gamma_1 \cdots \gamma_s \eta_{n-s}(\delta_1, \ldots, \delta_q)$ *where* η_{n-s} *is the* $(n-s)$*-th elementary symmetric polynomial.*

Proof. The estimation of c is trivial: there are $\gamma_1 \cdots \gamma_s$ choices of $\boldsymbol{u}$ and $\eta_{n-s}(\delta_1, \ldots, \delta_q)$ ways to choose indices $\boldsymbol{j}$ and $\boldsymbol{k}$. □

This proves the first part of Proposition 6.2.1.

6.2.5 Setting up parameters

In order to apply the homotopy algorithms of Propositions 5.2.11 and 5.2.12, we now need to ensure that we can prepare the three inputs they need: a straight-line program for $\boldsymbol{B}$, a zero-dimensional representation of the solutions of $\boldsymbol{A} = \boldsymbol{B}_{t=0}$ and an upper bound on the degree of the homotopy curve.

A zero-dimensional parametrization $\mathscr{R}_0$ of $V(\boldsymbol{A})$. We compute $\mathscr{R}_0$ by following the description of the solutions of $\boldsymbol{A}$ given in the previous paragraphs. For any choice of indices $\boldsymbol{u}, \boldsymbol{j}$, and $\boldsymbol{k}$ as above, the corresponding point $\boldsymbol{x} \in \overline{\mathbb{K}}^n \cap V(\boldsymbol{A})$ can be computed by solving the square linear system of size n. This system can be solve in time $O(n^3)$. In total, we need to solve c such systems, then the total cost of $O(c\, n^3)$ operations in $\mathbb{K}$.

Knowing all the points of $V(\boldsymbol{A})$, we can construct a zero-dimensional parametrization $\mathscr{R}_0$ such that $Z(\mathscr{R}_0) = V(\boldsymbol{A})$ in time $O^{\sim}(cn)$ by means of fast interpolation [80, Chapter 10]. The total cost hence is in $O(cn^3)$ operations in $\mathbb{K}$.

An upper bound on the degree of the homotopy curve. Let us write $V(\boldsymbol{B}) = V(J') \cup V' \cup V''$, where J' is the union of the one-dimensional irreducible components of $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$ whose images by the projection onto the first coordinate are Zariski dense, V' is the union of the other components of dimension one of $V(\boldsymbol{B})$, and V'' is the union of the components of higher dimension. We need to determine an upper bound e on the degree of the curve $V(J')$.

Let $H = h_0 + h_1 x_1 + \cdots + h_n x_n + h_{n+1} t$ be a generic hyperplane in coordinates $(t, x_1, \ldots, x_n)$. Then, $(V(J') \cup V') \cap V(H)$ is a finite set consisting of $\deg(V(J')) + \deg(V')$ points, whereas $V'' \cap V(H)$ consists only of components of positive dimension; these two sets are disjoint. Thus, we can take for e the number of isolated points of $V(\boldsymbol{B}) \cap V(H)$. The hyperplane H allows us to rewrite t as

$$\wp(x_1, \ldots, x_n) = -(h_0 + h_1 x_1 + \cdots + h_n x_n)/h_{n+1}.$$

The points in $V(\boldsymbol{B}) \cap V(H)$ are thus in one-to-one correspondence with the solutions of the system $(\beta_1, \ldots, \beta_s, \ldots, \beta_m)$, where $\beta_i = b_i(\wp(\boldsymbol{X}), \boldsymbol{X})$ and $(\beta_{s+1}, \ldots, \beta_m)$ are the

p-minors of $\boldsymbol{U}'$, following the ordering $\succ$, where

$$\boldsymbol{U}' = (1 - \wp(\boldsymbol{X})) \cdot \boldsymbol{L} + \wp(\boldsymbol{X}) \cdot \boldsymbol{F} \in \mathbb{K}[\boldsymbol{X}]^{p \times q}.$$

The degrees of $(\beta_1, \ldots, \beta_s)$ are $(\gamma_1 + 1, \ldots, \gamma_s + 1)$ and the column degrees of $\boldsymbol{U}'$ are $(\delta_1 + 1, \ldots, \delta_q + 1)$. We can then apply Proposition 5.2.1 which shows we can take for

$$e = (\gamma_1 + 1) \cdots (\gamma_s + 1)\eta_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1).$$

A straight-line program for $\boldsymbol{B}$. Finally, we need to estimate the size of a straight-line program that computes $\boldsymbol{B} = (b_1, \ldots, b_m)$, assuming that we are given a straight-line program Γ of size σ that computes polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ and the entries of $\boldsymbol{F}$.

For $i = 1, \ldots, s$, $b_i = (1 - t)a_i + tg_i$ where a_i is a product of γ_i linear forms in n variable. The polynomial a_i can be computed in $O(n\gamma_i)$ operations in $\mathbb{K}$, hence with a total of $O(n(\gamma_1 + \cdots + \gamma_s))$ operations for $(a_1, \ldots, a_s)$, and $O(\sigma + n(\gamma_1 + \cdots + \gamma_s))$ for $(b_1, \ldots, b_s)$.

For $i = s + 1, \ldots, m$, b_i are the p-minors of $\boldsymbol{U} = (1 - t) \cdot \boldsymbol{L} + t \cdot \boldsymbol{F}$. The polynomials $\lambda_1, \ldots, \lambda_q$ can be computed in $O(n(\delta_1 + \cdots + \delta_q))$ operations, so that the entries of $\boldsymbol{U}$ can be computed in $O(\sigma + n(\delta_1 + \cdots + \delta_q))$ operations. From that, all p-minors of $\boldsymbol{U}$ can be deduced in $O(\binom{q}{p}n^3)$ further steps. To summarize, all polynomials in $\boldsymbol{B}$ can be computed by a straight-line program of size $O(\sigma + \binom{q}{p}n^3 + n(\gamma_1 + \cdots + \gamma_s + \delta_1 + \cdots + \delta_q))$.

Example 6.2.3. In our running example, starting from the points given in Example 6.2.2, we obtain the zero-dimensional parametrization $\mathscr{R}_0 = ((w_0, v_{0,1}, v_{0,2}), x_2)$ for $V(\boldsymbol{A})$, with

$$\begin{aligned}
w_0 = {} & y^{12} - \frac{1055660}{27027}y^{11} + \frac{53137069}{108108}y^{10} - \frac{1093435073}{486486}y^9 - \frac{820013219}{972972}y^8 + \frac{18538617847}{486486}y^7 \\
& - \frac{2418753031}{24948}y^6 - \frac{1649924501}{162162}y^5 + \frac{1528208159}{5148}y^4 - \frac{16255281049}{69498}Y^3 - \frac{5525925412}{34749}y^2 \\
& + \frac{7236468568}{34749}y - \frac{36111040}{891}, \\
v_{0,1} = {} & \frac{770785}{108108}y^{11} - \frac{20800447}{216216}y^{10} + \frac{50442596}{81081}y^9 - \frac{28536694169}{5837832}y^8 + \frac{30893680099}{1459458}y^7 + \frac{3580073831}{216216}y^6 - \\
& \frac{8167305065}{27027}y^5 + \frac{73892907181}{176904}y^4 + \frac{60113381407}{138996}y^3 - \frac{13255132849}{16038}y^2 + \frac{23446514308}{104247}y - \frac{5841976}{1287}, \\
v_{0,2} = {} & \frac{1055660}{27027}y^{11} - \frac{53137069}{54054}y^{10} + \frac{1093435073}{162162}y^9 + \frac{820013219}{243243}y^8 - \frac{92693089235}{486486}y^7 + \frac{2418753031}{4158}y^6 \\
& + \frac{1649924501}{23166}y^5 - \frac{3056416318}{1287}y^4 + \frac{16255281049}{7722}y^3 + \frac{55259254120}{34749}y^2 - \frac{7236468568}{3159}y + \frac{144444160}{297}.
\end{aligned}$$

The degree bound for the homotopy curve is $e = 3 \cdot 3 + 3 \cdot 3 + 3 \cdot 3 = 36$.

6.2.6 Completing the cost analysis

We can now apply Proposition 5.2.11 and Proposition 5.2.12 to find the isolated solutions and the simple points of $V_p(\boldsymbol{F}, \boldsymbol{G})$, respectively.

Algorithms in Proposition 5.2.11 have runtime is $O^{\sim}(c^5 m n^2 + c(e+c^5)n(\sigma' + n^3))$ operations in $\mathbb{K}$. Since $m \leq n + \binom{q}{p}$, this complexity can be simplified as

$$O^{\sim}\left(c(e+c^5)n\left(\sigma + \binom{q}{p}n^3 + n(\gamma_1 + \cdots + \gamma_s + \delta_1 + \cdots + \delta_q)\right)\right).$$

Since $s \leq n$, $\gamma = \max(\gamma_1, \ldots, \gamma_s)$, and $\delta = \max(\delta_1, \ldots, \delta_q)$, our bound becomes

$$O^{\sim}\left(c(e+c^5)n(\sigma + \binom{q}{p}n^3 + n^2\gamma + nq\delta)\right).$$

This can also be rewritten as

$$O^{\sim}\left(c(e+c^5)(\sigma + \binom{q}{p}n^3 + n^2\gamma + nq\delta)\right),$$

since one easily checks that $e \geq 2^n$ (because by assumption we have $\gamma_i \geq 1$ and $\delta_i \geq 1$), so that $n \in O^{\sim}(e)$. A last factorization shows that the bound can be simplified to

$$O^{\sim}\left(\binom{q}{p}c(e+c^5)n^3(\sigma + \gamma + q\delta)\right).$$

Using again that $n \leq \log_2(e)$, we can omit the factor n^3 from the $O^{\sim}(\ )$, and we conclude the proof of Proposition 6.2.1. The resulting algorithm is called ColumnDegree.

Finally, to prove Proposition 6.2.2, we design an algorithm called ColumnDegree_simple, which differs from ColumnDegree only at the last step, where Algorithm Homotopy_simple is called instead of Homotopy. One applies Proposition 5.2.12, which yields a runtime $O^{\sim}(c^2\, m\, n^2 + c\, e\, n(\sigma' + n^2))$ operations in $\mathbb{K}$. Using again $m \leq n + \binom{q}{p} \leq n\binom{q}{p}$, and $\sigma' = O(\sigma + \binom{q}{p}n^3 + n(n\gamma + q\delta))$, we obtain as a bound

$$O^{\sim}\left(\binom{q}{p}\, c^2\, n^3 + c\, e\, n(\sigma + \binom{q}{p}n^3 + n^2\gamma + nq\delta)\right),$$

which we simplify as

$$O^{\sim}\left(\binom{q}{p}c\, e\, n^4(\sigma + \gamma + q\delta)\right),$$

taking into account that $c \leq e$. Since $e \geq 2^n$, the term n^4 can be absorbed in the $O^{\sim}(\ )$. This concludes the proof of Proposition 6.2.2.

Example 6.2.4. We apply the symbolic homotopy algorithm to the system $\boldsymbol{B} = (b_1, b_2, b_3)$ of 2×2 minors of matrix $\boldsymbol{U} = (1-t) \cdot \boldsymbol{L} + t \cdot \boldsymbol{F}$, where $\boldsymbol{F}$ is as in Example 4.3.1 and $\boldsymbol{L}$ as in Example 6.2.1.

Starting from $\mathscr{R}_0$ as obtained in Example 6.2.3, we obtain a zero-dimensional parametrization $\mathscr{S}$ of degree 12 with coefficients in $\mathbb{Q}(t)$ that describes the homotopy curve defined

Algorithm 5 ColumnDegree(Γ)

Input: a straight-line program Γ of length σ that computes

- $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with $\deg(f_{i,j}) \leq \delta_j$ for all j and $p \leq q$
- polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$, with $n = q - p + s + 1$

Output: a zero-dimensional parametrization of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

1. for any sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, with $u_i \in \{1, \ldots, \gamma_i\}$ for all i
   (a) for any subsequence $\boldsymbol{j} = (j_1, \ldots, j_{n-s})$ of $(1, \ldots, q)$
      i. for any sequence $\boldsymbol{k} = (k_1, \ldots, k_{n-s})$, with k_i in $\{1, \ldots, \delta_{j_i}\}$ for all i
         - compute a zero-dimensional parametrization $\mathscr{R}_{\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}}$ of the solution of the system

$$\mu_{1,u_1} = \cdots = \mu_{s,u_s} = \lambda_{j_1,k_1} = \cdots = \lambda_{j_{n-s},k_{n-s}} = 0$$

cost: $O(cn^3)$, with $c = \gamma_1 \cdots \gamma_s \eta_{n-s}(\delta_1, \ldots, \delta_q)$

2. combine all $(\mathscr{R}_{\boldsymbol{u},\boldsymbol{j},\boldsymbol{k}})_{\boldsymbol{u},\boldsymbol{j},\boldsymbol{k}}$ into a zero-dimensional parametrization $\mathscr{R}_0$

cost: $O\tilde{}(cn)$

3. construct a straight-line program Γ' that computes all polynomials $\boldsymbol{B}$

length of Γ' is $\sigma' = O(\sigma + \binom{q}{p} n^3 + n(\alpha_1 + \cdots + \alpha_p) + n(\gamma_1 + \cdots + \gamma_s))$

4. return Homotopy($\Gamma', \mathscr{R}_0, e$)

cost: $O\tilde{}\,(c^5 m n^2 + c(e + c^5) n(\sigma' + n^3))$,
with $e = (\gamma_1 + 1) \cdots (\gamma_s + 1) \eta_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1)$

---

by $\boldsymbol{B} = 0$. The polynomials in $\mathscr{S}$ are too large to be displayed here, all the more as we are only interested in the points that $\mathscr{S}$ describes in the limit $t \to 1$.

Note that one cannot simply substitute $t = 1$ in $\mathscr{S}$, since most denominators vanish. Instead, we apply the procedure in [155] which is recalled in Lemma 3.7.9, which in this case amounts to multiplying the polynomials in $\mathscr{S}$ by $(t-1)^5$ before applying the substitution $t = 1$. This leaves us with a zero-dimensional parametrization of degree $12 - 5 = 7$, which is precisely the one given in Example 4.3.2.

6.3 The row-degree homotopy

In this section, we are going to finish our proof for the second halves of Theorem 4.2.1, Theorem 4.2.2, and Theorem 4.2.3 by using the homotopy algorithms and taking into

Algorithm 6 ColumnDegree_simple(Γ)

Input: a straight-line program Γ of length σ that computes

- $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with $\deg(f_{i,j}) \leq \delta_j$ for all j and $p \leq q$
- polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$, with $n = q - p + s + 1$

Output: a zero-dimensional parametrization of the simple points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

1. run steps 1. to 3. of ColumnDegree(Γ) to have Γ' and $\mathscr{R}_0$
2. return Homotopy_simple($\Gamma', \mathscr{R}_0, e$)

cost: $O^{\sim}\left(c^2 mn^2 + cen(\sigma' + n^2)\right)$

with $e = (\gamma_1 + 1) \cdots (\gamma_s + 1)\eta_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1)$

account the row-degree structure of our matrices.

Suppose we are given a matrix $\boldsymbol{F} = [f_{i,j}] \in \mathbb{K}[\boldsymbol{X}]^{p \times q}$ with $\boldsymbol{X} = (x_1, \ldots, x_n)$ and polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[\boldsymbol{X}]$ such that $p \leq q$ and $n = q - p + s + 1$, and we want to compute either the isolated points or the simple points of $V_p(\boldsymbol{F}, \boldsymbol{G})$, with

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = \{\boldsymbol{x} \in \overline{\mathbb{K}}^n \mid \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p \text{ and } g_1(\boldsymbol{x}) = \cdots = g_s(\boldsymbol{x}) = 0\}.$$

In this case we want to exploit the row-degree structure of $\boldsymbol{F}$. For this purpose, we define $\alpha_i = \operatorname{rdeg}(\boldsymbol{F}, i)$ for $i = 1, \ldots, p$, write $\gamma_k = \deg(g_k)$ for $k = 1, \ldots, s$, and let $\alpha = \max(\alpha_1, \ldots, \alpha_p)$ and $\gamma = \max(\gamma_1, \ldots, \gamma_s)$.

Our result is the following propositions. The first one gives the complexity for computing the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$, while the second proposition contains the complexity result to find the simple points of the same set. Recall that $h_{n-s}(\cdot)$ is the complete homogeneous symmetric function of degree $n - s$.

Proposition 6.3.1. *The sum of the multiplicities of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$ is at most $c' = \gamma_1 \cdots \gamma_s h_{n-s}(\alpha_1, \ldots, \alpha_p)$.*

Suppose that the matrix $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ and the polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ are given by a straight-line program of length σ. Assume that all γ_i's and α_j's are at least equal to 1. Then, there exists a randomized algorithm called RowDegree *that computes the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$ using*

$$O^{\sim}\left(\binom{q}{p} c'(e' + c'^5)(\sigma + \gamma + p\alpha)\right)$$

operations in $\mathbb{K}$, where

$$e' = (\gamma_1 + 1) \cdots (\gamma_s + 1) h_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1),$$
$$\gamma = \max(\gamma_1, \ldots, \gamma_s), \text{ and } \delta = \max(\delta_1, \ldots, \delta_q).$$

Proposition 6.3.2. *Reusing the notations introduced above, there exists a randomized algorithm which is called* RowDegree_simple *that computes the simple points of* $V_p(\boldsymbol{F}, \boldsymbol{G})$ *using*

$$O^{\sim}\left(\binom{q}{p} c'e'(\sigma+\gamma+p\alpha)\right)$$

operations in $\mathbb{K}$.

Before giving a detailed description for our algorithms, we set up some necessary material for the row-degree homotopy algorithms.

6.3.1 Preliminaries for the row-degree homotopy

In this subsection, we work with two families of matrices of size $p \times q$, with $p \leq q$, and with all entries being polynomials in $n = q - p + 1$ variables. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ be positive integers. The first matrices we consider are

$$\boldsymbol{P}^H = \begin{pmatrix} \lambda_{1,1}^H & \lambda_{1,2}^H & \cdots & \lambda_{1,q}^H \\ \lambda_{2,1}^H & \lambda_{2,2}^H & \cdots & \lambda_{2,q}^H \\ \vdots & & & \vdots \\ \lambda_{p,1}^H & \lambda_{p,2}^H & \cdots & \lambda_{p,q}^H \end{pmatrix} \tag{6.3}$$

and matrices of a more specialized kind of the form

$$\boldsymbol{L}^H = \begin{pmatrix} \lambda_{1,1}^H & 0 & \cdots & 0 & \lambda_{1,p+1}^H & \cdots & \lambda_{1,q}^H \\ 0 & \lambda_{2,2}^H & \cdots & 0 & \lambda_{2,p+1}^H & \cdots & \lambda_{2,q}^H \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p}^H & \lambda_{p,p+1}^H & \cdots & \lambda_{p,q}^H \end{pmatrix}, \tag{6.4}$$

where the ^{H} superscript indicates that all entries are homogeneous. In both cases, for all i, j, the entry $\lambda_{i,j}^H$ is a product of α_i homogeneous linear forms in $n+1$ variables $x_0, x_1, \ldots, x_n$ with coefficients in $\mathbb{K}$ (except when $\lambda_{i,j}^H$ is explicitly set to zero in the second case), that is, $\lambda_{i,j}^H = \prod_{k=1}^{\alpha_i} \lambda_{i,j,k}^H$. In this subsection, we are interested in describing the projective algebraic sets in $\mathbb{P}^n(\overline{\mathbb{K}})$.

In what follows, for any matrix $A \in R^{m \times n}$, where R is a ring, and sequences of integers S, U, we denote by $A_{S,U}$ the submatrix of A obtained by keeping rows indexed by S and columns indexed by U. We define A^H is the homogenization of A, and for any integer r, we use the notation $V_r(A^H)$ to denote the projective algebraic set in $\mathbb{P}^n(\overline{\mathbb{K}})$ defined by the r-minors of A^H.

Proposition 6.3.3. *For generic choices of the coefficients of the linear forms* $\lambda_{i,j,k}^H$*, the following holds.*

(i) *The projective algebraic sets* $V_p(\boldsymbol{P}^H)$ *and* $V_p(\boldsymbol{L}^H)$ *have no solution at infinity (that is, with* $x_0 = 0$*).*

(ii) *The Jacobian matrices of the sets of* p*-minors of* $\boldsymbol{P}^H$*, resp. of* $\boldsymbol{L}^H$*, has rank* n *at every point in* $V_p(\boldsymbol{P}^H)$*, resp.* $V_p(\boldsymbol{L}^H)$*.*

The rest of this subsection is devoted to proving this proposition. Our strategy is to work all along with linear forms with indeterminate coefficients, and establish the properties we want in this context.

Let $\mathcal{A} = q(n+1)(\alpha_1 + \cdots + \alpha_p)$ be the number of coefficients needed to define homogeneous linear forms $\lambda^H_{i,j,k}$ in $x_0, \ldots, x_n$, for $i = 1, \ldots, p$, $j = 1, \ldots, q$ and $k = 1, \ldots, \alpha_i$. If needed, we will write $\mathcal{A} = \mathcal{A}(\boldsymbol{\alpha}, q)$ to make the dependency in $\boldsymbol{\alpha}$ and q explicit. Let then $\mathfrak{Q}$ be the sequence of $\mathcal{A}$ indeterminates, that is, $\mathfrak{Q} = (\mathfrak{l}_{i,j,k,r})$, for i, j, k as above and $r = 0, \ldots, n$, and define

$$\mathfrak{l}^H_{i,j,k} = \mathfrak{l}_{i,j,k,0}x_0 + \mathfrak{l}_{i,j,k,1}x_1 + \cdots + \mathfrak{l}_{i,j,k,n}x_n,$$

as well as

$$\mathfrak{l}^H_{i,j} = \mathfrak{l}^H_{i,j,1} \cdots \mathfrak{l}^H_{i,j,\alpha_i} \in \mathbb{K}[\mathfrak{Q}][x_0, \ldots, x_n].$$

From now on, we will denote by $\boldsymbol{X}'$ the set of variables $(x_0, \ldots, x_n)$. We can then define the matrix

$$\mathfrak{P}^H(\boldsymbol{\alpha}, q) = \begin{bmatrix} \mathfrak{l}^H_{1,1} & \cdots & \mathfrak{l}^H_{1,q} \\ \vdots & & \vdots \\ \mathfrak{l}^H_{p,1} & \cdots & \mathfrak{l}^H_{p,q} \end{bmatrix} \in \mathbb{K}[\mathfrak{Q}][\boldsymbol{X}']^{p \times q}. \tag{6.5}$$

We remark that for any i, j, $\mathfrak{l}^H_{i,j}$ has degree α_i in $\boldsymbol{X}'$ and $\mathfrak{P}^H$ is the generic model of the matrix $\boldsymbol{P}^H$ in (6.3).

Given $\Lambda = (\lambda_{i,j,k,r}) \in \overline{\mathbb{K}}^{\mathcal{A}}$, for any polynomial $\mathfrak{f}$ in $\mathbb{K}(\mathfrak{Q})[\boldsymbol{X}']$, we write $\Theta_\Lambda(\mathfrak{f})$ in $\mathbb{K}[\boldsymbol{X}']$ for the polynomial obtained by evaluating $\mathfrak{l}_{i,j,k,r}$ at $\lambda_{i,j,k,r}$, for all indices i, j, k, r as above, as long as no denominator vanishes through this evaluation; the notation extends to polynomial matrices. More generally, for a field $\mathbb{L}$ containing $\mathbb{K}$, and Λ in $\mathbb{L}^{\mathcal{A}}$, the notation $\Theta_\Lambda(\mathfrak{f})$ is defined similarly.

We also define the generic model of the matrix $\boldsymbol{L}^H$ in (6.4). Let $\mathcal{A}' = n(n+1)(\alpha_1 + \cdots + \alpha_p)$; as above, we will write $\mathcal{A}' = \mathcal{A}'(\boldsymbol{\alpha}, q)$ when needed. Let $\mathfrak{Q}' = (\mathfrak{l}_{i,j,k,r}) \subset \mathfrak{Q}$ be the sequence of $\mathcal{A}'$ indeterminates, for indices i, j, k, r as follows: i is in $\{1, \ldots, p\}$, j is in $\{i, p+1, \ldots, q\}$, and as previously, k is in $\{1, \ldots, \alpha_i\}$ and r is in $\{0, \ldots, n\}$. Note that the polynomials $\mathfrak{l}^H_{i,j}$, for i, j as above, are in $\mathbb{K}[\mathfrak{Q}'][\boldsymbol{X}'] \subset \mathbb{K}[\mathfrak{Q}][\boldsymbol{X}']$, and allow us to define

$$\mathfrak{L}^H(\boldsymbol{\alpha}, q) = \begin{bmatrix} \mathfrak{l}^H_{1,1} & 0 & 0 & \mathfrak{l}^H_{1,p+1} & \cdots & \mathfrak{l}^H_{1,q} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \mathfrak{l}^H_{p,p} & \mathfrak{l}^H_{p,p+1} & \cdots & \mathfrak{l}^H_{p,q} \end{bmatrix} \in \mathbb{K}[\mathfrak{Q}'][\boldsymbol{X}']^{p \times q}. \tag{6.6}$$

For $\Lambda' \in \overline{\mathbb{K}}^{\mathcal{A}'}$ and $\mathfrak{f} \in \mathbb{K}(\mathfrak{Q}')[\boldsymbol{X}']$, the polynomial $\Theta_{\Lambda'}$ in $\mathbb{K}[\boldsymbol{X}']$ is defined as in the case of polynomials $\mathfrak{f}$ over $\mathbb{K}(\mathfrak{Q})[\boldsymbol{X}']$.

The basic ideal behind the proofs below is the following: to prove that a property such as rank-deficiency holds for a matrix $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$, we prove that it holds for a matrix of the form $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$, and then use an openness property to conclude our claim. To prove that property for the latter matrices, we proceed by induction, relying on the presence of the left-hand diagonal block.

Setting up the recurrences.

As we have seen in Lemma 3.2.3, for a matrix such as $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ to be rank-deficient at $\boldsymbol{x}' \in \mathbb{P}^n(\overline{\mathbb{K}(\mathfrak{L}')})$, at least one of $\mathfrak{l}^H_{1,1}, \ldots, \mathfrak{l}^H_{p,p}$ must vanish at $\boldsymbol{x}'$. For instance, suppose that

$$\mathfrak{l}^H_{1,1}(\boldsymbol{x}') = \mathfrak{l}^H_{2,2}(\boldsymbol{x}') = 0, \tag{6.7}$$

while all other terms are non-zero. Then, the submatrix $\mathfrak{L}^H_{((1,2),(p+1,\ldots,q))}(\boldsymbol{\alpha}, q)$ of $\mathfrak{L}^H(\boldsymbol{\alpha}, q))$ itself must be rank-deficient at $\boldsymbol{x}'$. The constraints in (6.7) give us two linear equations, which allow us to eliminate two coordinates of $\boldsymbol{x}'$, say x_n and x_{n-1}. We can perform the corresponding substitution in the above submatrix, and we are left with a matrix of size $2 \times (n-1)$ that is of the form $\mathfrak{P}^H((\alpha_1, \alpha_2), n-1)$ in $\mathbb{K}[\mathfrak{H}][x_0, \ldots, x_{n-2}]^{2\times(q-p)}$, for some vector of coefficients $\mathfrak{H}$ obtained through the elimination of x_n and x_{n-1}. We can then invoke our induction assumption on the latter matrix $\mathfrak{P}^H((\alpha_1, \alpha_2), n-1)$.

To formalize this process, for a subsequence $\boldsymbol{i} = (i_1, \ldots, i_k)$ of $(1, \ldots, p)$, we call the submatrix of $\mathfrak{L}^H_{(\boldsymbol{i},(p+1,\ldots,q))}(\boldsymbol{\alpha}, q)$ the submatrix of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ *associated* to $\boldsymbol{i}$; it consists of the rows of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ indexed by $\boldsymbol{i}$ and columns $p+1, \ldots, q$. For such an $\boldsymbol{i}$, we let $R_{\boldsymbol{i}}$ be the set of all tuples $\boldsymbol{r} = (r_1, \ldots, r_k)$, with r_s in $\{1, \ldots, \alpha_{i_s}\}$ for $s = 1, \ldots, k$; for any s in $\{1, \ldots, k\}$, r_s will be the index of the factor $\mathfrak{l}^H_{i_k,i_k,r_s}$ of $\mathfrak{l}^H_{i_k,i_k}$ we cancel. For given $\boldsymbol{i}$ and $\boldsymbol{r}$, we will let $\mathfrak{Q}'_{\boldsymbol{i},\boldsymbol{r}} \subset \mathfrak{Q}'$ be the indeterminates corresponding to the coefficients of $\mathfrak{l}^H_{i_1,i_1,r_1}, \ldots, \mathfrak{l}^H_{i_k,i_k,r_k}$, and of all entries $\mathfrak{l}^H_{i_1,p+1}, \ldots, \mathfrak{l}^H_{i_k,q}$ of the submatrix $\mathfrak{L}^H_{(\boldsymbol{i},(p+1,\ldots,q))}(\boldsymbol{\alpha}, q)$ associated to $\boldsymbol{i}$ in $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$.

Example 6.3.1. Let $p = 3, q = 6$, and $n = 4$. Consider $\boldsymbol{i} = (1, 2) \subset (1, 2, 3)$. The submatrix $\mathfrak{L}^H((\alpha_1, \alpha_2, \alpha_3), 3)$ associated to $\boldsymbol{i}$ is the green part of $\mathfrak{L}^H$.

$$\mathfrak{L}^H = \begin{bmatrix} \times & & & \times & \times & \times \\ & \times & & \times & \times & \times \\ & & \times & \times & \times & \times \end{bmatrix}$$

If we consider $\alpha_1 = 1$ and $\alpha_2 = 2$, then $R_{\boldsymbol{i}} = \{(1, 1), (1, 2)\}$. In particular, for $\boldsymbol{r} = (1, 1) \in R_{\boldsymbol{i}}$, one has $\mathfrak{Q}'_{\boldsymbol{i},\boldsymbol{r}} = (\mathfrak{l}_{1,1,1,0}, \ldots, \mathfrak{l}_{1,1,1,4}, \mathfrak{l}_{2,2,1,0}, \ldots, \mathfrak{l}_{2,2,1,4}) \cup (\mathfrak{l}_{1,j,1,0}, \ldots, \mathfrak{l}_{1,j,1,4})_{4\leq j\leq 6} \cup (\mathfrak{l}_{2,j,1,0}, \ldots, \mathfrak{l}_{2,j,1,4})_{4\leq j\leq 6} \cup (\mathfrak{l}_{2,j,2,0}, \ldots, \mathfrak{l}_{2,j,2,4})_{4\leq j\leq 6}$.

By using Gaussian elimination, we can rewrite the linear equations $\mathfrak{l}^H_{i_1,i_1,r_1} = \cdots = \mathfrak{l}^H_{i_k,i_k,r_k} = 0$ as

$$x_{n-k+1} = \mathfrak{f}_{n-k+1,\boldsymbol{i},\boldsymbol{r}}(x_0,\dots,x_{n-k}),\dots,x_n = \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(x_0,\dots,x_{n-k}), \tag{6.8}$$

for some homogeneous linear forms $\mathfrak{f}_{n-k+1,\boldsymbol{i},\boldsymbol{r}},\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}$ of $(x_0,\dots,x_{n-k})$ with coefficients in $\mathbb{K}(\mathfrak{Q}'_{\boldsymbol{i},\boldsymbol{r}})$. Applying this substitution in the entries of the submatrix of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$ associated to $\boldsymbol{i}$ gives us the $k\times(q-p)$ matrix $\mathfrak{P}^H(\boldsymbol{\alpha_i},q-p)$ in $\mathbb{K}[\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}},\tilde{\boldsymbol{X}}']$, with $\boldsymbol{\alpha_i}=(\alpha_{i_1},\dots,\alpha_{i_k})$, whose entries are products of homogeneous linear forms in $\tilde{\boldsymbol{X}}'=(x_0,\dots,x_{n-k})$, and where $\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}$ is a vector of $\mathcal{A}(\boldsymbol{\alpha_i},q-p)$ elements in $\mathbb{K}(\mathfrak{Q}'_{\boldsymbol{i},\boldsymbol{r}})$. Recall that $n=q-p+1$, so $q-p=n-1$.

The main result we will use in this subsubsection is the following lemma, which summarizes how the above process allows us to describe the projective zero-set of t-minors of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$, for any $t\le p$. This will be the basis of several recursions.

Lemma 6.3.4. *For t in $\{1,\dots,p\}$, $V_t(\mathfrak{L}^H_{\boldsymbol{\alpha},q})\subset\mathbb{P}^n(\overline{\mathbb{K}(\mathfrak{Q}')})$ is the union of the sets*

$$\left\{(\tilde{\boldsymbol{x}}',\mathfrak{f}_{n-k+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'),\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'))\mid\tilde{\boldsymbol{x}}'\in V_{k-(p-t)}(\mathfrak{P}^H(\boldsymbol{\alpha_i},n-1))\subset\mathbb{P}^{n-k}(\overline{\mathbb{K}(\mathfrak{Q}')})\right\}, \tag{6.9}$$

for $\boldsymbol{i}=(i_1,\dots,i_k)$ of length $k\in\{p-t+1,\dots,\min(p,n-1)\}$ and $\boldsymbol{r}$ in $R_{\boldsymbol{i}}$, and with $\tilde{\boldsymbol{X}}'=(x_0,\dots,x_{n-k})$, together with

$$\{(1,\mathfrak{f}_{1,\boldsymbol{i},\boldsymbol{r}}(1),\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(1))\}$$

if $t=p$ and $n\le p$, with $\boldsymbol{i}=(i_1,\dots,i_n)$ and $\boldsymbol{r}$ in $R_{\boldsymbol{i}}$.

We have to write a special case for $t=p$ and $n\le p$ in the last part of the lemma, since taking $\boldsymbol{i}=(i_1,\dots,i_n)$ of length $k=n$ in (6.9) would lead us to consider points in $\mathbb{P}^0(\overline{\mathbb{K}(\mathfrak{Q}')})$.

Proof. Similar to result in Lemma 3.2.3, a point $\tilde{\boldsymbol{x}}\in\mathbb{P}^n(\overline{\mathbb{K}(\mathfrak{Q}')})$ belongs to $V_t(\mathfrak{L}^H(\boldsymbol{\alpha},q))$ if and only if some diagonal terms of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$ vanish at $\tilde{\boldsymbol{x}}$, say $\mathfrak{l}^H_{i_1,i_1}(\tilde{\boldsymbol{x}})=\cdots=\mathfrak{l}^H_{i_k,i_k}(\tilde{\boldsymbol{x}})=0$ (all other $\mathfrak{l}^H_{i,i}(\tilde{\boldsymbol{x}})$ being non-zero), and if the submatrix $\mathfrak{L}^H_{\boldsymbol{i},(p+1,\dots,q)}(\boldsymbol{\alpha},q)$ associated to $\boldsymbol{i}=(i_1,\dots,i_k)$ has rank less than $t-(p-k)$ at $\tilde{\boldsymbol{x}}$. In particular, we must have $t-(p-k)>0$, that is, $k\ge p-t+1$.

For $s=1,\dots,k$, $\mathfrak{l}^H_{i_s,i_s}(\tilde{\boldsymbol{x}})=0$ if and only if there exists r_s in $\{1,\dots,\alpha_{i_s}\}$ such that $\mathfrak{l}^H_{i_s,i_s,r_s}(\tilde{\boldsymbol{x}})=0$. Thus, $\tilde{\boldsymbol{x}}$ is in $V_t(\mathfrak{L}^H_{\boldsymbol{\alpha},q})$ if and only if there exists a subsequence $\boldsymbol{i}=(i_1,\dots,i_k)$ of $(1,\dots,p)$, with $k\ge p-t+1$, and $\boldsymbol{r}=(r_1,\dots,r_k)$ in $R_{\boldsymbol{i}}$ such that $\mathfrak{l}^H_{i_1,i_1,r_1}(\tilde{\boldsymbol{x}})=\cdots=\mathfrak{l}^H_{i_k,i_k,r_k}(\tilde{\boldsymbol{x}})=0$ and the submatrix of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$ associated to $\boldsymbol{i}$ has rank less than $k-(p-t)$ at $\tilde{\boldsymbol{x}}$.

Applying (6.8), we deduce that the coordinates $(\tilde{x}_0,\dots,\tilde{x}_n)$ of $\tilde{\boldsymbol{x}}$ satisfy

$$\tilde{x}_{n-k+1}=\mathfrak{f}_{n-k+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'),\dots,\tilde{x}_n=\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'),$$

with $\tilde{\boldsymbol{x}}' = (\tilde{x}_0, \ldots, \tilde{x}_{n-k})$. In particular, $k \leq n$, since otherwise this linear system would have no solution. Recall that the coefficients are algebraically independent indeterminates. Remark also that $\tilde{\boldsymbol{x}}'$ is a well-defined element of $\mathbb{P}^{n-k}(\overline{\mathbb{K}(\mathfrak{Q}')})$, that is, it is not identically zero, since otherwise $\tilde{\boldsymbol{x}}$ would vanish as well.

For $\boldsymbol{i} = (i_1, \ldots, i_k)$ with $k \leq n-1$, applying the above substitution in the submatrix of $\mathfrak{L}^H_{\boldsymbol{i},(p+1,\ldots,q)}(\boldsymbol{\alpha}, q)$ associated to $\boldsymbol{i}$ which has size $k \times (n-1)$, the rank condition above becomes that $\mathfrak{P}^H(\boldsymbol{\alpha}_{\boldsymbol{i}}, n-1) \in \mathbb{K}[\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}][\tilde{\boldsymbol{X}}']^{(k-(p-t))\times(n-1)}$ has rank less than $k-(p-t)$ at $\tilde{\boldsymbol{x}}'$, that is, $\tilde{\boldsymbol{x}}'$ is in $V_{k-(p-t)}(\mathfrak{P}^H(\boldsymbol{\alpha}_{\boldsymbol{i}}, n-1))$. In this case, we are done.

When k equals n, that is, $\boldsymbol{i} = (i_1, \ldots, i_n)$ (this can happen only if $n \leq p$), the linear equations above determine $\tilde{\boldsymbol{x}}$ entirely; setting $\tilde{x}_0 = 1$, we obtain

$$\tilde{x}_1 = \mathfrak{f}_{1,\boldsymbol{i},\boldsymbol{r}}(1), \ldots, \tilde{x}_n = \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(1).$$

In this case, the submatrix of $\mathfrak{L}^H_{\boldsymbol{i},(p+1,\ldots,q)}(\boldsymbol{\alpha}, q)$ associated to $\boldsymbol{i}$ has size $n \times (n-1)$. Using the specialization of the coefficients that sets the off-diagonal entry to 0 and the i-th diagonal entries to $x_0^{\alpha_i}$, $i = 1, \ldots, n-1$, we see that its evaluation at $\tilde{\boldsymbol{x}}$ has rank $n-1$; as a result $\mathfrak{L}^H_{\boldsymbol{\alpha},q}$ has rank $p-1$ at $\tilde{\boldsymbol{x}}$. Thus, we need to take $k = n$ into account only if $t = p$, that is, if we are interested in the maximal minors; in this case, we have to take into account the point $\{(1, \mathfrak{f}_{1,\boldsymbol{i},\boldsymbol{r}}(1), \ldots, \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(1))\}$. □

Solutions with higher rank defect.

We discuss here the case $t = p-1$. We take parameters $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q, with $2 \leq p \leq q$, and we write $\mathcal{A} = \mathcal{A}(\boldsymbol{\alpha}, q)$ and $\mathcal{A}' = \mathcal{A}'(\boldsymbol{\alpha}, q)$.

Lemma 6.3.5. *The following holds:*

$\mathsf{J}_1(\boldsymbol{\alpha}, q)$. *The projective algebraic set* $V_{p-1}(\mathfrak{P}^H(\boldsymbol{\alpha}, q)) \subset \mathbb{P}^n(\overline{\mathbb{K}(\mathfrak{Q}')})$ *is empty.*

$\mathsf{K}_1(\boldsymbol{\alpha}, q)$. *The projective algebraic set* $V_{p-1}(\mathfrak{L}^H(\boldsymbol{\alpha}, q)) \subset \mathbb{P}^n(\overline{\mathbb{K}(\mathfrak{Q}')})$ *is empty.*

Proof. The proof consists two step. The first step is to establish that for $\boldsymbol{\alpha}$ and q as above, $\mathsf{K}_1(\boldsymbol{\alpha}, q)$ implies $\mathsf{J}_1(\boldsymbol{\alpha}, q)$ and the second one is using an inductive argument to conclude our claim.

Let us consider the ideal generated by the $(p-1)$-minors of $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$ in the polynomial ring $\mathbb{K}[\mathfrak{Q}, \boldsymbol{X}']$ in $\mathcal{A} + n + 1$ variables, with $\boldsymbol{X}' = (x_0, x_1, \ldots, x_n)$. This ideal defines an algebraic set $Z_{\boldsymbol{\alpha},q}$ in $\overline{\mathbb{K}}^{\mathcal{A}} \times \mathbb{P}^n(\overline{\mathbb{K}})$. Let $\Delta_{\boldsymbol{\alpha},q} \subset \overline{\mathbb{K}}^{\mathcal{A}}$ be its projection on the first factor; this is the set of all Λ such that $V_{p-1}(\mathfrak{P}^H(\boldsymbol{\alpha}, q))$ is not empty. In particular, $\Delta_{\boldsymbol{\alpha},q}$ is closed $\overline{\mathbb{K}}^{\mathcal{A}}$, and it is sufficient to verify that it is not equal to the whole space $\overline{\mathbb{K}}^{\mathcal{A}}$. This follows readily from property $\mathsf{K}_1(\boldsymbol{\alpha}, q)$, which proves that generic matrices of the form $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ in $\mathbb{K}[\Lambda', \boldsymbol{X}']$ do not belong to $\Delta_{\boldsymbol{\alpha},q}$. Therefore, if $\mathsf{K}_1(\boldsymbol{\alpha}, q)$ holds, $\mathsf{J}_1(\boldsymbol{\alpha}, q)$ holds as well.

We finish the proof by induction. We first take $p = q$ and consider $\mathsf{K}_1(\boldsymbol{\alpha}, q)$. In this case, $n = 1$ and $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ is a diagonal matrix, whose diagonal entries are products of linear forms in (x_0, x_1) with indeterminate coefficients. Hence, no pair of entries $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ have any common solution in $\mathbb{P}^1(\overline{\mathbb{K}(\mathfrak{Q}')})$, so the rank of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ is at least $p-1$ at any $\tilde{\boldsymbol{x}} \in \mathbb{P}^1(\overline{\mathbb{K}(\mathfrak{Q}')})$. As a result, $\mathsf{K}_1(\boldsymbol{\alpha}, p)$ holds, and so does $\mathsf{J}_1(\boldsymbol{\alpha}, p)$, by the claim in the previous paragraph.

Consider next a pair $(\boldsymbol{\alpha}, q)$, with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and $2 \leq p < q$, and suppose that $\mathsf{J}_1(\boldsymbol{\alpha}', q')$ holds for all $(\boldsymbol{\alpha}', q')$ with $\boldsymbol{\alpha}' = (\alpha'_1, \ldots, \alpha'_{p'})$, $2 \leq p' \leq q'$, $p' \leq p$ and $q' < q$; we prove that $\mathsf{K}_1(\boldsymbol{\alpha}, q)$ holds. As above, this will also imply $\mathsf{J}_1(\boldsymbol{\alpha}, q)$.

Take $t = p - 1$ in Lemma 6.3.4. Then, the parameters $(k - (p-t), \boldsymbol{\alpha_i}, n-1)$ used in each expression (6.9) are of the form $(k-1, \boldsymbol{\alpha_i}, n-1)$, with $2 \leq k \leq \min(p, n-1)$. Since the $\mathcal{A}(\boldsymbol{\alpha_i}, n-1)$ entries of $\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}$ are algebraically independent over $\mathbb{K}$, $\mathbb{K}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}})$ is isomorphic to $\mathbb{K}(\lambda_{s,j,u,r})$, for $s = 1, \ldots, k$, $j = 1, \ldots, n-1$, $u = 1, \ldots, \alpha_{i_s}$ and $r = 0, \ldots, n-k$, so that $V_{k-1}(\mathfrak{P}^H(\boldsymbol{\alpha_i}, n-1)$ has the same cardinality as $V_{k-1}(\mathfrak{P}^H(\boldsymbol{\alpha_i}, n-1))$. As a result, since $\boldsymbol{\alpha_i}$ has length $k \geq 2$, and since we also have $k \leq n-1$, $k \leq p$ and $n - 1 < q$, we can apply the induction hypothesis and deduce that all $V_{k-1}(\mathfrak{P}^H_{\boldsymbol{\alpha_i}, n-1})$ appearing in Lemma 6.3.4 are empty. This implies that $V_{p-1}(\mathfrak{L}^H(\boldsymbol{\alpha}, q))$ is empty, as claimed. □

Solutions at infinity.

Now, we consider $t = p$. We take parameters $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q, with $1 \leq p \leq q$, and we write $\mathcal{A} = \mathcal{A}(\boldsymbol{\alpha}, q)$ and $\mathcal{A}' = \mathcal{A}'(\boldsymbol{\alpha}, q)$. We prove the following properties which imply the first item in Proposition 6.3.3.

Lemma 6.3.6. *The following holds:*

$\mathsf{J}_2(\boldsymbol{\alpha}, q)$. *The projective algebraic set* $V_p(\mathfrak{P}^H(\boldsymbol{\alpha}, q)) \subset \mathbb{P}^n(\overline{\mathbb{K}(\mathfrak{L})})$ *has no solution at infinity, that is, with* $x_0 = 0$.

$\mathsf{K}_2(\boldsymbol{\alpha}, q)$. *The projective algebraic set* $V_p(\mathfrak{L}^H(\boldsymbol{\alpha}, q)) \subset \mathbb{P}^n(\overline{\mathbb{K}(\mathfrak{Q}')})$ *has no solution at infinity, that is, with* $x_0 = 0$.

In particular, this lemma implies that the sets $V_p(\mathfrak{P}^H(\boldsymbol{\alpha}, q))$ and $V_p(\mathfrak{L}^H(\boldsymbol{\alpha}, q))$ are finite.

Proof. We follow the same strategy as what we did in the proof of Lemma 6.3.5: the first step is to establish that for $\boldsymbol{\alpha}$ and q as above, $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ implies $\mathsf{J}_2(\boldsymbol{\alpha}, q)$ and the second one is using an inductive argument to conclude our claim.

Let us fix $\boldsymbol{\alpha}$ and q and assume that $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ holds. We will show that for a generic choice of Λ in $\overline{\mathbb{K}}^{\mathcal{A}}$, $V_p(\Theta_\Lambda(\mathfrak{P}^H(\boldsymbol{\alpha}, q)))$ has no point at infinity, which means $\mathsf{J}_2(\boldsymbol{\alpha}, q)$ holds. Let us consider the ideal generated by the p-minors of $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$ and x_0 in the polynomial ring $\mathbb{K}[\mathfrak{Q}, \boldsymbol{X}']$ in $\mathcal{A} + n + 1$ variables, with $\boldsymbol{X}' = (x_0, x_1, \ldots, x_n)$. This ideal defines an

algebraic set $Z'_{\boldsymbol{\alpha},q}$ in $\overline{\mathbb{K}}^{\mathcal{A}} \times \mathbb{P}^n(\overline{\mathbb{K}})$. Let $\Delta'_{\boldsymbol{\alpha},q} \subset \overline{\mathbb{K}}^{\mathcal{A}}$ be its projection on the first factor. This is the set of all Λ such that $V_p(\mathfrak{P}^H(\boldsymbol{\alpha}, q))$ has a point satisfying $x_0 = 0$. Since the projection of a closed set is closed, it is sufficient to verify that it is not equal to the whole space $\overline{\mathbb{K}}^{\mathcal{A}}$. This follows readily from property $\mathsf{K}_2(\boldsymbol{\alpha}, q)$, which proves that generic matrices of the form $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ in $\mathbb{K}[\Lambda', \boldsymbol{X}']$ do not belong to $\Delta'_{\boldsymbol{\alpha},q}$. Therefore, if $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ holds, $\mathsf{J}_2(\boldsymbol{\alpha}, q)$ holds as well.

We finish the proof by induction. We first take $p = q$ and prove $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ holds. In this case, $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ is a diagonal matrix, whose diagonal entries are products of linear forms in (x_0, x_1) with indeterminate coefficients. Hence, no pair of entries $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ have any common solution in $\mathbb{P}^1(\overline{\mathbb{K}(\mathfrak{Q}')})$, so the rank of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ less than p at any $\tilde{\boldsymbol{x}} \in \mathbb{P}^1(\overline{\mathbb{K}(\mathfrak{Q}')})$ if and only if one of the linear factors of the diagonal terms vanishes at $\tilde{\boldsymbol{x}}$. None of these linear forms has a projective solution satisfying $x_0 = 0$. As a result, $\mathsf{K}_2(\boldsymbol{\alpha}, p)$ holds; and so does $\mathsf{J}_2(\boldsymbol{\alpha}, p)$, by the claim in the previous paragraph.

Consider next a pair $(\boldsymbol{\alpha}, q)$, with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and $2 \leq p < q$, and suppose that $\mathsf{J}_2(\boldsymbol{\alpha}', q')$ holds for all $(\boldsymbol{\alpha}', q')$ with $\boldsymbol{\alpha}' = (\alpha'_1, \ldots, \alpha'_{p'})$, $2 \leq p' \leq q'$, $p' \leq p$ and $q' < q$; we prove that $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ holds. As above, this will also imply $\mathsf{J}_2(\boldsymbol{\alpha}, q)$.

Take $t = p$ in Lemma 6.3.4. If $n \leq p$, the corresponding sequences are $\boldsymbol{i} = (i_1, \ldots, i_n)$ with $k = n$. By design in Lemma 6.3.4, the corresponding projective point does not satisfy $x_0 = 0$. Let us consider now $n > p$. The parameters $(k - (p - t), \boldsymbol{\alpha_i}, n - 1)$ used in (6.9) are now of the form $(k, \boldsymbol{\alpha_i}, n - 1)$, with $\boldsymbol{\alpha_i}$ of length $k \in \{1, \ldots, \min(p, n - 1)\}$. Since all conditions $1 \leq k \leq n - 1$, $k \leq p$ and $n - 1 < q$ are satisfied, we can invoke the induction assumption. The projective sets $V_k(\mathfrak{P}^H_{\boldsymbol{\alpha_i},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}'))$ appearing in Lemma 6.3.4 has any point with $x_0 = 0$ because the coefficients $\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}$ are algebraically independent. As a consequence, $V_p(\mathfrak{L}^H(\boldsymbol{\alpha}, q))$ has no projective point satisfying $x_0 = 0$, as claimed. □

At this stage, we complete our proof for the first property of Proposition 6.3.3. We are going to finish the proof for second one by refining first the property $\mathsf{J}_1(\boldsymbol{\alpha}, q)$. The property $\mathsf{J}_1(\boldsymbol{\alpha}, q)$ property asserts that for any $\tilde{\boldsymbol{x}}$ in $\mathbb{P}^n(\overline{\mathbb{K}(\mathfrak{Q}')})$, the $p \times q$ matrix $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$ evaluating at $\tilde{\boldsymbol{x}}$ has rank at least $p - 1$. In other words, there exists a $(p - 1)$-minor in $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$ that does not vanish at $\tilde{\boldsymbol{x}}$. In the next property, we claim that each $(p - 1) \times q$ submatrix of $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$ has rank $p - 1$ at $\tilde{\boldsymbol{x}}$.

Refining $\mathsf{J}_1(\boldsymbol{\alpha}, q)$.

Consider $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q, with $1 \leq p \leq q$, together with a matrix $\mathfrak{p}^H(\boldsymbol{\alpha}, q)$, built as $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$ before, but using products of homogeneous linear forms in $(n-1)+1 = q-p+1$ variables $x_0, \ldots, x_{n-1}$, instead of $n+1$ variables $x_0, \ldots, x_n$. Such a matrix takes the form

$$\mathfrak{p}^H(\boldsymbol{\alpha}, q) = \begin{bmatrix} \mathfrak{g}^H_{1,1} & \cdots & \mathfrak{g}^H_{1,q} \\ \vdots & & \vdots \\ \mathfrak{g}^H_{p,1} & \cdots & \mathfrak{g}^H_{p,q} \end{bmatrix} \in \mathbb{K}[\mathfrak{G}][x_0, \ldots, x_{n-1}]^{p \times q}, \tag{6.10}$$

with

$$\mathfrak{g}^H_{i,j,k} = \mathfrak{g}_{i,j,k,0}x_0 + \mathfrak{g}_{i,j,k,1}x_1 + \cdots + \mathfrak{g}_{i,j,k,n-1}x_{n-1},$$

and

$$\mathfrak{g}^H_{i,j} = \mathfrak{g}^H_{i,j,1} \cdots \mathfrak{g}^H_{i,j,\alpha_i} \in \mathbb{K}[\mathfrak{G}][x_0, \ldots, x_{n-1}],$$

where $\mathfrak{G} = (\mathfrak{g}_{i,j,k,\ell})$ are indeterminates, for $i = 1, \ldots, p$, $j = 1, \ldots, q$, $k = 1, \ldots, \alpha_i$ and $\ell = 0, \ldots, n-1$. We let $\mathcal{B} = qn(\alpha_1 + \cdots + \alpha_p)$ be the total number of coefficients $\mathfrak{g}_{i,j,k,\ell}$ involved.

Lemma 6.3.7. *The following holds:*

$\mathsf{J}_3(\boldsymbol{\alpha}, q)$. *The projective algebraic set* $V_p(\mathfrak{p}^H_{\boldsymbol{\alpha},q}) \subset \mathbb{P}^{n-1}(\overline{\mathbb{K}(\mathfrak{G})})$ *is empty.*

Proof. If $p = q$, then $n = 1$, so the (i,j)-entry of $\mathfrak{p}^H(\boldsymbol{\alpha}, q)$ has the form $\mathfrak{g}_{i,j,1,0} \cdots \mathfrak{g}_{i,j,\alpha_i,0}x_0^{\alpha_i}$. Then, the determinant of this matrix is non-zero, and the claim follows.

Suppose now that $q > p$, so that $q - 1 \geq p$. Then, the $((1, \ldots, p), (1, \ldots, q-1))$-submatrix of $\mathfrak{p}^H(\boldsymbol{\alpha}, q)$ is of the form $\mathfrak{P}^H(\boldsymbol{\alpha}, q-1)$, with entries depending on $\mathcal{A}(\boldsymbol{\alpha}, q-1)$ parameters. Let $(c_i)_{i \in I}$ be the p-minors of $\mathfrak{p}^H(\boldsymbol{\alpha}, q)$ built by taking $p-1$ of the first $q-1$ columns of $\mathfrak{p}^H(\boldsymbol{\alpha}, q)$, together with its last column. Any such minor can be expanded along the last column as

$$c_i = \mathfrak{g}^H_{1,q}c_{i,1} + \cdots + \mathfrak{g}^H_{p,q}c_{i,p}, \tag{6.11}$$

where $\mathfrak{g}^H_{1,q}, \ldots, \mathfrak{g}^H_{p,q}$ are the entries of the last column of $\mathfrak{p}^H(\boldsymbol{\alpha}, q)$, and $c_{i,1}, \ldots, c_{i,p}$ are some $(p-1)$-minors of $\mathfrak{P}^H(\boldsymbol{\alpha}, q-1)$. We remark that $(c_{i,j})_{i \in I, 1 \leq j \leq p}$ are *all* $(p-1)$-minors of $\mathfrak{P}^H(\boldsymbol{\alpha}, q-1)$. If $p = 1$, we have $I = \{1\}$ and $c_1 = \mathfrak{g}^H_{1,q}$, with $c_{1,1} = 1$.

For any point $\tilde{\boldsymbol{x}}$ in $\mathbb{P}^{n-1}(\overline{\mathbb{K}(\mathfrak{G})}) - V_p(\mathfrak{P}^H(\boldsymbol{\alpha}, q-1))$, the matrix $\mathfrak{P}^H(\boldsymbol{\alpha}, q-1)$ has full rank p at $\tilde{\boldsymbol{x}}$, and thus so does $\mathfrak{p}^H(\boldsymbol{\alpha}, q)$. Therefore, we can focus on the points in $V_p(\mathfrak{P}^H(\boldsymbol{\alpha}, q-1))$. Note that, by $\mathsf{J}_2(\boldsymbol{\alpha}, q-1)$, the set $V_p(\mathfrak{P}^H(\boldsymbol{\alpha}, q-1))$ is finite in $\mathbb{P}^{n-1}(\overline{\mathbb{K}(\mathfrak{G})})$, and for any point $\tilde{\boldsymbol{x}} = (\tilde{x}_0, \ldots, \tilde{x}_{n-1})$, we can take the first coordinate $\tilde{x}_0$ equal to 1. Using $\mathsf{J}_1(\boldsymbol{\alpha}, q-1)$ and the fact that $(c_{i,j})_{i \in I, 1 \leq j \leq p}$ are all the $(p-1)$-minors of $\mathfrak{P}^H(\boldsymbol{\alpha}, q-1)$, we can deduce that not all minors $(c_{i,j})_{i \in I, 1 \leq j \leq p}$ vanish at $\tilde{\boldsymbol{x}}$. Suppose that $c_{i_0,j_0}(\tilde{\boldsymbol{x}}) \neq 0$, we prove that $c_{i_0}(\tilde{\boldsymbol{x}}) \neq 0$, which is enough to conclude our claim.

From (6.11) and the fact that $c_{i_0,j_0}(\tilde{\boldsymbol{x}}) \neq 0$, in order to obtain $c_{i_0}(\tilde{\boldsymbol{x}}) \neq 0$, it is sufficient to show that $g_{j_0,q}(\tilde{\boldsymbol{x}}) \neq 0$. Let us split the $\mathcal{B}$ indeterminates $\mathfrak{G}$ into $\mathfrak{G}_1$ and $\mathfrak{G}_2$, where $\mathfrak{G}_1$ has cardinality $\mathcal{B}_1 = \mathcal{A}(\boldsymbol{\alpha}, q-1)$ and corresponds to the coefficients used in the entries $\mathfrak{g}^H_{1,1}, \ldots, \mathfrak{g}^H_{p,q-1}$ in $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$, and $\mathfrak{G}_2$ of cardinality $\mathcal{B}_2 = \mathcal{B} - \mathcal{B}_1$ stands for the coefficients of the entries $\mathfrak{g}^H_{1,q}, \ldots, \mathfrak{g}^H_{p,q}$ in the last column of $\mathfrak{p}^H(\boldsymbol{\alpha}, q)$. Since $V_p(\mathfrak{P}^H(\boldsymbol{\alpha}, q-1))$ is finite, the coordinates of $\tilde{\boldsymbol{x}}$ are algebraic over $\mathbb{K}(\mathfrak{G}_1)$.

Thus, since $\tilde{x}_0 = 1$, the polynomial $\mathfrak{g}^H_{j_0,q}(\tilde{\boldsymbol{x}}) \in \overline{\mathbb{K}(\mathfrak{G}_1)}[\mathfrak{G}_2]$ admits $\mathfrak{g}_{j_0,q,1,0} \cdots \mathfrak{g}_{j_0,q,\alpha_{j_0},0}$ as a specialization, by setting to zero all coefficients $\mathfrak{g}_{j_0,q,k,\ell}$, for $k = 1, \ldots, \alpha_{j_0}$ and $\ell = 1, \ldots, n-1$. Note that the coefficients $\mathfrak{g}_{j_0,q,k,\ell}$ are in $\mathfrak{G}_2$. For $j \neq j_0$, $\mathfrak{g}^H_{j,q}(\tilde{\boldsymbol{x}}) \in \overline{\mathbb{K}(\mathfrak{G}_1)}[\mathfrak{G}_2]$ admits 0 as a specialization, by setting to zero all coefficients $\mathfrak{g}_{j,q,k,\ell}$, for $k = 1, \ldots, \alpha_j$ and

$\ell = 0, \ldots, n-1$. We remark that $\mathfrak{g}_{j,q,k,\ell}$ also belong to $\mathfrak{G}_2$. The coefficients $c_{i_0,j}(\tilde{\boldsymbol{x}})$ are algebraic over $\mathbb{K}(\mathfrak{G}_1)$, so that $c_{i_0}(\tilde{\boldsymbol{x}})$ is in $\overline{\mathbb{K}(\mathfrak{G}_1)}[\mathfrak{G}_2]$. Therefore, it admits

$$\mathfrak{g}_{j_0,q,1,0} \cdots \mathfrak{g}_{j_0,q,\alpha_{j_0},0} c_{i_0,j_0}(\tilde{\boldsymbol{x}})$$

as a specialization, which is non-zero. Thus, $c_{i_0}(\tilde{\boldsymbol{x}})$ is non-zero, as claimed. □

Multiplicity of the solutions.

We now can finish our proof for the second property of Proposition 6.3.3. This is a directly consequence of the following lemma.

Lemma 6.3.8. *The following holds:*

$\mathsf{J}_4(\boldsymbol{\alpha}, q)$. *The Jacobian matrix of the p-minors of $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$ with respect to $\boldsymbol{X}' = (x_0, \ldots, x_n)$ has rank n at all points in $V_p(\mathfrak{P}^H(\boldsymbol{\alpha}, q))$.*

$\mathsf{K}_4(\boldsymbol{\alpha}, q)$. *The Jacobian matrix of the p-minors of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ with respect to $\boldsymbol{X}' = (x_0, \ldots, x_n)$ has rank n at all points in $V_p(\mathfrak{L}^H(\boldsymbol{\alpha}, q))$.*

The rest of this subsection is devoted for a proof of this lemma. We follow the same strategy which consists of 2 steps as what we did above. The first step is to establish that for $\boldsymbol{\alpha}$ and q as above, $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ implies $\mathsf{J}_4(\boldsymbol{\alpha}, q)$ and the second one is using an inductive argument to conclude our claim.

Let us fix $\boldsymbol{\alpha}$ and q and assume that $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ holds. We will show that for a generic choice of Λ in $\overline{\mathbb{K}}^{\mathcal{A}}$, the Jacobian matrix of the p-minors of $\Theta_\Lambda(\mathfrak{P}^H(\boldsymbol{\alpha}, q))$ with respect to $\boldsymbol{X}'$ has full rank at all points in $V_p(\Theta_\Lambda(\mathfrak{P}^H(\boldsymbol{\alpha}, q))$, which means $\mathsf{J}_4(\boldsymbol{\alpha}, q)$ holds. Let us consider the ideal in the polynomial ring $\mathbb{K}[\mathfrak{Q}, \boldsymbol{X}']$ in $\mathcal{A} + n + 1$ variables generated by the p-minors of $\mathfrak{P}^H(\boldsymbol{\alpha}, q)$ together with the n-minors of the Jacobian of these equations with respect to $\boldsymbol{X}'$. This ideal defines an algebraic set $Z''_{\boldsymbol{\alpha},q}$ in $\overline{\mathbb{K}}^{\mathcal{A}} \times \mathbb{P}^n(\overline{\mathbb{K}})$. Let $\Delta''_{\boldsymbol{\alpha},q} \subset \overline{\mathbb{K}}^{\mathcal{A}}$ be its projection on the first factor. This is the set of all Λ such that the Jacobian matrix of the p-minors of $\Theta_\Lambda(\mathfrak{P}^H(\boldsymbol{\alpha}, q))$ has not full-rank n at all points in $V_p(\Theta_\Lambda(\mathfrak{P}^H(\boldsymbol{\alpha}, q)))$. Therefore, for $\Lambda \in \overline{\mathbb{K}}^{\mathcal{A}} - \Delta''_{\boldsymbol{\alpha},q}$, the Jacobian matrix of the p-minors of $\Theta_\Lambda(\mathfrak{P}^H(\boldsymbol{\alpha}, q))$ has full-rank n at all points in $V_p(\Theta_\Lambda(\mathfrak{P}^H(\boldsymbol{\alpha}, q)))$. Since the projection of a closed set is closed, so it is sufficient to verify that $\Delta''_{\boldsymbol{\alpha},q}$ is not equal to the whole space $\overline{\mathbb{K}}^{\mathcal{A}}$. This follows readily from property $\mathsf{K}_4(\boldsymbol{\alpha}, q)$, which proves that generic matrices of the form $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ in $\mathbb{K}[\Lambda', \boldsymbol{X}']$ do not belong to $\Delta''_{\boldsymbol{\alpha},q}$. Therefore, if $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ holds, $\mathsf{J}_4(\boldsymbol{\alpha}, q)$ holds as well.

We finish the proof by induction. We first take $p = q$ and prove $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ holds. In this case, $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ is a diagonal matrix, whose diagonal entries are products of linear forms in (x_0, x_1) with indeterminate coefficients. The ideal of p-minors of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ is generated by the product of the terms $\mathfrak{l}^H_{i,i}$, which admits no repeated factors; the conclusion follows.

Consider next a pair $(\boldsymbol{\alpha}, q)$, with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and $2 \leq p < q$, and suppose that $\mathsf{J}_4(\boldsymbol{\alpha}', q')$ holds for all $(\boldsymbol{\alpha}', q')$ with $\boldsymbol{\alpha}' = (\alpha'_1, \ldots, \alpha'_{p'})$, $2 \leq p' \leq q'$, $p' \leq p$ and $q' < q$; we prove that $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ holds. As above, this will also imply $\mathsf{J}_4(\boldsymbol{\alpha}, q)$.

We take $t = p$ in the formula of Lemma 6.3.4, and we first deal with the terms in (6.9). Thus, we choose a subsequence $\boldsymbol{i} = (i_1, \ldots, i_k)$ of $(1, \ldots, p)$, with $1 \leq k \leq \min(p, n-1)$, and indices $\boldsymbol{r} = (r_1, \ldots, r_k)$, with $1 \leq r_s \leq \alpha_{i_s}$ for all $s = 1, \ldots, k$. We prove that the Jacobian matrix of the p-minors of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ with respect to $\boldsymbol{X}'$ has rank n at all points $\tilde{\boldsymbol{x}} = (\tilde{x}_0, \ldots, \tilde{x}_n)$ of $V_p(\mathfrak{L}^H(\boldsymbol{\alpha}, q))$ such that $\tilde{\boldsymbol{x}}' = (\tilde{x}_0, \ldots, \tilde{x}_{n-k})$ is in $V_k(\mathfrak{P}^H_{\boldsymbol{\alpha_i}, n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \boldsymbol{X}')) \subset \mathbb{P}^{n-\kappa}(\overline{\mathbb{K}(\mathfrak{Q}')})$, and such that

$$\tilde{x}_{n-k+1} = \mathfrak{f}_{n-k+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'), \ldots, \tilde{x}_n = \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'). \tag{6.12}$$

By Lemma 6.3.4, taking all such $\tilde{\boldsymbol{x}}$ into account, for all $\boldsymbol{i}$ and $\boldsymbol{r}$, will cover all points in $V_p(\mathfrak{L}^H(\boldsymbol{\alpha}, q))$, up to the exception of those points obtained from $k = n$, which will admit a simpler treatment. For simplicity, we continue the proof with $\boldsymbol{i} = (1, \ldots, k)$, so that we have $\boldsymbol{\alpha_i} = (\alpha_1, \ldots, \alpha_k)$. We are going to exhibit some polynomials from the maximal minors of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$, for which the Jacobian matrix of these polynomials has rank n at $\tilde{\boldsymbol{x}}$. First, we establish the following property.

Lemma 6.3.9. *For $i \in \{1, \ldots, k\}$ and $r \in \{1, \ldots, \alpha_i\} - \{r_i\}$, as well as $i \in \{k+1, \ldots, p\}$ and $r \in \{1, \ldots, \alpha_i\}$, the value $\mathfrak{l}_{i,i,r}(\tilde{\boldsymbol{x}})$ is non-zero.*

Proof. Recall that $\mathfrak{Q}'_{\boldsymbol{i},\boldsymbol{r}}$ is the subset of $\mathfrak{Q}'$ which contains indeterminates corresponding to the coefficients of $\mathfrak{l}^H_{i_1,i_1,r_1}, \ldots, \mathfrak{l}^H_{i_k,i_k,r_k}$, and of all entries $\mathfrak{l}^H_{i_1,p+1}, \ldots, \mathfrak{l}^H_{i_k,q}$ of the submatrix associated to $\boldsymbol{i}$ in $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$. We subdivide $\mathfrak{Q}' = \mathfrak{Q}'_{\boldsymbol{i},\boldsymbol{r}} \cup \mathfrak{Q}''_{\boldsymbol{i},\boldsymbol{r}}$.

By $\mathsf{J}_2(\boldsymbol{\alpha_i}, n-1)$, the set $V_k(\mathfrak{P}^H(\boldsymbol{\alpha_i}, n-1)$ is finite, with $\boldsymbol{\alpha_i} = (\alpha_1, \ldots, \alpha_k)$ and the matrix $\mathfrak{P}^H(\boldsymbol{\alpha_i}, n-1)$ is in $\mathbb{K}[\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}][\tilde{\boldsymbol{X}}']^{k \times (n-1)}$. As a result, since all entries of $\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}$ are in $\mathbb{K}(\mathfrak{Q}'_{\boldsymbol{i},\boldsymbol{r}})$, all coordinates of $\tilde{\boldsymbol{x}}$ are algebraic over $\mathbb{K}(\mathfrak{Q}'_{\boldsymbol{i},\boldsymbol{r}})$. For i, r as above, the coefficients of the equation

$$\mathfrak{l}^H_{i,i,r} = \mathfrak{l}_{i,i,r,0} x_0 + \mathfrak{l}_{i,i,r,1} x_1 + \cdots + \mathfrak{l}_{i,i,r,n} x_n$$

are in $\mathbb{K}(\mathfrak{Q}''_{\boldsymbol{i},\boldsymbol{r}})$, thus algebraically independent over the field of definition of $\tilde{\boldsymbol{x}}$, so that $\mathfrak{l}^H_{i,i,r}(\tilde{\boldsymbol{x}})$ is non-zero. □

Let us assume now $k \geq 2$ and take $i \in \{1, \ldots, k\}$. If $k = 1$, we let the polynomial c_1 in Lemma 6.3.10 below as $c_1 = 1$. We define the sequences $\boldsymbol{i}^* = (1, \ldots, i-1, i+1, \ldots, k)$ and $\boldsymbol{\alpha}^* = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_k)$. Then, we denote by $\mathfrak{L}^H_{\boldsymbol{i}^*,(p+1,\ldots,q)} \in \mathbb{K}[\mathfrak{Q}', \boldsymbol{X}']^{(k-1)\times(n-1)}$ the submatrix of $\mathfrak{L}^H(\boldsymbol{\alpha}, q)$ obtained by keeping rows indexed $\boldsymbol{i}^*$ and columns indexed by $(p+1, \ldots, q)$

Lemma 6.3.10. *There exists a $(k-1)$-minor c_i of $\mathfrak{L}^H_{\boldsymbol{i}^*,(p+1,\ldots,q)}$ such that $c_i(\tilde{\boldsymbol{x}})$ is non-zero.*

Proof. Let $\mathfrak{p}^H_{\boldsymbol{i}^*}$ be the matrix obtained by applying the substitution (6.12) in $\mathfrak{L}^H_{\boldsymbol{i}^*,(p+1,\dots,q)}$. This matrix has size $(k-1)\times(n-1)$ with all entries are products of linear forms in $n-k+1$ variables $(x_0,\dots,x_{n-k})$, with coefficients are algebraically independent over $\mathbb{K}$. We can thus apply $\mathsf{J}_3(\boldsymbol{\alpha}^*, n-1)$ in Lemma 6.3.7 to $\mathfrak{p}^H_i$, and deduce that this matrix has full rank $k-1$ at $\tilde{\boldsymbol{x}}'$. Thus, $\mathfrak{L}^H_{\boldsymbol{i}^*,(p+1,\dots,q)}$ has rank $k-1$ at $\tilde{\boldsymbol{x}}$, from which the existence of the minor c_i follows. □

Lemma 6.3.11. *For any $i\in\{1,\dots,k\}$, there exists a polynomial of the form $b_i\mathfrak{l}^H_{i,i,r_i}$ in the p-minors of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$ such that $b_i(\tilde{\boldsymbol{x}})$ is non-zero.*

Proof. Let us consider the p-minor of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$ obtained by taking the columns $(i,k+1,\dots,p)$ and all $k-1$ columns in the $(k-1)$-minor c_i, where c_i is defined in Lemma 6.3.10 if $k\geq 2$ and c_1 if $k=1$. Using the factorization

$$\mathfrak{l}^H_{i,i}=\beta_i\mathfrak{l}^H_{i,i,r_i},\ \text{with}\ \beta_i=\mathfrak{l}^H_{i,i,1}\cdots\mathfrak{l}^H_{i,i,r_i-1}\mathfrak{l}^H_{i,i,r_i+1}\cdots\mathfrak{l}^H_{i,i,\alpha_i},$$

that minor equals to

$$b_i\mathfrak{l}^H_{i,i,r_i}\ \text{with}\ b_i=\beta_i\mathfrak{l}^H_{k+1,k+1}\cdots\mathfrak{l}^H_{p,p}c_i.$$

By Lemma 6.3.10, $c_i(\tilde{\boldsymbol{x}})$ is non-zero and by Lemma 6.3.9, $\mathfrak{l}^H_{s,s}(\tilde{\boldsymbol{x}})$ is non-zero, for $s=k+1,\dots,p$. This implies that $b_i(\tilde{\boldsymbol{x}})\neq 0$, as desired. □

In what follows, we write $b=b_1\cdots b_k$, so that $b(\tilde{\boldsymbol{x}})\neq 0$ and $b\,\mathfrak{l}^H_{i,i,r_i}$ is in the ideal of p-minors of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$. This implies that all polynomials

$$b(x_{n-k+1}-\mathfrak{f}_{n-k+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}')),\dots,b(x_n-\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'))$$

are in this ideal as well. Similarly, for every k-minor η of the submatrix of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$ associated to $\boldsymbol{i}$, the polynomial $\mathfrak{l}^H_{k+1,k+1}\cdots\mathfrak{l}^H_{p,p}\,\eta$ belongs to ideal of p-minors of $\mathfrak{L}^H_{k,q}$. Thus, $b\,\eta$ is in this ideal as well. As a result, the polynomial $b\,\eta(\tilde{\boldsymbol{X}}',\mathfrak{f}_{n-k+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'),\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'))$ belongs to that same ideal. Now, $\gamma=\eta(\tilde{\boldsymbol{X}}',\mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'),\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'))$ is one of the k-minors of $\mathfrak{P}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}$, and all k-minors of this matrix are obtained this way.

In summary, we have proved that

$$b\,\mathfrak{l}^H_{1,1,r_1},\dots,b\,\mathfrak{l}^H_{k,k,r_k}\quad\text{and}\quad b\,\gamma,\ \text{for all } k\text{-minors } \gamma \text{ of } \mathfrak{P}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}$$

are in the p-minor ideal of $\mathfrak{L}^H_{\boldsymbol{\alpha},q}$, with $b(\tilde{\boldsymbol{x}})\neq 0$. The Jacobian matrix of these polynomials at $\tilde{\boldsymbol{x}}$ is, up to the non-zero constant $b(\tilde{\boldsymbol{x}})$, equal to that of $\mathfrak{l}^H_{1,1,r_1},\dots,\mathfrak{l}^H_{k,k,r_k}$ (which is simply a matrix of constants), and of all k-minors γ. Using our induction assumption, we know that the Jacobian matrix of the ideal of k-minors γ with respect to $\tilde{\boldsymbol{X}}'$ has rank $n-k$ at $\tilde{\boldsymbol{x}}'$. As a result, the larger Jacobian matrix of all equations above has rank n at $\tilde{\boldsymbol{x}}$, as claimed.

It remains to deal with the case when $k=n$, for $n\leq p$. As above, we may simplify the discussion by assuming that $\boldsymbol{i}=(1,\dots,n)$. In this case, the discussion is simpler: proceeding as above, but dealing only with the polynomials $\mathfrak{l}^H_{1,1},\dots,\mathfrak{l}^H_{n,n}$, we obtain the fact that equations of the form $b\,\mathfrak{l}^H_{1,1,r_1},\dots,b\,\mathfrak{l}^H_{n,n,r_n}$ belong to the p-minor ideal of $\mathfrak{L}^H(\boldsymbol{\alpha},q)$, with $b(\tilde{\boldsymbol{x}})\neq 0$. The conclusion follows directly.

6.3.2 Setting up the systems

Similar to the process we did in the column-degree homotopy algorithms, we first show how to construct a polynomial matrix $\boldsymbol{L}$ in $\mathbb{K}[\boldsymbol{X}]^{p\times q}$ and polynomials $\boldsymbol{M} = (m_1, \ldots, m_s)$ in $\mathbb{K}[\boldsymbol{X}]^s$ used as the starting point for the homotopy deformation.

The polynomials $\boldsymbol{M} = (v_1, \ldots, v_s)$ are defined in the same way as in Subsection 6.2.1. For $i = 1, \ldots, s$, let v_i be

$$m_i = \prod_{k=1}^{\gamma_i} \mu_{i,k} \quad \text{with } \mu_{i,k} = \mu_{i,k,0} + \sum_{\ell=1}^{n} \mu_{i,k,\ell} x_\ell, \tag{6.13}$$

where all $\mu_{i,k,\ell}$ are random elements in $\mathbb{K}$. Then $\boldsymbol{M} = (m_1, \ldots, m_s)$. The difference between the column-degree case and the row-degree case lies in the construction of the start matrix $\boldsymbol{L}$. In the latter case, we use a deformation that cancels out many off-diagonal terms which allows us to take row degrees into account. We define

$$\boldsymbol{L} = \begin{pmatrix} \lambda_{1,1} & 0 & \cdots & 0 & \lambda_{1,p+1} & \cdots & \lambda_{1,q} \\ 0 & \lambda_{2,2} & \cdots & 0 & \lambda_{2,p+1} & \cdots & \lambda_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p} & \lambda_{p,p+1} & \cdots & \lambda_{p,q} \end{pmatrix}, \tag{6.14}$$

where for all i, j, $\lambda_{i,j}$ is a product of α_i linear forms with random coefficients in $\mathbb{K}$, that is,

$$\lambda_{i,j} = \prod_{k=1}^{\alpha_i} \lambda_{i,j,k}, \text{ with } \lambda_{i,j,k} = \lambda_{i,j,k,0} + \sum_{\ell=1}^{n} \lambda_{i,j,k,\ell} x_\ell.$$

Our start system $\boldsymbol{A} = (a_1, \ldots, a_s, \ldots, a_m)$ is then defined by taking $(a_1, \ldots, a_s) = (v_1, \ldots, v_s)$ and $(a_{s+1}, \ldots, a_m)$ are the p-minors of $\boldsymbol{L}$ following the ordering $\succ$. We define

$$\boldsymbol{U} = (1-t) \cdot \boldsymbol{L} + t \cdot \boldsymbol{F} \in \mathbb{K}[t, \boldsymbol{X}]^{p\times q}.$$

Then the deformed system $\boldsymbol{B} = (b_1, \ldots, b_s, \ldots, b_m)$ is given by $b_i = (1-t) \cdot m_i + t \cdot g_i$ for $i = 1, \ldots, s$, and $(b_{s+1}, \ldots, b_m)$ are the p-minors of $\boldsymbol{U}$ following the ordering $\succ$. So, in particular, $\boldsymbol{B}_{t=0} = \boldsymbol{A}$ and $\boldsymbol{B}_{t=1} = \boldsymbol{C}$.

Keeping in mind that we want to apply Propositions 5.2.11 and 5.2.12, we need to verify that all required assumptions are satisfied. From Proposition 5.3.1, the determinantal ideal $J = \langle \boldsymbol{B} \rangle \subset \mathbb{K}[t, \boldsymbol{X}]$ satisfy properties B_1 and B_2. Recall that to have C_1, it suffices to show two properties stated in Lemma 6.1.1. Therefore, it is enough to prove these properties and condition C_2.

Degrees of the start and deformed systems. We need to show that $\deg_{\boldsymbol{X}}(a_k) = \deg_{\boldsymbol{X}}(b_k)$ for all $k = 1, \ldots, m$. For $k = 1, \ldots, s$, we have seen in Subsection 6.2.2 that $\deg_{\boldsymbol{X}}(a_k) = \deg_{\boldsymbol{X}}(b_k)$. Similarly to column-degree case, we can see that, for $k = s+1, \ldots, m$, $b_k(0, \boldsymbol{X}) = a_k$, and

$$\deg_{\boldsymbol{X}}(b_k) \leq \delta_1 + \cdots + \delta_p.$$

Then, it is enough to prove that $\deg(a_k) = \delta_1 + \cdots + \delta_p$, for $k = s+1, \ldots, m$.

Indeed, any p-minor of $\boldsymbol{L}$ is of the form $\lambda_{i_1,i_1} \cdots \lambda_{i_\ell,i_\ell}\zeta$, for some sequence $\boldsymbol{i} = (i_1, \ldots, i_\ell) \subset (1, \ldots, p)$ of length $\ell \in \{0, \ldots, p\}$ and some $(p-\ell)$-minor ζ of $\boldsymbol{L}_{\boldsymbol{i},(p+1,\ldots,q)}$. Since the entries of $\boldsymbol{L}_{\boldsymbol{i},(p+1,\ldots,q)}$ are products of linear form with generic choice of the coefficients $(\lambda_{i,j,k,\ell})$, the determinant ζ has degree $\sum_{i' \notin \boldsymbol{i}} \alpha_{i'}$. Hence, the corresponding p-minor of $\boldsymbol{L}$ has degree $\alpha_1 + \cdots + \alpha_p$, as claimed.

Solutions of the homogenization of the start system. We need to prove that the start system $\boldsymbol{A} = \boldsymbol{B}_{t=0}$ has no solution at infinity. Let x_0 be a new variable and we consider the system $\boldsymbol{A}^H = (a_1^H, \ldots, a_s^H, \ldots, a_m^H)$ obtained by homogenizing all equations in $\boldsymbol{A}$. Thus we have

$$a_i^H = \prod_{k=1}^{\gamma_i} \mu_{i,k}^H \quad \text{with} \quad \mu_{i,k}^H = \mu_{i,k,0}x_0 + \sum_{\ell=1}^{n} \mu_{i,k,\ell}x_\ell$$

for $i = 1, \ldots, s$. Since the coefficients of $\lambda_{i,j}$ are generic for all i, j, the polynomials $(a_{s+1}^H, \ldots, a_m^H)$ are the p-minors, following the ordering $\succ$, of the matrix

$$\boldsymbol{L}^H = \begin{pmatrix} \lambda_{1,1}^H & 0 & \cdots & 0 & \lambda_{1,p+1}^H & \cdots & \lambda_{1,q}^H \\ 0 & \lambda_{2,2}^H & \cdots & 0 & \lambda_{2,p+1}^H & \cdots & \lambda_{2,q}^H \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p}^H & \lambda_{p,p+1}^H & \cdots & \lambda_{p,q}^H \end{pmatrix},$$

where $\lambda_{i,j}^H$ is the homogenization of $\lambda_{i,j}$.

As in Subsection 6.2.3, in order to cancel $a_1^H, \ldots, a_s^H$, we choose indices $\boldsymbol{u} = (u_1, \ldots, u_s)$, with $u_1 \in \{1, \ldots, \gamma_1\}$, $\ldots$, $u_s \in \{1, \ldots, \gamma_s\}$, and we consider the equations

$$\mu_{i,u_i}^H = 0, \quad \text{that is,} \quad \mu_{i,u_i,0}x_0 + \sum_{\ell=1}^{n} \mu_{i,u_i,\ell}x_\ell = 0,$$

for $i = 1, \ldots, s$. Then for a generic choice of coefficients of $\mu_{i,k,\ell}$, these equations are equivalent to

$$x_{n-s+1} = \Phi_{n-s+1,\boldsymbol{u}}(x_0, \ldots, x_{n-s}), \ldots, x_n = \Phi_{n,\boldsymbol{u}}(x_0, \ldots, x_{n-s}),$$

for some homogeneous linear forms $\Phi_{n-s+1,\boldsymbol{u}}, \ldots, \Phi_{n,\boldsymbol{u}}$. After applying this substitution, for all i, j, $\boldsymbol{L}^H$ can be rewritten as

$$\boldsymbol{L}_{\boldsymbol{u}}^H = \begin{pmatrix} \lambda_{1,1,\boldsymbol{u}}^H & 0 & \cdots & 0 & \lambda_{1,p+1,\boldsymbol{u}}^H & \cdots & \lambda_{1,q,\boldsymbol{u}}^H \\ 0 & \lambda_{2,2,\boldsymbol{u}}^H & \cdots & 0 & \lambda_{2,p+1,\boldsymbol{u}}^H & \cdots & \lambda_{2,q,\boldsymbol{u}}^H \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p,\boldsymbol{u}}^H & \lambda_{p,p+1,\boldsymbol{u}}^H & \cdots & \lambda_{p,q,\boldsymbol{u}}^H \end{pmatrix} \in \mathbb{K}[x_0, \ldots, x_{n-s}]^{p \times q}, \qquad (6.15)$$

with

$$\lambda^H_{i,j,\boldsymbol{u}} = \prod_{k=1}^{\alpha_i} \lambda^H_{i,j,k,\boldsymbol{u}}, \quad \text{and} \quad \lambda^H_{i,j,k,\boldsymbol{u}} = \sum_{\ell=0}^{n-s} \lambda_{i,j,k,\ell} x_\ell + \sum_{\ell=n-s+1}^{n} \lambda_{i,j,k,\ell} \Phi_{\ell,\boldsymbol{u}}(x_0, \ldots, x_{n-s}).$$

By Proposition 6.3.3(i), for a generic choice of the coefficients $\mu_{i,k,\ell}$ and $\lambda_{i,j,k,\ell}$, there is no projective solution to the p-minors of $\boldsymbol{L}^H_{\boldsymbol{u}}$ satisfying $x_0 = 0$. Considering all possible choices of $\boldsymbol{u}$, we can deduce that there is no projective solution to the system $\boldsymbol{A}^H$ satisfying $x_0 = 0$.

Radical and zero-dimensional properties of $\langle \boldsymbol{A} \rangle$. From the previous paragraph, we know that there is no projective solution of $\boldsymbol{A}^H$ at infinity, so it is finite. As a result, the affine algebraic set defined by $\boldsymbol{A}$ is finite as well. It remains to show that the ideal $\langle \boldsymbol{A} \rangle$ is radical in $\overline{\mathbb{K}}[\boldsymbol{X}]$; equivalently, we need to prove that the Jacobian matrix of $\boldsymbol{A}$ has full rank at any point in $V(\boldsymbol{A}) \subset \overline{\mathbb{K}}^n$.

Let $\boldsymbol{x} = (\upsilon_1, \ldots, \upsilon_n) \in \overline{\mathbb{K}}^n$ be a point in $V(\boldsymbol{A})$. Then $\tilde{\boldsymbol{x}} = (1, \boldsymbol{x})$ is a projective solution of $\boldsymbol{A}^H$. Following the argument from the previous paragraph, there exist indices $\boldsymbol{u} = (u_1, \ldots, u_s)$, with $u_1 \in \{1, \ldots, \gamma_1\}$, $\ldots$, $u_s \in \{1, \ldots, \gamma_s\}$, such that

$$x_{n-s+1} = \phi_{n-s+1,\boldsymbol{u}}(\upsilon_1 \ldots, \upsilon_{n-s}), \ldots, x_n = \phi_{n,\boldsymbol{u}}(\upsilon_1, \ldots, \upsilon_{n-s}),$$

where $\phi_{k,\boldsymbol{u}}(x_1 \ldots, x_{n-s}) = \Phi_{k,\boldsymbol{u}}(1, x_1 \ldots, x_{n-s})$ for $k = n-s+1, \ldots, n$. Let $\boldsymbol{L}^H_{\boldsymbol{u}}$ be a matrix defined as in (6.15). So, $\boldsymbol{L}^H_{\boldsymbol{u}}$ has rank deficient at any $\tilde{\boldsymbol{x}}' = (1, \upsilon_1, \ldots, \upsilon_{n-s})$. By Proposition 6.3.3(ii), one can deduce that the Jacobian matrix of the p-minors of $\boldsymbol{L}^H_{\boldsymbol{u}}$ with respect to $x_0, \ldots, x_{n-s}$ has full rank at $\tilde{\boldsymbol{x}}'$.

Let $\boldsymbol{L}_u = \boldsymbol{L}^H_u(1, x_1, \ldots, x_{n-s})$ be the dehomogenized matrix of $\boldsymbol{L}^H_u$. That is

$$\boldsymbol{L}_{\boldsymbol{u}} = \begin{pmatrix} \lambda_{1,1,\boldsymbol{u}} & 0 & \cdots & 0 & \lambda_{1,p+1,\boldsymbol{u}} & \cdots & \lambda_{1,q,\boldsymbol{u}} \\ 0 & \lambda_{2,2,\boldsymbol{u}} & \cdots & 0 & \lambda_{2,p+1,\boldsymbol{u}} & \cdots & \lambda_{2,q,\boldsymbol{u}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p,\boldsymbol{u}} & \lambda_{p,p+1,\boldsymbol{u}} & \cdots & \lambda_{p,q,\boldsymbol{u}} \end{pmatrix}, \tag{6.16}$$

with

$$\lambda_{i,j,\boldsymbol{u}} = \prod_{k=1}^{\alpha_i} \lambda_{i,j,k,\boldsymbol{u}}, \text{ and } \lambda_{i,j,k,\boldsymbol{u}} = \lambda_{i,j,k,0} + \sum_{\ell=1}^{n-s} \lambda_{i,j,k,\ell} x_\ell + \sum_{\ell=n-s+1}^{n} \lambda_{i,j,k,\ell} \phi_{\ell,\boldsymbol{u}}(x_1, \ldots, x_{n-s}).$$

Since the first coordinate of $\tilde{\boldsymbol{x}}'$ is non-zero and all p-minors of $\boldsymbol{L}^H_{\boldsymbol{u}}$ are homogeneous, Euler's relation implies that the Jacobian matrix of $\boldsymbol{L}_u$ with respect to $(x_1, \ldots, x_{n-s})$ has full rank $n-s$ at $\tilde{\boldsymbol{x}}$.

We now can prove at any points in $V(\boldsymbol{A})$, the Jacobian matrix of $\boldsymbol{A}$ with respect to $x_1, \ldots, x_n$ has full rank n. The first step is similar to what we did in Subsection 6.2.4. For

$i = 1, \ldots, s$, the equation a_i is a product of linear forms $a_i = \prod_{k=1}^{\gamma_i} \mu_{i,k}$ with $\mu_{i,u_i}(\boldsymbol{x}) = 0$. Since the coefficients $\mu_{i,k,\ell}$ are chosen generically, then $\mu_{i,k}(\boldsymbol{x}) \neq 0$ for $i = 1, \ldots, s$ and $k \neq u_i$. As a result, in the local ring at $\boldsymbol{x}$, the polynomials $(a_1, \ldots, a_s)$ are equal, up to units, to the linear forms $(\mu_{1,u_1}, \ldots, \mu_{s,u_s})$. This further implies that

$$x_{n-s+1} - \phi_{n-s+1,\boldsymbol{u}}(x_1, \ldots, x_{n-s}), \ldots, x_n - \phi_{n,\boldsymbol{u}}(x_1, \ldots, x_{n-s}) \tag{6.17}$$

belong to the ideal generated by $(a_1, \ldots, a_s)$ in $\mathcal{O}_{\boldsymbol{x}}$.

In the next step, we consider p-minor $\zeta \in \mathbb{K}[x_1, \ldots, x_n]$ of $\boldsymbol{L}$. Let $\zeta_{\boldsymbol{u}} \in \mathbb{K}[x_1, \ldots, x_{n-s}]$ be the corresponding polynomial obtained after applying the substitution in (6.17) in $\boldsymbol{L}$. Note that $\zeta_{\boldsymbol{u}}$ is a p-minor of $\boldsymbol{L}_{\boldsymbol{u}}$, where $\boldsymbol{L}_{\boldsymbol{u}}$ is defined in (6.16), and all p-minors of $\boldsymbol{L}_{\boldsymbol{u}}$ are obtained by this way. Since ζ and all polynomials in (6.17) are in $\langle \boldsymbol{A} \rangle \cdot \mathcal{O}_{\boldsymbol{x}}$, the polynomial $\zeta_{\boldsymbol{u}}$ is in this ideal as well. Further, we have shown above that the Jacobian matrix of the p-minors of $\boldsymbol{L}_{\boldsymbol{u}}$ with respect to $(x_1, \ldots, x_{n-s})$ has full rank $n - s$ at $\tilde{\boldsymbol{x}}'$. Then taking all $\zeta_{\boldsymbol{u}}$ into account, together with the equations in (6.17), we obtain a family of polynomials in $\langle \boldsymbol{A} \rangle \cdot \mathcal{O}_{\boldsymbol{x}}$ whose Jacobian matrix has rank n at $\boldsymbol{x}$. This finishes our proof.

In view of the previous paragraphs, we can then apply Proposition 5.2.1 and Proposition 5.2.7. We deduce that the sum of multiplicities of the isolated solutions of $\boldsymbol{C} = \boldsymbol{B}_{t=1}$ is at most c', where c' is the number of isolated solutions of $\boldsymbol{A}$. We will establish precisely the value of c' in Subsection 6.3.5.

6.3.3 A subroutine to solve the start systems

In this subsection, we let $s = 0$, and so $n = q - p + 1$. We consider matrices $\boldsymbol{P}$ and $\boldsymbol{L}$ as in Subsection 6.3.1, but with $x_0 = 1$. That is

$$\boldsymbol{P} = \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,q} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,q} \\ \vdots & & & \vdots \\ \lambda_{p,1} & \lambda_{p,2} & \cdots & \lambda_{p,q} \end{pmatrix}, \tag{6.18}$$

and

$$\boldsymbol{L} = \begin{pmatrix} \lambda_{1,1} & 0 & \cdots & 0 & \lambda_{1,p+1} & \cdots & \lambda_{1,q} \\ 0 & \lambda_{2,2} & \cdots & 0 & \lambda_{2,p+1} & \cdots & \lambda_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p} & \lambda_{p,p+1} & \cdots & \lambda_{p,q} \end{pmatrix}, \tag{6.19}$$

where for all i, j, $\lambda_{i,j}$ is the product of α_i linear forms $(\lambda_{i,j,k})_{1 \leq k \leq \alpha_i}$ in variables $\boldsymbol{X} = (x_1, \ldots, x_n)$, with coefficients in $\mathbb{K}$. The main result in this subsection is an algorithm called RowDegreeDiagonal, that takes as input $(\lambda_{i,j,k})$ as above and computes a zero-dimensional

parametrization of the set $V_p(\boldsymbol{L})$. This algorithm will be used later to solve our start system, when s can be positive.

Note that Proposition 6.3.3(i) implies that, for a generic choice of coefficients of the linear forms $(\lambda_{i,j,k})_{1\leq k\leq \alpha_i}$, there is no projective solution of $V_p(\boldsymbol{P}^H)$ and $V_p(\boldsymbol{L}^H)$ at infinity, so they are finite. As a result, the algebraic sets $V_p(\boldsymbol{P})$ and $V_p(\boldsymbol{L})$ are finite in $\overline{\mathbb{K}}^n$. We also remark that the structure of $\boldsymbol{L}$ in (6.19) is similar to the matrix in (6.14); and we have seen in Subsection 6.3.2 that the ideal $I_p(\boldsymbol{L})$ (when s equals 0) in $\mathbb{K}[\boldsymbol{X}]$ are radical. Hence, all points in $V_p(\boldsymbol{L})$ are simple and isolated.

The main idea in RowDegreeDiagonal algorithm is the observation that $\boldsymbol{x}$ belongs to $V_p(\boldsymbol{L})$ if and only if some diagonal terms of $\boldsymbol{L}$ vanish at $\boldsymbol{x}$, saying $\lambda_{i_1,i_1}(\boldsymbol{x}) = \cdots = \lambda_{i_k,i_k}(\boldsymbol{x})$ for some indices $1 \leq i_1 < \cdots < i_k \leq p$ and all others $\lambda_{i,i}(\boldsymbol{x}) \neq 0$. Then the submatrix $\boldsymbol{L}_{(i_1,\ldots,i_k),(p+1,\cdots,q)}$ of $\boldsymbol{L}$ by keeping rows $(i_1,\ldots,i_k)$ and columns $(p+1,\cdots,q)$ has rank deficient at $\boldsymbol{x}$. Furthermore, since λ_{i_r,i_r} for $r = 1,\ldots,k$ is a products of α_{i_r} linear forms, so $\lambda_{i_r,i_r}(\boldsymbol{x}) = 0$ if and only if there exits $r \in \{1,\ldots,\alpha_{i_r}\}$ such that $\lambda_{i_r,i_r,r}(\boldsymbol{x}) = 0$. Therefore, it is sufficient to do the following:

1. Consider all choices of indices $\boldsymbol{i} = (1 \leq i_1 < \cdots < i_k \leq p)$, with $1 \leq k \leq \min(n,p)$.
2. For any such $\boldsymbol{i}$, consider all $\boldsymbol{r} = (r_1,\ldots,r_k)$, with $r_t \in \{1,\ldots,\alpha_{i_t}\}$ for all t.
3. For any such $\boldsymbol{i},\boldsymbol{r}$, using the linear system $\lambda_{i_1,i_1,r_1} = \cdots = \lambda_{i_k,i_k,r_k} = 0$ to rewrite $(x_{n-x+1},\ldots,x_n)$ linearly in $(x_1,\ldots,x_{n-k})$.
4. If $k = n$, we are done. Otherwise, eliminate $(x_{n-k+1},\ldots,x_n)$ in the submatrix $\boldsymbol{L}_{\boldsymbol{i},(p+1,\ldots,q)}$ of $\boldsymbol{L}$ to obtain a matrix $\boldsymbol{L}'_{\boldsymbol{i},(p+1,\ldots,q)} \in \mathbb{K}[x_1,\ldots,x_{n-k}]^{k\times(q-p)}$. Find the values of $(x_1,\ldots,x_{n-k})$ for which $\boldsymbol{L}'_{\boldsymbol{i},(p+1,\ldots,q)}$ has rank less than k, and the corresponding values of $(x_{n-k+1},\ldots,x_n)$ by back-substitution. Note that the latter matrix is as in (6.18), but of size $k \times (q-p)$

In Step 4 above, we reduce to Problem (2) which compute the simple points of $V_k(\boldsymbol{L}'_{\boldsymbol{i},(p+1,\ldots,q)})$ (without any extra polynomials $\boldsymbol{G}$). Therefore, in the RowDegreeDiagonal algorithm, we assume the existence of a subroutine RowDegree_simple which take as input a straight-line program Γ that computes a polynomial matrix $\boldsymbol{F}$ and a sequence of polynomials $\boldsymbol{G}$, and solves Problem (2) for this input using a row-degree homotopy algorithm. We give such an algorithm RowDegree_simple in Subsection 6.3.5.

Example 6.3.2. Let $\boldsymbol{L} \in \mathbb{K}[x_1,x_2]^{2\times 3}$ given by

$$\boldsymbol{L} = \begin{bmatrix} -x_1+10x_2+1 & 0 & x_1+x_2+2 \\ 0 & (x_1-3x_2+5)(x_1+2x_2-4) & (3x_1+2x_2-1)(2x_1-3x_2+5) \end{bmatrix}.$$

Here, $n = 2, p = 2$, $q = 3$ and $(\alpha_1,\alpha_2) = (1,2)$. Let us follow the procedure above for this particular example:

Algorithm 7 RowDegreeDiagonal$((\lambda_{i,j,k})_{i,j,k})$

Input: linear forms $(\lambda_{i,j,k})_{i,j,k}$ making up the entries of $\boldsymbol{L} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ as in (6.19), with $p \leq q$ and $n = q - p + 1$
Output: a zero-dimensional parametrization $\mathscr{R}$ of $V_p(\boldsymbol{L})$

1. for any subsequence $\boldsymbol{i} = (i_1, \ldots, i_k)$ of $(1, \ldots, p)$ with $1 \leq k \leq \min(n-1, p)$
   (a) for any sequence $\boldsymbol{r} = (r_1, \ldots, r_k)$, with r_t in $\{1, \ldots, \alpha_{i_t}\}$ for all t
      i. apply Gaussian elimination to the system $\lambda_{i_1,i_1,r_1} = \cdots = \lambda_{i_k,i_k,r_k} = 0$ to rewrite $(x_{n-k+1}, \ldots, x_n)$ as linear forms $(f_{j,\boldsymbol{i},\boldsymbol{r}})_{n-k+1 \leq j \leq n}$ in $(x_1, \ldots, x_{n-k})$.
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} n^3)$
      ii. construct a straight-line program $\Gamma_{\boldsymbol{i},\boldsymbol{r}}$ that computes the matrix $\boldsymbol{P}_{(\boldsymbol{i},\boldsymbol{r})}$ in $\mathbb{K}[x_1, \ldots, x_{n-k}]^{k \times (n-1)}$ obtained by substituting $(f_{j,\boldsymbol{i},\boldsymbol{r}})_{n-k+1 \leq j \leq n}$ into $\boldsymbol{L}_{\boldsymbol{i},(p+1,\ldots,q)}$. The length of $\Gamma_{\boldsymbol{i},\boldsymbol{r}}$ is $O((n-k)n(\alpha_{i_1} + \cdots + \alpha_{i_k}))$.
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} (\alpha_{i_1} + \cdots + \alpha_{i_k}) n^3)$
      iii. $\mathscr{R}'_{\boldsymbol{i},\boldsymbol{r}} \leftarrow$ RowDegree_simple$(\Gamma_{\boldsymbol{i},\boldsymbol{r}})$ (points have coordinates $(x_1, \ldots, x_{n-k})$)
      cost: $\sum_{\boldsymbol{i},\boldsymbol{r}} T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1}, \ldots, \alpha_{i_k}), n-1)$
      iv. deduce $\mathscr{R}_{\boldsymbol{i},\boldsymbol{r}}$ from $\mathscr{R}'_{\boldsymbol{i},\boldsymbol{r}}$ by adding the expressions for $(x_{n-k+1}, \ldots, x_n)$
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} c'_{\boldsymbol{i},\boldsymbol{r}} n^2)$
2. if $n \leq p$, for any subsequence $\boldsymbol{i} = (i_1, \ldots, i_n)$ of $(1, \ldots, p)$
   (a) for any sequence $\boldsymbol{r} = (r_1, \ldots, r_n)$, with $r_t \in \{1, \ldots, \alpha_t\}$ for all t
      i. let $\boldsymbol{x}_{\boldsymbol{i},\boldsymbol{r}}$ be the solution of the system $\lambda_{i_1,i_1,r_1} = \cdots = \lambda_{i_n,i_n,r_n} = 0$
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} n^3)$
      ii. create a zero-dimensional parametrization $\mathscr{R}_{\boldsymbol{i},\boldsymbol{r}}$ such that $Z(\mathscr{R}_{\boldsymbol{i},\boldsymbol{r}}) = \{\boldsymbol{x}_{\boldsymbol{i},\boldsymbol{r}}\}$
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} n)$
3. combine all $(\mathscr{R}_{\boldsymbol{i},\boldsymbol{r}})_{\boldsymbol{i},\boldsymbol{r}}$ into the output $\mathscr{R}$
   cost: $O^{\sim}(\sum_{\boldsymbol{i},\boldsymbol{r}} c'_{\boldsymbol{i},\boldsymbol{r}} n)$

- With $\boldsymbol{i} = (1)$, we can only take $\boldsymbol{r} = (1)$. The equation $-x_1 + 10x_2 + 1 = 0$ gives the substitution $x_2 = (x_1 - 1)/10$, which we inject into $\boldsymbol{L}_{(1),(3)} = [x_1 + x_2 + 2]$, to find the solution $(-19/11, -3/11)$.
- With $\boldsymbol{i} = (2)$, we first take $\boldsymbol{r} = (1)$, so we use $x_1 - 3x_2 + 5$ to obtain $x_2 = (x_1 + 5)/3$. We inject this expression into $\boldsymbol{L}_{(2),(3)} = [(3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5)]$ to find two solutions, namely $(-7/11, 16/11)$ and $(0, 5/3)$. With $\boldsymbol{r} = (2)$, we find two other solutions, $(2/7, 13/7)$ and $(-3/2, 11/4)$.
- With $\boldsymbol{i} = (1, 2)$, we can take $\boldsymbol{r} = (1, 1)$ or $\boldsymbol{r} = (1, 2)$, which lead us to solve respectively $-x_1 + 10x_2 + 1 = x_1 - 3x_2 + 5 = 0$ and $-x_1 + 10x_2 + 1 = x_1 + 2x_2 - 4 = 0$;

we obtain two solutions, $(-53/7, -6/7)$ and $(7/2, 1/4)$. Note that in Step 4, we are in the case $k = n$, so there is no need to deal with the matrix $\boldsymbol{L}_{\boldsymbol{i},(p+1,\ldots,q)}$.

Altogether, this gives us the 7 points where the rank of $\boldsymbol{L}$ is not two.

To analysis the complexity of RowDegreeDiagonal algorithm, we denote by $T_{\text{row}}(\sigma, \boldsymbol{\gamma}, \boldsymbol{\alpha}, q)$ the time spent by RowDegree_simple(Γ) on input a straight-line program of length σ that computes a polynomial matrix with row degrees $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q columns, and $\boldsymbol{G} = (g_1, \ldots, g_s)$ of degrees $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s)$. When the polynomials $\boldsymbol{G}$ are absent, we denote the cost of RowDegree_simple(Γ) by $T_{\text{row}}(\sigma, (), \boldsymbol{\alpha}, q)$. As we said above, for the moment, we only need to use this algorithm for a particular case when there are no additional equations $\boldsymbol{G}$, and the matrix $\boldsymbol{P}$ of size $k \times (q-p)$ as matrix $\boldsymbol{P}$ in (6.18). Each entry $\lambda_{i,j}$ of such $\boldsymbol{P}$ matrix is a product of α_i linear forms in n variables, so it can be computed in $O(n\alpha_i)$ operations in $\mathbb{K}$. Then the whole matrix $\boldsymbol{P}$ can be computed by a straight-line program of length $O(n(\alpha_1+\cdots+\alpha_p)q)$. Thus, we denote the cost of Algorithm RowDegree_simple for such input by

$$T_{\boldsymbol{P},\text{row}}(\boldsymbol{\alpha}, q) = T_{\text{row}}(nq(\alpha_1 + \cdots + \alpha_p), (), \boldsymbol{\alpha}, q).$$

We conclude this subsection with the detailed presentation and cost analysis of Algorithm RowDegreeDiagonal.

Lemma 6.3.12. *Let $h_n(\alpha_1, \ldots, \alpha_p)$ be the n-th complete symmetric function of $(\alpha_1, \ldots, \alpha_p)$. For generic choices of the coefficients of $(\lambda_{i,j,k})_{i,j,k}$,* RowDegreeDiagonal$((\lambda_{i,j,k})_{i,j,k})$ *computes a zero-dimensional parametrization of $V_p(\boldsymbol{L})$ in time*

$$\sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k)\\ k\le\min(n-1,p)}} \alpha_{i_1}\cdots\alpha_{i_k} T_{\boldsymbol{P},\text{row}}((\alpha_{i_1},\ldots,\alpha_{i_k}), n-1) + O^{\sim}\left(n^3(c' + h_n(\alpha_1,\ldots,\alpha_p))\right),$$

where c' is the cardinality of $V_p(\boldsymbol{L})$.

Proof. The cost of Step 1(a)i is straightforward as the cost of Gaussian elimination to a linear systems of k equations is $O(n^3)$; so the total is $\sum_{\boldsymbol{i},\boldsymbol{r}} n^3$. Step 1(a)ii uses the linear forms $(f_{j,\boldsymbol{i},\boldsymbol{r}})_{n-k+1\le j\le n}$ to construct a straight-line program $\Gamma_{\boldsymbol{i},\boldsymbol{r}}$ that computes the entries of $\boldsymbol{L}_{\boldsymbol{i},(p+1,\ldots,q)}$, in which we replace x_j by $f_{j,\boldsymbol{i},\boldsymbol{r}}(x_1,\ldots,x_{n-k})$, for $j = n-k+1,\ldots,n$. This is done by computing the coefficients of the linear forms in $(x_1,\ldots,x_{n-k})$ obtained after substitution. Each linear form requires a matrix-vector product with a matrix of size $(n-k)\times n$, for $O(n^2)$ operations, whence a total of $O((\alpha_{i_1}+\cdots+\alpha_{i_k})n^3)$ for all entries.

For fixed sequences $\boldsymbol{i}, \boldsymbol{r}$, the size of $\boldsymbol{P}_{\boldsymbol{i},\boldsymbol{r}}$ is $k\times(q-p)$ which is $k\times(n-1)$, then the cost of RowDegree_simple$(\Gamma_{\boldsymbol{i},\boldsymbol{r}})$ is $T_{\boldsymbol{P},\text{row}}((\alpha_{i_1},\ldots,\alpha_{i_k}), n-1)$; so the total cost of Step 1(a)iii is

$$\sum_{\boldsymbol{i},\boldsymbol{r}} T_{\boldsymbol{P},\text{row}}((\alpha_{i_1},\ldots,\alpha_{i_k}), n-1).$$

Step 1(a)iv consists in adding k coordinates $(x_{n-k+1}, \ldots, x_n)$ to a zero-dimensional parametrization in variables $(x_1, \ldots, x_{n-k})$, where $(x_{n-k+1}, \ldots, x_n)$ are known as linear forms $(f_{j,\boldsymbol{i},\boldsymbol{r}})_{n-k+1\le j\le n}$ in $(x_1, \ldots, x_{n-k})$. This can be done by means of a matrix product in size $k \times (n-k)$ by $(n-k) \times c'_{\boldsymbol{i},r}$, where $c'_{\boldsymbol{i},\boldsymbol{r}}$ is the number of solutions we obtain from $\mathsf{RowDegree_simple}(\Gamma_{\boldsymbol{i},\boldsymbol{r}})$ (that is the number of points in $V_k(\boldsymbol{P}_{\boldsymbol{r},\boldsymbol{i}})$). The cost is thus $O(c'_{\boldsymbol{i},\boldsymbol{r}} n^2)$ which gives the total cost for Step 1(a)iv is $O(c'n^2)$ since the sum of all $c'_{\boldsymbol{i},\boldsymbol{r}}$ is equal to c'.

The analysis for the Step 2's complexity is straightforward. Gaussian elimination take $O(n^3)$ operations in $\mathbb{K}$, for fixed sequences $\boldsymbol{i}, \boldsymbol{r}$ and creating a zero-dimensional parametrization for a point of n coordinates requires $O(n)$ operations. Finally, the combination in Step 3 is done by fast Chinese Remaindering, in quasi-linear time $O^{\sim}(\sum_{\boldsymbol{i},\boldsymbol{r}} c'_{\boldsymbol{i},\boldsymbol{r}} n)$, which is $O^{\sim}(c'n)$.

Thus, the total runtime is

$$\sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k)\\ \boldsymbol{r}=(r_1,\ldots,r_k)\\ k\le\min(n-1,p)}} T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1},\ldots,\alpha_{i_k}), n-1) + O^{\sim}\left(c'n^2 + \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k)\\ \boldsymbol{r}=(r_1,\ldots,r_k)\\ k\le\min(n-1,p)}} (\alpha_{i_1}+\cdots+\alpha_{i_k})n^3 + \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_n)\\ \boldsymbol{r}=(r_1,\ldots,r_n)}} n^3 \right).$$

The costs reported in the sums do not depend on $\boldsymbol{r}$, so that this can be rewritten as

$$\sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k)\\ k\le\min(n-1,p)}} \alpha_{i_1}\cdots\alpha_{i_k} T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1},\ldots,\alpha_{i_k}), n-1) + O^{\sim}\left(c'n^2 + \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k)\\ k\le\min(n-1,p)}} \alpha_{i_1}\cdots\alpha_{i_k}(\alpha_{i_1}+\cdots+\alpha_{i_k})n^3 + \sum_{\boldsymbol{i}=(i_1,\ldots,i_n)} \alpha_{i_1}\cdots\alpha_{i_n} n^3 \right).$$

Finally, since

$$\sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k)\\ k\le\min(n-1,p)}} \alpha_{i_1}\cdots\alpha_{i_k}(\alpha_{i_1}+\cdots+\alpha_{i_k}) \le h_n(\alpha_1,\ldots,\alpha_p) \text{ and } \sum_{\boldsymbol{i}=(i_1,\ldots,i_n)} \alpha_{i_1}\cdots\alpha_{i_n} \le h_n(\alpha_1,\ldots,\alpha_p),$$

we obtain our claim. □

Example 6.3.3. In Example 6.3.2, we already found the coordinates of all points in $V_2(\boldsymbol{L})$ (they may not be rational for other values of p, q). The only thing left to do is to describe

them by means of a univariate representation; we write it as $((w, v_1, v_2), x_2)$, with

$$w = y^7 - \frac{226}{33}y^6 + \frac{1428899}{94864}y^5 - \frac{2137943}{284592}y^4 - \frac{1146637}{94864}y^3 + \frac{3111547}{284592}y^2 + \frac{46547}{47432}y - \frac{390}{539}$$
$$v_1 = -\frac{589}{77}y^6 + \frac{3963109}{71148}y^5 - \frac{14713869}{94864}y^4 + \frac{1345585}{6776}y^3 - \frac{9415375}{94864}y^2 - \frac{843103}{71148}y + \frac{138935}{6776}$$
$$v_2 = \frac{226}{33}y^6 - \frac{1428899}{47432}y^5 + \frac{2137943}{94864}y^4 + \frac{1146637}{23716}y^3 - \frac{15557735}{284592}y^2 - \frac{139641}{23716}y + \frac{390}{77}.$$

6.3.4 Solving the start systems

To perform the homotopy, we need the solutions of the start system, that is, a zero-dimensional parametrization of $V(\boldsymbol{A})$. In this subsection, we describe how to obtain it.

The main step in our algorithm uses algorithm RowDegreeDiagonal given in the previous subsection. Recall that our start system $\boldsymbol{A} = (a_1, \ldots, a_s, \ldots, a_m)$ is built as $(a_1, \ldots, a_s) = (m_1, \ldots, m_s)$, where $(m_1, \ldots, m_s)$, of degrees $(\gamma_1, \ldots, \gamma_s)$, are given in (6.13) and $(a_{s+1}, \ldots, a_m)$ are p-minors of $\boldsymbol{L}$, where $\boldsymbol{L}$, of row degrees $(\alpha_1, \ldots, \alpha_p)$, is defined in (6.14).

For any sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, with u_i in $\{1, \ldots, \gamma_i\}$ for all i, we start by using the equations $\mu_{1,u_1} = \cdots = \mu_{s,u_s} = 0$, to express $(x_{n-s+1}, \ldots, x_n)$ as linear forms $(\phi_{n-s+1,\boldsymbol{u}}, \ldots, \phi_{n,\boldsymbol{u}})$ in $(x_1, \ldots, x_{n-s})$. After substituting these linear forms into $\boldsymbol{L}$, we get the matrix $\boldsymbol{L}_{\boldsymbol{u}}$ from (6.16) which is in $\mathbb{K}[x_1, \ldots, x_{n-s}]^{p\times q}$; we remark that $n-s = q-p+1$. Then, we can apply Algorithm RowDegreeDiagonal with the input is the entries of $\boldsymbol{L}_{\boldsymbol{u}}$. The final step is finding the values of $(x_{n-s+1}, \ldots, x_n)$ by back-substitution. All of the discussion lead to Algorithm RowDegreeStart(Δ) which takes a straight-line program that computes $\boldsymbol{M}$ in (6.13) and $\boldsymbol{L}$ (6.14), and outputs a zero-dimensional parametrization of $V_p(\boldsymbol{L}, \boldsymbol{V})$.

The rest of this subsection is devoted to analyze the cost of Algorithm RowDegreeStart.

Lemma 6.3.13. *For generic choices of the coefficients of $(\lambda_{i,j,k})_{i,j,k}$ and $(\mu_{i,k})_{i,k}$, the Algorithm* RowDegreeStart$(\boldsymbol{L}, \boldsymbol{V})$ *computes a zero-dimensional parametrization of $V_p(\boldsymbol{L}, \boldsymbol{V})$ in time*

$$\gamma_1 \cdots \gamma_s \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k) \\ k\le \min(n-s-1,p)}} \alpha_{i_1} \cdots \alpha_{i_k} T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1}, \ldots, \alpha_{i_k}), n - s - 1) + \tilde{O}(c' n^3). \quad (6.20)$$

Proof. Let $\Delta_{\boldsymbol{L}}$ be a straight-line program that computes $\boldsymbol{L}$. For all i, j, $\Delta_{\boldsymbol{L}}$ computes and multiplies the values of the α_i linear forms invoked in $\lambda_{i,j}$ using $O(n\alpha_i)$ steps. So, the total length of $\Delta_{\boldsymbol{L}}$ is $\sigma_{\boldsymbol{L}} = O(n^2(\alpha_1 + \cdots + \alpha_p))$, which is $O(n^2 p\alpha)$, with $\alpha = \max(\alpha_1, \ldots, \alpha_p)$. For any sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, expressing $(x_{n-s+1}, \ldots, x_n)$ as linear forms $(\phi_{1,\boldsymbol{u}}, \ldots, \phi_{n-s,\boldsymbol{u}})$ in $(x_1, \ldots, x_{n-s})$ takes a total of $O(\gamma_1 \cdots \gamma_s n^3)$ operations in $\mathbb{K}$. From this, we deduce a

Algorithm 8 RowDegreeStart(Δ)

Input: a straight-line program Δ that computes $\boldsymbol{L} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ as in (6.19) and $\boldsymbol{M} \in \mathbb{K}[x_1, \ldots, x_n]^s$ as in (6.13) with $p \leq q$ and $n = q - p + s + 1$
Output: a zero-dimensional parametrization of the points of $V_p(\boldsymbol{L}, \boldsymbol{V})$

1. for any sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, with $u_i \in \{1, \ldots, \gamma_i\}$ for all i
   (a) apply Gaussian elimination to the system $\mu_{1,u_1} = \cdots = \mu_{s,u_s} = 0$ from (6.13) to rewrite $(x_{n-s+1}, \ldots, x_n)$ as linear forms $(\phi_{k,\boldsymbol{u}})_{n-s+1 \leq k \leq n}$ in $(x_1, \ldots, x_{n-s})$
   cost: $O(\gamma_1 \cdots \gamma_s n^3)$
   (b) construct a straight-line program $\Delta_{\boldsymbol{u}}$ that computes the matrix $\boldsymbol{L}_{\boldsymbol{u}} \in \mathbb{K}[x_1, \ldots, x_{n-s}]^{p \times q}$ obtained by substituting $(\phi_{k,\boldsymbol{u}})_{n-s+1 \leq k \leq n}$ into $\boldsymbol{L}$
   length of $\Delta_{\boldsymbol{u}}$ is $O(n^2 p \alpha)$
   (c) $\mathscr{R}'_{\boldsymbol{u}} \leftarrow$ RowDegreeDiagonal($\Gamma_{\boldsymbol{u}}$) (points have coordinates $(x_1, \ldots, x_{n-s})$
   cost: $\gamma_1 \cdots \gamma_s \mathscr{T}$, for $\mathscr{T}$ as in (6.21)
   (d) deduce $\mathscr{R}_{\boldsymbol{u}}$ from $\mathscr{R}'_{\boldsymbol{u}}$ by adding the expressions for $(x_{n-s+1}, \ldots, x_n)$
   cost: $O(c' n^2)$, with $c' = \gamma_1 \cdots \gamma_s h_{n-s}(\alpha_1, \ldots, \alpha_p)$
2. combine all $\mathscr{R}_{\boldsymbol{u}}$ into $\mathscr{R}$
   cost: $O^{\sim}(c'n)$

straight-line program $\Delta_{\boldsymbol{u}}$ that computes the entries of matrix $\boldsymbol{L}_{\boldsymbol{u}}$ from (6.16): it simply consists in $\Delta_{\boldsymbol{L}}$, to which we add $O(n^2)$ operations that evaluate $(\phi_{n-s+1,\boldsymbol{u}}, \ldots, \phi_{n,\boldsymbol{u}})$.

Given a straight-line program $\Delta_{\boldsymbol{u}}$, we can then apply Algorithm RowDegreeDiagonal to compute a zero-dimensional parametrization $\mathscr{R}'_{\boldsymbol{u}}$ of $V_p(\boldsymbol{L}_{\boldsymbol{u}})$. Corollary 6.3.15 in the next subsection implies that the number of points in the output is $h_{n-s}(\alpha_1, \ldots, \alpha_p)$, so by Lemma 6.3.12, Algorithm RowDegreeDiagonal takes time

$$\mathscr{T} := \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k) \\ k \leq \min(n-s-1,p)}} \alpha_{i_1} \cdots \alpha_{i_k} T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1}, \ldots, \alpha_{i_k}), n-s-1) + O^{\sim}(h_{n-s}(\alpha_1, \ldots, \alpha_p) n^3). \tag{6.21}$$

Since there are $\gamma_1 \cdots \gamma_s$ choices of $\boldsymbol{u}$, then the total cost of Step 1c is $\gamma_1 \cdots \gamma_s \mathscr{T}$.

Step 1d adds to each $\mathscr{R}'_{\boldsymbol{u}}$, which involves only variables $(x_1, \ldots, x_{n-s})$, the expression of $(x_{n-s+1}, \ldots, x_n)$ obtained from $(\phi_{n-s+1,\boldsymbol{u}}, \ldots, \phi_{n,\boldsymbol{u}})$. As in the analysis of Algorithm RowDegreeDiagonal, the total runtime is $O(\gamma_1 \cdots \gamma_s h_{n-s}(\alpha_1, \ldots, \alpha_p) n^2) = O(c' n^2)$. Finally, we combine the resulting parametrizations $(\mathscr{R}_{\boldsymbol{u}})_{\boldsymbol{u}}$ into a single parametrization $\mathscr{R}$ using Chinese Remaindering, in time $O^{\sim}(\gamma_1 \cdots \gamma_s h_{n-s}(\alpha_1, \ldots, \alpha_p) n) = O^{\sim}(c'n)$.

Thus, the overall time spent in computing the zero-dimensional parametrization $\mathscr{R}$ of $V(\boldsymbol{L}, \boldsymbol{V})$ is $\gamma_1 \cdots \gamma_s \mathscr{T} + O^{\sim}(c' n^3)$, as desired. □

6.3.5 The row-degree homotopy algorithms

We can now finish our proofs for Propositions 6.3.1 and 6.3.2 by establishing first a bound for the number of isolated points, counting with multiplicities, of $V_p(\boldsymbol{F}, \boldsymbol{G})$. Then we show how to compute the simple points in $V_p(\boldsymbol{F}, \boldsymbol{G})$ by an algorithm called RowDegree_simple. This algorithm is used by algorithm RowDegreeStart of the previous subsection. Finally, by a minor modification of the algorithm, we show how to compute the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

It is shown in Subsection 6.3.2 that the sum of the multiplicities of the isolated solutions of $\boldsymbol{C} = \boldsymbol{B}_{t=1}$ is at most c', where c' is the number of isolated points in $V(\boldsymbol{A})$, with $\boldsymbol{A} = \boldsymbol{B}_{t=0}$. It remains to establish the value of c' which is given in Corollary 6.3.15 below.

Lemma 6.3.14. *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ be positive integers, and let $h_t(\alpha_1, \ldots, \alpha_p)$ be the complete symmetric function of degree k in $\alpha_1, \ldots, \alpha_p$. For generic $p \times q$ matrices $\boldsymbol{L}$ as in (6.19) or $\boldsymbol{P}$ as in (6.18), with entries in $t = q - p + 1$ variables, $V_p(\boldsymbol{L})$ and $V_p(\boldsymbol{P})$ have cardinality $h_t(\alpha_1, \ldots, \alpha_p)$.*

Proof. We first show that if the claim holds for $\boldsymbol{L}$ of size $p \times q$, it holds for $\boldsymbol{P}$ of size $p \times q$ as well. To do it, we set up a homotopy between $\boldsymbol{L}$ and $\boldsymbol{P}$, where $\boldsymbol{L}$ is the start matrix and $\boldsymbol{P}$ is the target one, by considering a deformation $(1-t)\cdot\boldsymbol{L} + t\cdot\boldsymbol{P}$. The discussion in Subsection 6.3.2 shows that, for generic choices of the coefficients of the entries of $\boldsymbol{L}$, this matrix satisfies the properties C_1 and C_2 at $t = 0$. Recall that the property C_1 is equivalent to degree bound and no solution at infinity properties which are stated in Lemma 6.1.1. We claim that the C_1 and C_2 properties (equivalently, degree bound, no solution at infinity, no multiplicities) hold as well at $t = 1$. The degree bound can be obtained by a similar way as what we did for $t = 0$, and the latter two are restatements of Proposition 6.3.3. As a result, we can apply Proposition 5.2.7 to the specializations of $(1-t)\cdot\boldsymbol{L} + t\cdot\boldsymbol{P}$ at both $t = 0$ and $t = 1$, and conclude that $V_p(\boldsymbol{L})$ and $V_p(\boldsymbol{P})$ have the same cardinality, for generic choices of the coefficients of $\boldsymbol{L}$ and $\boldsymbol{P}$.

We finish our proof by induction on the sizes of the matrices and their row degrees. If $p = q$, then $t = 1$, $\boldsymbol{L}$ is diagonal and its entries are products of generic linear forms, so its determinant has degree $\alpha_1 + \cdots + \alpha_p = h_1(\alpha_1, \cdots, \alpha_p)$. Then, our claim holds for $\boldsymbol{L}$, and so for $\boldsymbol{P}$. Suppose now that the claim is true for all $p' \leq p$ and all $q' < q$ with $p' \leq q'$ and for all choices of degrees $(\alpha_1, \ldots, \alpha_{p'})$. Following Algorithm RowDegreeDiagonal, we obtain

$$|V_p(\boldsymbol{L})| = \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k)\\ \boldsymbol{r}=(r_1,\ldots,r_k)}} |V_k(\boldsymbol{P}_{\boldsymbol{i},\boldsymbol{r}})|,$$

for all subsequences $\boldsymbol{i} = (i_1, \ldots, i_k)$ of length $k \in \{1, \ldots, \min(t-1, p)\}$ and $\boldsymbol{r} = (r_1, \ldots, r_k)$, with $r_k \in \{1, \ldots, \alpha_k\}$ for all k, and where matrix $\boldsymbol{P}_{(\boldsymbol{i},\boldsymbol{r})}$ is from Step 1(a)ii of that algorithm. If $k \leq p$ and $t - 1 < q$, with row degrees $(\alpha_{i_1}, \ldots, \alpha_{i_p})$, we can apply our induction

assumption to such matrices. In addition, if $t \leq p$, we should take into account one extra point for each subsequence $(i_1, \ldots, i_t)$ of $(1, \ldots, p)$. Altogether, we obtain

$$|V_p(\boldsymbol{L})| = \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_k),\\ \boldsymbol{r}=(r_1,\ldots,r_k)}} h_{t-k}(\alpha_{i_1}, \ldots, \alpha_{i_k}),$$

for $k \in \{1, \ldots, \min(t, p)\}$, since $h_0 = 1$. For any given $\boldsymbol{i} = (i_1, \ldots, i_k)$, there are $\alpha_{i_1} \cdots \alpha_{i_k}$ choices of indices $\boldsymbol{r}$, so that we have

$$|V_p(\boldsymbol{L})| = \sum_{\boldsymbol{i}=(i_1,\ldots,i_k)} \alpha_{i_1} \cdots \alpha_{i_k} h_{t-k}(\alpha_{i_1}, \ldots, \alpha_{i_k}),$$

for $\boldsymbol{i} = (i_1, \ldots, i_k)$ subsequence of $(1, \ldots, p)$ with $k \in \{1, \ldots, \min(t, p)\}$. The latter sum is precisely $h_t(\alpha_1, \ldots, \alpha_p)$, so we are done. □

Corollary 6.3.15. *For a generic choice of coefficients $\mu_{i,k,\ell}$ and $\lambda_{i,j,k,\ell}$, the cardinality c' of the algebraic set $V(\boldsymbol{A})$ is $\gamma_1 \cdots \gamma_s h_{n-s}(\alpha_1, \ldots, \alpha_p)$.*

Proof. For a sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, where $u_i \in \{1, \ldots, \gamma_i\}$, as above, let $V_{\boldsymbol{u}}$ be the subset of $V(\boldsymbol{A})$ consisting of all points $\boldsymbol{x}$ such that $\mu_{i,u_i}(\boldsymbol{x}) = 0$ for all $i = 1, \ldots, s$. We remark that the sets $V_{\boldsymbol{u}}$ are generically pairwise disjoint as the ideal $\langle \boldsymbol{A} \rangle \subset \overline{\mathbb{K}}[\boldsymbol{X}]$ is radical.

For a fixed sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, the cardinality of $V_{\boldsymbol{u}}$ is equal the number of points in $V(\boldsymbol{L}_{\boldsymbol{u}})$, with $V(\boldsymbol{L}_{\boldsymbol{u}})$ is a polynomial matrix of size $p \times q$ and all entries of $\boldsymbol{L}_{\boldsymbol{u}}$ are products of generic linear forms in $n - s = q - p + 1$ variables. Moreover, the row degrees of $\boldsymbol{L}_{\boldsymbol{u}}$ are $(\alpha_1, \ldots, \alpha_p)$. By Lemma 6.3.14, the cardinality of $V_p(\boldsymbol{L}_{\boldsymbol{u}})$ is $h_{n-s}(\alpha_1, \ldots, \alpha_p)$; and then the conclusion follows as there are $\gamma_1 \cdots \gamma_s$ choices of $\boldsymbol{u}$. □

Next, we show how to use Homotopy_simple in Proposition 5.2.12 to compute the simple points in $V_p(\boldsymbol{F}, \boldsymbol{G})$. We start by a description of the required input for this algorithm. We assume that we are given a straight-line program Γ of length σ that compute the matrix $\boldsymbol{F}$ and the system of equations $\boldsymbol{G}$.

A zero-dimensional parametrization of $V(\boldsymbol{A})$. To perform the homotopy, we need a zero-dimensional parametrization of the start system. This is done by using Algorithm RowDegeeStart in Subsection 6.3.4 with the cost is given in (6.20).

An upper bound on the degree of the homotopy curve. Next, we need to determine an upper bound e' on the degree of the homotopy curve $V(J')$, where J' is the union of the one-dimensional irreducible components of $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$whose projection on the t-axis is dense. Following a similar process as what we did in Subsection 6.2.5, we conclude that we can take $e' = (\gamma_1 + 1) \cdots (\gamma_s + 1) \cdot h_{n-s}(\alpha_1 + 1, \ldots, \alpha_p + 1)$.

Algorithm 9 RowDegree_simple(Γ)

Input: a straight-line program Γ of length σ that computes $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with $\deg(f_{i,j}) \leq \alpha_i$ and $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ with $p \leq q$, $n = q - p + s + 1$
Output: a zero-dimensional parametrization of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$

1. construct a straight-line program Δ that computes $\boldsymbol{L} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ as in (6.14) and $\boldsymbol{M} \in \mathbb{K}[x_1, \ldots, x_n]^s$ as in (6.13).

   length of Δ is $O(n^2 p\alpha + nsγ)$

2. $\mathscr{R}_0 \leftarrow$ RowDegreeStart(Δ)

   cost: given in (6.20)

3. construct a straight-line program Γ' that computes all polynomials $\boldsymbol{B}$

   length of Γ' is $\sigma' = O(\sigma + \binom{q}{p} n^3 + n^2 p\alpha + n^2\gamma)$

4. return Homotopy_simple($\Gamma', \mathscr{R}_0, e'$)

   cost: $O^{\sim}(c'^2 mn^2 + c'e'n(\sigma' + n^2))$, with
   $e' = (\gamma_1 + 1) \cdots (\gamma_s + 1) h_{n-s}(\alpha_1 + 1, \ldots, \alpha_p + 1)$

A straight-line program for $\boldsymbol{B}$. Finally, we need to give an estimate on the size of a straight-line program that computes $\boldsymbol{B} = (b_1, \ldots, b_m)$, assuming that we are give a straight-line program Γ of length σ that computes the input $(\boldsymbol{F}, \boldsymbol{G})$.

As we have seen in Subsection 6.3.4, a straight-line program Δ that computes the matrix $\boldsymbol{L}$ and polynomials $\boldsymbol{V}$ has length $O(n^2 p\alpha + n^2\gamma)$, where $\alpha = \max(\alpha_1, \ldots, \alpha_p)$. For an extra $O(\binom{q}{p} n^3)$ operations, we can compute all entries of $\boldsymbol{U} = (1 - t) \cdot \boldsymbol{L} + t \cdot \boldsymbol{F}$ and all p-minors $(b_{s+1}, \ldots, b_m)$ of this matrix. Therefore, we have obtained a straight-line program Γ' that computes $\boldsymbol{B} = (b_1, \ldots, b_m)$ using

$$\sigma' = \sigma + O\left(\binom{q}{p} n^3 + n^2 p\alpha + n^2\gamma\right)$$

operations in $\mathbb{K}$.

With all above, we can now give the Algorithm RowDegree_simple and its cost. To estimate this complexity, we use Lemma 6.3.13, which provides a cost to compute the solutions of the start system, and Proposition 5.2.12 for the cost of Algorithm Homotopy_simple.

Example 6.3.4. We show how to solve the example given in the introduction (Example 4.3.1), using this time a row-degree homotopy. Recall that in this example, we have $s = 0$, $(\alpha_1, \alpha_2) = (1, 2)$ and $c' = 7$. Thus, we do not need polynomials $\boldsymbol{V}$; our start matrix $\boldsymbol{L}$ is taken as in Example 6.3.2.

We already gave in Example 6.3.3 a zero-dimensional parametrization $\mathscr{R}_0$ of the solutions of the start system, that is, of the 2-minors of $\boldsymbol{L}$. The upper bound e' on the degree of the homotopy curve is $e' = 2^2 + 2 \cdot 3 + 3^3 = 19$.

Running algorithm Homotopy_simple, we construct a zero-dimensional parametrization $\mathscr{S}$ with coefficients in $\mathbb{Q}(t)$ that describes the homotopy curve; specialization at $t = 1$ in it does not induce any division by zero. Doing so gives us the zero-dimensional parametrization describing the zeros of the 2-minors of $\boldsymbol{F}$ already seen in Example 4.3.2.

Given σ', the length of a straight-line program that computes $\boldsymbol{B}$, the complexity of Algorithm Homotopy_simple is $O^{\sim}(c'^2mn^2 + c'e'n(\sigma' + n^2))$ operations in $\mathbb{K}$. Since $\sigma' = \sigma + O\left(\binom{q}{p}n^3 + n^2p\alpha + n^2\gamma\right)$, we can use $O\left(\binom{q}{p}n^3(\sigma + p\alpha + \gamma)\right)$ as an upper bound for $\sigma' + n^2$. This gives an upper bound of

$$O^{\sim}\left(c'^2mn^2 + c'e'n\binom{q}{p}n^3(\sigma + p\alpha + \gamma)\right)$$

for the cost of Algorithm Homotopy_simple. Moreover, since $c' \leq e'$ and $m \leq n + \binom{q}{p} \leq n\binom{q}{p}$, the total cost of this algorithm becomes

$$O^{\sim}\left(c'e'\binom{q}{p}n^4(\sigma + p\alpha + \gamma)\right).$$

Together with the complexity of Algorithm RowDegreeStart which is given in (6.20), the total cost of Algorithm RowDegree_simple is

$$T_{\mathrm{row}}(\sigma, \boldsymbol{\gamma}, \boldsymbol{\alpha}, q) = \gamma_1 \cdots \gamma_s \mathscr{T} + O^{\sim}\left(\binom{q}{p}n^4c'e'(\sigma + p\alpha + \gamma)\right),$$

with $\mathscr{T}$ as in (6.21). Since $e' \geq 2^n$ (because $\alpha_i \geq 1$ and $\gamma_i \geq 1$ by assumption), this complexity becomes

$$T_{\mathrm{row}}(\sigma, \boldsymbol{\gamma}, \boldsymbol{\alpha}, q) = \gamma_1 \cdots \gamma_s \mathscr{T} + O^{\sim}\left(\binom{q}{p}c'e'(\sigma + p\alpha + \gamma)\right). \tag{6.22}$$

Note that $\mathscr{T}$ is depended on the $T_{\boldsymbol{P},\mathrm{row}}$. This allows us to give an estimate on $T_{\boldsymbol{P},\mathrm{row}}$ by solving a few recurrence relations. Recall that $T_{\boldsymbol{P},\mathrm{row}}$ describes the case where $s = 0$, so that $\gamma_1 \cdots \gamma_s = 1$, and $\boldsymbol{P}$ is a $p \times q$ input matrix as in (6.18). In this case, we can take $\sigma = O((q-p)q(\alpha_1 + \cdots + \alpha_p)) \in O((q-p)pq\alpha)$. Following our convention, the runtime $T_{\mathrm{row}}(\sigma, (), (\alpha_1, \ldots, \alpha_p), q)$ is then written $T_{\boldsymbol{P},\mathrm{row}}((\alpha_1, \ldots, \alpha_p), q)$.

Lemma 6.3.16. *One can take*

$$T_{\boldsymbol{P},\mathrm{row}}((\alpha_1, \ldots, \alpha_p), q) = O^{\sim}\left(\binom{q}{p}h_{q-p+1}(\alpha_1, \ldots, \alpha_p)h_{q-p+1}(\alpha_1 + 1, \ldots, \alpha_p + 1)pq\alpha\right),$$

with $\alpha = \max(\alpha_1, \ldots, \alpha_p)$.

Proof. Taking into account that $\gamma = 1$, Equation (6.22), combined with the definition of $\mathscr{T}$ in (6.21), gives the recursion

$$T_{\boldsymbol{P},\mathrm{row}}((\alpha_1,\dots,\alpha_p),q) = \sum_{\substack{\boldsymbol{i}=(i_1,\dots,i_\kappa)\\ \kappa\le\min(q-p,p)}} \alpha_{i_1}\cdots\alpha_{i_\kappa} T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1},\dots,\alpha_{i_\kappa}),q-p)$$
$$+ \tilde{O}\left(\binom{q}{p} h_{q-p+1}(\alpha_1,\dots,\alpha_p) S_{q-p+1}(\alpha_1+1,\dots,\alpha_p+1)pq\alpha\right); \quad (6.23)$$

notice that a factor $(q-p)$ disappeared from the last term, since it can be absorbed in the logarithmic factors in the $\tilde{O}(\ )$. Let us rewrite the second summand as

$$h_{q-p+1}(\alpha_1,\dots,\alpha_p) C((\alpha_1,\dots,\alpha_p),q),$$

with

$$C((\alpha_1,\dots,\alpha_p),q) = \tilde{O}\left(\binom{q}{p} h_{q-p+1}(\alpha_1+1,\dots,\alpha_p+1)pq\alpha\right).$$

This term is at its maximum at the root of the recursion tree. Thus, we can find an upper bound on $T_{\boldsymbol{P},\mathrm{row}}$ by finding a solution to the recurrence

$$T_{\boldsymbol{P},\mathrm{row}}((\alpha_1,\dots,\alpha_p),q) = \sum_{\substack{\boldsymbol{i}=(i_1,\dots,i_\kappa)\\ \kappa\le\min(q-p,p)}} \alpha_{i_1}\cdots\alpha_{i_\kappa} T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1},\dots,\alpha_{i_\kappa}),q-p) \quad (6.24)$$
$$+ h_{q-p+1}(\alpha_1,\dots,\alpha_p)K, \quad (6.25)$$

for some constant K, and replacing K by $\tilde{O}\left(\binom{q}{p} h_{q-p+1}(\alpha_1+1,\dots,\alpha_p+1)pq\alpha\right)$. Now, a quick induction shows that the solution of (6.24) satisfies

$$T_{\boldsymbol{P},\mathrm{row}} \le (q-p+1) h_{q-p+1}(\alpha_1,\dots,\alpha_p)K,$$

and the conclusion follows. □

The following discussion will complete the proof of Proposition 6.3.2. From the expression given in Lemma 6.3.16, the definition of $\mathscr{T}$ given in (6.21), and using the fact that $n-s-1 = q-p$, we have

$$\mathscr{T} = \sum_{\substack{\boldsymbol{i}=(i_1,\dots,i_k)\\ k\le\min(q-p,p)}} \alpha_{i_1}\cdots\alpha_{i_k} T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1},\dots,\alpha_{i_k}),q-p) + \tilde{O}(h_{q-p+1}(\alpha_1,\dots,\alpha_p)n^3). \quad (6.26)$$

Using Lemma 6.3.16 for $T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1},\dots,\alpha_{i_k}),q-p)$, we obtain

$$T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1},\dots,\alpha_{i_k}),q-p) =$$
$$\tilde{O}\left(\binom{q-p}{k} h_{q-p+1-k}(\alpha_{i_1},\dots,\alpha_{i_k}) h_{q-p+1-k}(\alpha_{i_1}+1,\dots,\alpha_{i_k}+1)k(q-p)\alpha\right),$$

which can be expressed as $h_{q-p+1-k}(\alpha_{i_1},\dots,\alpha_{i_k})D(\alpha_{i_1},\dots,\alpha_{i_k},p,q)$ where

$$D(\alpha_{i_1},\dots,\alpha_{i_k},p,q) = O^{\tilde{}}\left(\binom{q-p}{k} h_{q-p+1-k}(\alpha_{i_1}+1,\dots,\alpha_{i_k}+1)k(q-p)\alpha\right).$$

We use the fact that $\binom{q-p}{k} \leq \binom{q}{p}$, for the values of k that show up in the sum in (6.26), and

$$h_{q-p+1-k}(\alpha_{i_1}+1,\dots,\alpha_{i_k}+1) \leq h_{q-p+1}(\alpha_1+1,\dots,\alpha_p+1),$$

to obtain

$$D(\alpha_{i_1},\dots,\alpha_{i_k},p,q) = O^{\tilde{}}\left(\binom{q}{p} h_{q-p+1}(\alpha_1+1,\dots,\alpha_p+1)p(q-p)\alpha\right),$$

for any sequence $\boldsymbol{i} = (i_1,\dots,i_k)$. This implies that

$$T_{\boldsymbol{P},\mathrm{row}}((\alpha_{i_1},\dots,\alpha_{i_k}),q-p) = O^{\tilde{}}\left(h_{q-p+1-k}(\alpha_{i_1},\dots,\alpha_{i_k})\binom{q}{p} h_{q-p+1}(\alpha_1+1,\dots,\alpha_p+1)p(q-p)\alpha\right),$$

Therefore,

$$\mathscr{T} = \left(\sum_{\substack{\boldsymbol{i}=(i_1,\dots,i_k)\\ k\leq \min(q-p,p)}} \alpha_{i_1}\cdots\alpha_{i_\kappa} h_{q-p+1-k}(\alpha_{i_1},\dots,\alpha_{i_k})\right)\times O^{\tilde{}}\left(\binom{q}{p} h_{q-p+1}(\alpha_1+1,\dots,\alpha_p+1)p(q-p)\alpha\right) + O^{\tilde{}}(h_{q-p+1}(\alpha_1,\dots,\alpha_p)n^3).$$

Furthermore, since

$$\sum_{\substack{\boldsymbol{i}=(i_1,\dots,i_k)\\ k\leq \min(q-p,p)}} \alpha_{i_1}\cdots\alpha_{i_\kappa} h_{q-p+1-k}(\alpha_{i_1},\dots,\alpha_{i_k}) \leq h_{q-p+1}(\alpha_1,\dots,\alpha_p),$$

we can deduce that

$$\gamma_1\cdots\gamma_s\mathscr{T} = O^{\tilde{}}\left(c'\binom{q}{p} e'p(q-p)\alpha + c'n^3\right).$$

Injecting the above value in the runtime analysis (6.22) and using the fact that terms such as $q-p$ or n^3 are poly-logarithmic in e', we have the first term $\gamma_1\cdots\gamma_s\mathscr{T}$ in (6.22) is bounded above by the second one in (6.22). Thus, the runtime of the RowDegree_simple algorithm is

$$T_{\mathrm{row}}(\sigma,\boldsymbol{\gamma},\boldsymbol{\alpha},q) = O^{\tilde{}}\left(\binom{q}{p} c'e'(\sigma+p\alpha+\gamma)\right). \tag{6.27}$$

This finishes our proof of Proposition 6.3.2.

Proof of Proposition 6.3.1. Finally, we design an algorithm called RowDegree, which differs from RowDegree_simple only at the last step, where Algorithm Homotopy is called instead of Homotopy_simple. One applies Proposition 5.2.11, which yields a runtime of $O^{\sim}(c'^5mn^2 + c'(e' + c'^5)(\sigma' + n^3))$ operations in $\mathbb{K}$. Using the facts that $\sigma' = \sigma + O(\binom{q}{p}n^3 + n^2p\alpha + n^2\gamma)$, and that n is in $O^{\sim}(e')$, we rewrite this as $O^{\sim}(c'^5mn^2 + c'(e' + c'^5)\binom{q}{p}(\sigma + p\alpha + \gamma))$. Using again the inequality $m \leq n + \binom{q}{p} \leq n\binom{q}{p}$ gives $c'^5mn^2 \leq (e' + c'^5)\binom{q}{p}n^3$. Then the runtime of Homotopy is thus

$$O^{\sim}\left(c'(e' + c'^5)\binom{q}{p}(\sigma + p\alpha + \gamma)\right)$$

operations in $\mathbb{K}$.

The costs of all other steps are the same as those is RowDegree_simple, and the analysis above shows that can be neglected. As a result, the bound given above holds for the whole RowDegree algorithm. This ends our proof for Proposition 6.3.1

Algorithm 10 RowDegree(Γ)

Input: a straight-line program Γ of length σ that computes

- $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with $\deg(f_{i,j}) \leq \delta_j$ for all j and $p \leq q$
- polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$, with $n = q - p + s + 1$

Output: a zero-dimensional parametrization of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

1. run steps 1. to 3. of RowDegree_simple(Γ) to have Γ' and $\mathscr{R}_0$
2. return Homotopy($\Gamma', \mathscr{R}_0, e'$)

cost: $O^{\sim}(c'^5mn^2 + c'(e' + c'^5)(\sigma' + n^3))$

Chapter 7

Determinantal ideals in sparse domains and application in weighted polynomial rings

Let $\mathbb{K}$ be a field of characteristic zero with $\overline{\mathbb{K}}$ its algebraic closure. Given a sequence of sparse polynomials $\boldsymbol{G} = (g_1, \ldots, g_s) \in \mathbb{K}[x_1, \ldots, x_n]^s$ and a polynomial matrix $\boldsymbol{F} = [f_{i,j}] \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$, with its entries being sparse, such that $p \leq q$ and $n = q - p + s + 1$, we are interested in determining the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$, the algebraic set of points in $\overline{\mathbb{K}}$ at which all polynomials in $\boldsymbol{G}$ and all p-minors of $\boldsymbol{F}$ vanish. We design homotopy algorithms for computing the isolated points in $V_p(\boldsymbol{F}, \boldsymbol{G})$ which take advantage of the determinantal structure of the system defining $V_p(\boldsymbol{F}, \boldsymbol{G})$ and its sparsity. The complexity of our algorithms depends on the support of the polynomials in $\boldsymbol{G}$ and $\boldsymbol{F}$. In addition we use these homotopy algorithms to compute the isolated points of $\boldsymbol{V}_p(\boldsymbol{F}, \boldsymbol{G})$ when all entries of $\boldsymbol{F}$ and elements of $\boldsymbol{G}$ lies in weighted domains.

7.1 The column-support homotopy

Reusing notations from previous chapters, we are interested in describing the set

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = \{\boldsymbol{x} \in \overline{\mathbb{K}}^n \mid \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p \text{ and } g_1(\boldsymbol{x}) = \cdots = g_s(\boldsymbol{x}) = 0\},$$

which is an algebraic set defined by $V_p(\boldsymbol{F}, \boldsymbol{G}) = V(I_p(\boldsymbol{F}, \boldsymbol{G}))$, where

$$I_p(\boldsymbol{F}, \boldsymbol{G}) = \langle g_1, \ldots, g_s \rangle + \langle M_p(\boldsymbol{F}) \rangle,$$

the ideal generated by $\boldsymbol{G}$ and $M_p(\boldsymbol{F})$, the set of p-minors of $\boldsymbol{F}$. We first discuss some properties of sequences of generic sparse equations.

7.1.1 Generic sparse polynomials

In the later of the chapter, we will define a family of possible start systems, and we show that a generic member of this family allows us to carry out the procedure successfully. In this subsection, we give the definition of generic sparse polynomials and some properties of the systems defined by these polynomials.

Consider finite sets $\mathcal{A}_1, \ldots, \mathcal{A}_\ell$ in $\mathbb{N}^n$, with δ_i denoting the cardinality of $\mathcal{A}_i$ for all i. For each i, we let $\mathcal{M}_i = (m_{i,1}, \ldots, m_{i,\delta_i})$ be the corresponding set of monomials in $x_1, \ldots, x_n$. This allows us to define the "generic polynomials" $\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell$ supported on $\mathcal{A}_1, \ldots, \mathcal{A}_\ell$ by

$$\mathfrak{f}_i = \sum_{k=1}^{\delta_i} \mathfrak{c}_{i,k} m_{i,k} \in \mathbb{K}[\mathfrak{C}][x_1, \ldots, x_n],$$

where $\mathfrak{C} = (\mathfrak{c}_{i,k})_{1 \le i \le \ell, 1 \le k \le \delta_i}$ are new indeterminates. The total number of indeterminates $\mathfrak{C}$ is $L = \sum_{i=1}^{\ell} \delta_i$.

Identifying $\overline{\mathbb{K}}^L$ with $\overline{\mathbb{K}}^{\delta_1} \times \cdots \times \overline{\mathbb{K}}^{\delta_\ell}$, we can view any element $\rho \in \overline{\mathbb{K}}^L$ as a vector of coefficients, first for $\mathfrak{f}_1$, then for $\mathfrak{f}_2$, etc. Then, for such a ρ, we will denote by Θ_ρ the mapping

$$\begin{array}{rcl} \mathbb{K}[\mathfrak{C}][x_1, \ldots, x_n] & \to & \overline{\mathbb{K}}[x_1, \ldots, x_n] \\ \displaystyle\sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} g_{\boldsymbol{\alpha}}(\mathfrak{C}) x_1^{\alpha_1} \cdots x_n^{\alpha_n} & \mapsto & \displaystyle\sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} g_{\boldsymbol{\alpha}}(\rho) x_1^{\alpha_1} \cdots x_n^{\alpha_n}; \end{array}$$

the notation carries over to vectors or matrices of polynomials.

Proposition 7.1.1. *Suppose that for $i = 1, \ldots, \ell$, $\mathcal{A}_i$ contains the origin $\mathbf{0} \in \mathbb{N}^n$. Then there exists a non-empty Zariski open set $\Omega_1 \subset \overline{\mathbb{K}}^L$ such that for $\rho \in \Omega_1$, we have the following:*

(i) *if $\ell \le n$, $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$ generates a radical ideal, whose zero-set in $\overline{\mathbb{K}}^n$ is either empty or smooth and $(n-\ell)$-equidimensional;*

(ii) *if $\ell > n$, the zero-set of $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$ in $\overline{\mathbb{K}}^n$ is empty.*

Proof. Without loss of generality, assume that $m_{i,\delta_i} = 1$ holds for all i. Consider the map

$$\begin{aligned} \Phi : \overline{\mathbb{K}}^n \times \overline{\mathbb{K}}^L &\to \overline{\mathbb{K}}^\ell \\ (\boldsymbol{x}, \rho) &\mapsto \Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)(\boldsymbol{x}). \end{aligned}$$

We first claim that $\mathbf{0}$ is a regular value of Φ, that is, the Jacobian matrix of this sequence of polynomials has full rank at all points of the zero-set of $(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$.

Indeed, since $m_{i,\delta_i} = 1$, the columns corresponding to partial derivatives with respect to $\mathfrak{f}_i$ contain an $\ell \times \ell$ identity matrix. As a result, by Thom's weak transversality theorem

(see the algebraic version in e.g. [158]), there exists a non-empty Zariski open set $\Omega_1 \subset \overline{\mathbb{K}}^L$ such that for ρ in Ω_1, $\mathbf{0}$ is a regular value of the specialized mapping

$$\Phi_\rho : \boldsymbol{x} \in \overline{\mathbb{K}}^n \mapsto \Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)(\boldsymbol{x}).$$

In other words, the Jacobian matrix of $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$ has rank ℓ at any zero $\boldsymbol{x} \in \overline{\mathbb{K}}^n$ of $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$.

For $\ell \leq n$, by Lemma 3.1.8, the ideal $\langle \Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell) \rangle$ is therefore radical, and its zero-set is either empty or smooth and $(n-\ell)$-equidimensional. For $\ell > n$, this means that this set is empty (since the matrix above has n columns, it cannot have rank ℓ). □

7.1.2 Setting up the systems

We first construct a polynomial matrix $\boldsymbol{L}$ in $\mathbb{K}[\boldsymbol{X}]^{p\times q}$ and polynomials $\boldsymbol{M} = (m_1, \ldots, m_s)$ in $\mathbb{K}[\boldsymbol{X}]^s$ which are used as the start matrix and start polynomials for the homotopy deformation. In order to build the polynomials $\boldsymbol{M}$, we take polynomials with the same supports at $\boldsymbol{G} = (g_1, \ldots, g_s)$ and generic coefficients, taking care to add the constant 1 to their monomial supports if it is missing. The construction of $\boldsymbol{L}$ is derived from the unions of the supports of the entries of $\boldsymbol{F}$ per columns.

For $1 \leq i \leq s$, let $\mathcal{A}_i \subset \mathbb{N}^n$ denote the support of g_i, to which we add the origin $\mathbf{0} \in \mathbb{N}^n$. For $1 \leq j \leq q$, let $\mathcal{B}_j \subset \mathbb{N}^n$ be the union of the supports of the polynomials in the j-th column of $\boldsymbol{F}$, to which we add $\mathbf{0}$ as well. For given i and j we denote by γ_i the cardinality of $\mathcal{A}_i$ and by δ_j the cardinality of $\mathcal{B}_j$, and let $(m_{i,1}, \ldots, m_{i,\gamma_i})$ and $(r_{j,1}, \ldots, r_{j,\delta_j})$ denote the monomials in $(x_1, \ldots, x_n)$ supported by $\mathcal{A}_i$ and $\mathcal{B}_j$, respectively. We can then define the "generic" polynomials supported on $\mathcal{A}_1, \ldots, \mathcal{A}_s$ and $\mathcal{B}_1, \ldots, \mathcal{B}_q$.

For $i = 1, \ldots, s$ and $j = 1, \ldots, q$, we define

$$\mathfrak{m}_i = \sum_{k=1}^{\gamma_i} \mathfrak{d}_{i,k} m_{i,k} \qquad \text{and} \quad \mathfrak{r}_j = \sum_{k=1}^{\delta_j} \mathfrak{e}_{j,k} r_{j,k}, \tag{7.1}$$

where all $\mathfrak{d}_{i,k}$ and $\mathfrak{e}_{j,k}$ are new indeterminates. Let $\mathfrak{c}_{i,j}$, for $1 \leq i \leq p$ and $1 \leq j \leq q$, be pq additional new indeterminates so that $\mathfrak{A} = \{\mathfrak{d}_{i,k}, \mathfrak{e}_{j,k}, \mathfrak{c}_{i,j}\}$, the set of all these new indeterminates, has size

$$N = \sum_{i=1}^{s} \gamma_i + \sum_{i=1}^{q} \delta_i + pq.$$

We then define the matrix

$$\mathfrak{L} = \begin{pmatrix} \mathfrak{c}_{1,1}\,\mathfrak{r}_1 & \mathfrak{c}_{1,2}\,\mathfrak{r}_2 & \ldots & \mathfrak{c}_{1,q}\,\mathfrak{r}_q \\ \vdots & \vdots & & \vdots \\ \mathfrak{c}_{p,1}\,\mathfrak{r}_1 & \mathfrak{c}_{p,2}\,\mathfrak{r}_2 & \ldots & \mathfrak{c}_{p,q}\,\mathfrak{r}_q \end{pmatrix} \in \mathbb{K}[\mathfrak{A}][x_1, \ldots, x_n]^{p\times q}. \tag{7.2}$$

As before, for ρ in $\overline{\mathbb{K}}^N$ and any polynomial $\mathfrak{f}$ having coefficients in $\overline{\mathbb{K}}[\mathfrak{A}]$, $\Theta_\rho(\mathfrak{f})$ is the polynomial with coefficients in $\overline{\mathbb{K}}$ obtained through evaluation of the indeterminates $\mathfrak{A}$ at ρ; the notation carries over to polynomial matrices as well.

We will use $\mathfrak{L}$ and $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_s)$ to construct our start system, by assigning random values to all indeterminates in $\mathfrak{A}$. Thus, we let t be a new indeterminate and we denote by $\mathfrak{B} = (\mathfrak{b}_1, \ldots, \mathfrak{b}_s, \ldots, \mathfrak{b}_m)$ the polynomials in $\mathbb{K}[\mathfrak{A}][t, x_1, \ldots, x_n]$ obtained by considering the equations

- $(\mathfrak{b}_1, \ldots, \mathfrak{b}_s) = (1-t) \cdot \mathfrak{M} + t \cdot \boldsymbol{G}$, and
- $(\mathfrak{b}_{s+1}, \ldots, \mathfrak{b}_m)$ are the p-minors of $(1-t) \cdot \mathfrak{L} + t \cdot \boldsymbol{F}$, following the order $\succ$.

Having in mind to apply Propositions 5.2.11, we need to verify that all required assumptions are satisfied. For any ρ in $\overline{\mathbb{K}}^N$, Proposition 5.3.1 implies that the determinantal ideal $\langle \Theta_\rho(\boldsymbol{B}) \rangle \subset \mathbb{K}[t, \boldsymbol{X}]$ satisfy properties B_1 and B_2. It remains to prove that, for a generic choice of ρ in $\overline{\mathbb{K}}^N$, our systems satisfy C_1 and C_2. Our goal in the next subsections, from Subsection 7.1.3 to Subsection 7.1.5, is to establish the following result.

Proposition 7.1.2. *There exists a non-empty Zariski open subset Ω of $\overline{\mathbb{K}}^N$ such that for ρ in Ω, the system $\boldsymbol{B} := \Theta_\rho(\mathfrak{B})$ satisfies the properties C_1 and C_2.*

In other words, we will prove that, for such a choice of ρ, the ideal generated by $\boldsymbol{B}_{t=0}$ in $\overline{\mathbb{K}}[x_1, \ldots, x_n]$ is radical and zero-dimensional and that the solutions of $\boldsymbol{B}$ in $\overline{\mathbb{K}}\langle\langle t \rangle\rangle^n$ are bounded. Consequently, the number of isolated solutions of the system we want to solve (counting multiplicities) is bounded above by the number of solutions of a generic start system $\Theta_\rho(\mathfrak{B})_{t=0}$. In Subsection 7.1.6, we will establish precisely the value of this number.

7.1.3 Radical and zero-dimensional properties of $\langle \boldsymbol{A} \rangle$

In this subsection, we prove that for a generic choice of ρ in $\overline{\mathbb{K}}^N$, if we write $\boldsymbol{B} := \Theta_\rho(\mathfrak{B})$ in $\mathbb{K}[t, \boldsymbol{X}]$, where $\boldsymbol{X} = (x_1, \ldots, x_n)$, the ideal generated by $\boldsymbol{B}_{t=0}$ in $\mathbb{K}[\boldsymbol{X}]$ is radical and zero-dimensional. The equations $\boldsymbol{B}_{t=0} = \boldsymbol{A}$ that we are considering given by $(a_1, \ldots, a_s) = \Theta_\rho(\mathfrak{m}_1, \ldots, \mathfrak{m}_s)$ and $(a_{s+1}, \ldots, a_m)$ are the p-minors of $\Theta_\rho(\mathfrak{L})$, following the order $\succ$.

Proposition 7.1.3. *There exists a non-empty Zariski open set $\Omega_1 \subset \overline{\mathbb{K}}^N$ such that for ρ in Ω_1, writing $\boldsymbol{B} := \Theta_\rho(\mathfrak{B})$, the ideal generated by $\boldsymbol{B}_{t=0}$ in $\overline{\mathbb{K}}[x_1, \ldots, x_n]$ is radical of dimension zero.*

The rest of this subsection is devoted for a proof of this proposition. First note that any p-minor of $\mathfrak{L}$ has the form $\mathfrak{C}_{i_1,\ldots,i_p} \mathfrak{m}_{i_1} \cdots \mathfrak{m}_{i_p}$, for some choice of columns $i_1, \ldots, i_p$, where

$\mathfrak{C}_{i_1,\ldots,i_p}$ is the determinant

$$\mathfrak{C}_{i_1,\ldots,i_p} = \begin{vmatrix} \mathfrak{c}_{1,i_1} & \mathfrak{c}_{1,i_2} & \cdots & \mathfrak{c}_{1,i_p} \\ \vdots & \vdots & & \vdots \\ \mathfrak{c}_{p,i_1} & \mathfrak{c}_{p,i_2} & \cdots & \mathfrak{c}_{p,i_p} \end{vmatrix} \in \mathbb{K}[\mathfrak{A}].$$

Our first constraint on ρ is thus that $\Theta_\rho(\mathfrak{C}_{i_1,\ldots,i_p})$ is non-zero in $\overline{\mathbb{K}}$, for all $\{i_1,\ldots,i_p\}$. In this case, a point $\boldsymbol{\alpha}$ in $\overline{\mathbb{K}}^n$ cancels all the p-minors of $\Theta_\rho(\mathfrak{L})$ if and only if it cancels all products $\Theta_\rho(\mathfrak{r}_{i_1})\cdots\Theta_\rho(\mathfrak{r}_{i_p})$. This is the case if and only if there exists $\boldsymbol{i} = \{i_1,\ldots,i_{q-p+1}\} \subset \{1,\ldots,q\}$ such that

$$\Theta_\rho(\mathfrak{r}_{i_1})(\boldsymbol{\alpha}) = \cdots = \Theta_\rho(\mathfrak{r}_{i_{q-p+1}})(\boldsymbol{\alpha}) = 0$$

(similar to what we have seen in Subsection 6.2 for column-degree homotopy algorithms). Since we assume $n = q-p+s+1$, we can rewrite $q-p+1$ as $n-s$.

Then, for a subset $\boldsymbol{i} = \{i_1,\ldots,i_{n-s}\} \subset \{1,\ldots,q\}$, consider the polynomials $\mathfrak{R}_{\boldsymbol{i}} = (\mathfrak{r}_{i_1},\ldots,\mathfrak{r}_{i_{n-s}})$. Proposition 7.1.1(i) implies that there exists a non-empty Zariski open set $\mathscr{O}_{\boldsymbol{i}} \subset \overline{\mathbb{K}}^N$ such that for ρ in $\mathscr{O}_{\boldsymbol{i}}$, the ideal generated by $\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}},\mathfrak{M})$ is radical of dimension zero. In addition, for subsets $\boldsymbol{i}'$ and $\boldsymbol{i}$ of $\{1,\ldots,q\}$ of cardinalities $n-s$ such that $\boldsymbol{i} \neq \boldsymbol{i}'$, the system defined by $\mathfrak{R}_{\boldsymbol{i}\cup\boldsymbol{i}'}$ and $\mathfrak{M}$ contains at least $n+1$ polynomials in $\mathbb{K}[\mathfrak{A}][x_1,\ldots,x_n]$. By using Proposition 7.1.1(ii), there exists a non-empty Zariski open set $\mathscr{O}_{\boldsymbol{i}\cup\boldsymbol{i}'} \subset \overline{\mathbb{K}}^N$ such that for ρ in $\mathscr{O}_{\boldsymbol{i}\cup\boldsymbol{i}'}$, the system $\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}\cup\boldsymbol{i}'},\mathfrak{M})$ has no solutions in $\overline{\mathbb{K}}^n$.

Taking the intersection of these $\mathscr{O}_{\boldsymbol{i}}$ and $\mathscr{O}_{\boldsymbol{i}\cup\boldsymbol{i}'}$ (which are finite in number), together with the condition that the determinants $\Theta_\rho(\mathfrak{C}_{i_1,\ldots,i_p})$ do not vanish, defines a non-empty Zariski open $\Omega_1 \subset \overline{\mathbb{K}}^N$. Thus, for ρ in Ω_1, the sets $V(\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}},\mathfrak{M}))$, for any subset $\boldsymbol{i}$ of $\{1,\ldots,q\}$ of cardinality $n-s$, are finite and pairwise disjoint, and their union is $V(\boldsymbol{B}_{t=0})$. In particular, the latter set is finite, which gives us the second half of our claim.

Take ρ in Ω_1 and $\boldsymbol{\alpha}$ in $V(\boldsymbol{B}_{t=0})$. We now prove that the ideal generated by $\boldsymbol{B}_{t=0}$, that is, by the p-minors of $\Theta_\rho(\mathfrak{R})$ and $\Theta_\rho(\mathfrak{m}_1,\ldots,\mathfrak{m}_s)$, has multiplicity one at $\boldsymbol{\alpha}$. This implies that the ideal $\langle \boldsymbol{B}_{t=0}\rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical. For this, we will use the fact that $\boldsymbol{\alpha}$ is the root of the system $\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}},\mathfrak{M})$, for a unique subset $\boldsymbol{i} = (i_1,\ldots,i_{n-s})$ of $\{1,\ldots,q\}$ of cardinality $n-s$, and that $\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}},\mathfrak{M})$ has multiplicity one at $\boldsymbol{\alpha}$.

Recall that $n = q-p+s+1$, so that $n-s = q-(p-1)$. Hence, there are exactly $p-1$ columns indices by $\boldsymbol{j} = (j_1,\ldots,j_{p-1})$ of $\mathfrak{L}$ such that $j_k \notin \boldsymbol{i} = (i_1,\ldots,i_{n-s})$ for all $k = 1,\ldots,p-1$. For $i \in \boldsymbol{i}$, the equations $\Theta_\rho(\mathfrak{C}_{j_1,\ldots,j_{p-1},i}\mathfrak{r}_{j_1}\cdots\mathfrak{r}_{j_{p-1}}\mathfrak{m}_i)$ appears among the generators of $\boldsymbol{B}_{t=0}$. In the local ring at $\boldsymbol{\alpha}$, we can divide by the non-zero quantity $\Theta_\rho(\mathfrak{C}_{j_1,\ldots,j_{p-1},i}\mathfrak{r}_{j_1}\cdots\mathfrak{r}_{j_{p-1}})(\boldsymbol{\alpha})$. This implies that locally at $\boldsymbol{\alpha}$, $\boldsymbol{B}_{t=0}$ is generated by the polynomials $\Theta_\rho(\mathfrak{r}_{i_1}),\ldots,\Theta_\rho(\mathfrak{r}_{i_{n-s}})$ and $\Theta_\rho(\mathfrak{M})$. The conclusion follows.

7.1.4 The associated Lagrange system

To establish the boundedness property, i.e., the property C_2, since $\mathfrak{B}$ is over-determined, it will be convenient to introduce new variables $\boldsymbol{\ell} = (\ell_1,\ldots,\ell_p)$ and to work with the

Lagrange system consist of $s+q+1$ equations defined by

$$(1-t)\mathfrak{M}+t\boldsymbol{G} \;=\; [\ell_1 \;\cdots\; \ell_p]((1-t)\mathfrak{M}+t\boldsymbol{F}) \;=\; \mathfrak{t}_1\ell_1+\cdots+\mathfrak{t}_p\ell_p-1=0, \tag{7.3}$$

where $\mathfrak{t}=(\mathfrak{t}_1,\dots,\mathfrak{t}_p)$ are new indeterminate coefficients. Recall that $n=q-p+s+1$, so $s+q+1=n+p$; we will write these equations as $\mathfrak{H}=(\mathfrak{H}_1,\dots,\mathfrak{H}_{n+p})$.

There are now $N+p$ parameters in these equations, with elements of the parameter space $\overline{\mathbb{K}}^{N+p}$ written as $\sigma=(\rho,\kappa)$, with ρ in $\overline{\mathbb{K}}^N$ and κ in $\overline{\mathbb{K}}^p$. For σ in $\overline{\mathbb{K}}^{N+p}$ and $\mathfrak{f}$ a polynomial with coefficients in $\mathbb{K}[\mathfrak{A},\mathfrak{t}]$, we write as usual $\Theta_\sigma(\mathfrak{f})$ for the polynomial whose coefficients are obtained from those of f, with $\mathfrak{A}$ evaluated at ρ and $\mathfrak{t}$ evaluated at κ. As before, the notation carries over to vectors or matrices of polynomials as well.

For $1\le i\le n+p$, $\mathfrak{H}_i$ can be decomposed as $\mathfrak{H}_i=\mu_i+t\mathfrak{h}_i$ with both μ_i and $\mathfrak{h}_i$ in $\mathbb{K}[\mathfrak{A},\mathfrak{t}][\boldsymbol{x},\boldsymbol{\ell}]$. In particular, note that the polynomials $\boldsymbol{\mu}=(\mu_1,\dots,\mu_{n+p})$ form the Lagrange system

$$\mathfrak{m}_1=\cdots=\mathfrak{m}_s \;=\; [\ell_1 \;\cdots\; \ell_p]\mathfrak{L} \;=\; \mathfrak{t}_1\ell_1+\cdots+\mathfrak{t}_p\ell_p+1=0$$

in $\mathbb{K}[\mathfrak{A},\mathfrak{t}][\boldsymbol{x},\boldsymbol{\ell}]$, so for $i=1,\dots,q$, the polynomial μ_{s+i} is $(\mathfrak{c}_{1,i}\ell_1+\cdots+\mathfrak{c}_{p,i}\ell_p)\mathfrak{r}_i$.

In what follows, we discuss properties of the polynomials $\Theta_\sigma(\boldsymbol{\mu})$ and their initial forms $\mathrm{init}_{\boldsymbol{e}}(\Theta_\sigma(\boldsymbol{\mu}))$, for $\boldsymbol{e}$ in $\mathbb{Q}^{n+p}$. Recall that the definition of initial forms can be found in Definition 3.3.4. Our first claim is the following and the proof is straightforward.

Lemma 7.1.4. *For σ in $(\overline{\mathbb{K}}-\{0\})^{N+p}$ and $\boldsymbol{e}$ in $\mathbb{Q}^{n+p}$, $\mathrm{init}_{\boldsymbol{e}}(\Theta_\sigma(\boldsymbol{\mu}))=\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\mu}))$.*

The second proposition uses the specific shape of the equations $\mathfrak{H}$ to derive information about their roots.

Proposition 7.1.5. *Let $\boldsymbol{\phi}=(t^{e_1}c_1+\cdots,\dots,t^{e_{n+p}}c_{n+p}+\cdots)$ be in $\overline{\mathbb{K}}\langle\langle t\rangle\rangle^{n+p}$ with, for all $i=1,\dots,n+p$, e_i in $\mathbb{Q}$ and c_i in $\overline{\mathbb{K}}-\{0\}$.*

Then for σ in $(\overline{\mathbb{K}}-\{0\})^{N+p}$, we have the following: if $\boldsymbol{\phi}$ cancels $\Theta_\sigma(\mathfrak{H})$, then $\boldsymbol{c}=(c_1,\dots,c_{n+p})$ cancels $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\mu}))$, with $\boldsymbol{e}=(e_1,\dots,e_{n+p})$.

Proof. For $i=1,\dots,s$, we have $\mathfrak{H}_i=\mathfrak{m}_i+t(g_i-\mathfrak{m}_i)$, so $\mu_i=\mathfrak{m}_i$ and $\mathfrak{h}_i=g_i-\mathfrak{m}_i$. Thus by construction, the monomial support of $\mathfrak{h}_i$ is the same as that of $\mathfrak{m}_i$. This means that for any term $kx_1^{u_1}\cdots\ell_p^{u_{n+p}}$ in $\mathfrak{h}_i$, with k in $\mathbb{K}[\mathfrak{A}]$, there exists a term $k'x_1^{u_1}\cdots\ell_p^{u_{n+p}}$ in μ_i, where k' is one of the indeterminates $\mathfrak{d}_{i,j}$.

Take σ as in the statement of the proposition, and write $a=\Theta_\sigma(\mathfrak{H}_i)$, $b=\Theta_\sigma(\mu_i)$ and $c=\Theta_\sigma(\mathfrak{h}_i)$, so that $b(\boldsymbol{\phi})+tc(\boldsymbol{\phi})=0$. Using our assumption on σ, we deduce that for any term of the form $kt\phi_1^{u_1}\cdots\phi_{n+p}^{u_{n+p}}$ appearing in $tc(\boldsymbol{\phi})$, there is a term $k'\phi_1^{u_1}\cdots\phi_{n+p}^{u_{n+p}}$ appearing in $b(\boldsymbol{\phi})$, with non-zero coefficient k'. In particular, all terms of smallest valuation in $a(\boldsymbol{\phi})$ appear in $b(\boldsymbol{\phi})$, and must add up to zero. Taking their first coefficient, this implies that $\boldsymbol{c}$ cancels $\mathrm{init}_{\boldsymbol{e}}(b)$.

The proof for the polynomials $\mathfrak{H}_{s+1}, \ldots, \mathfrak{H}_{s+q}$ and $\mu_{s+1}, \ldots, \mu_{s+q}$ is similar, taking into account that $\mu_{s+i} = (\mathfrak{c}_{1,i}\ell_1 + \cdots + \mathfrak{c}_{p,i}\ell_p)\mathfrak{r}_i$. Indeed, for $i = 1, \ldots, q$, the monomial support of $\mathfrak{h}_{s+i}$ is the same as that of μ_{s+i}. Then, if we define a, b, c as above, our assumption that no entry of σ vanishes implies again that all terms of smallest valuation in $a(\boldsymbol{\phi})$ appear in $b(\boldsymbol{\phi})$, and so add up to zero. Finally, for $\mathfrak{H}_{s+q+1} = \mathfrak{H}_{n+p}$, we have that $\mathfrak{h}_{n+p} = 0$, and the claim follows as above. □

Our last property requires a longer proof. For generic choices of σ, it constrains the possible roots of the system $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\mu}))$ introduced in the previous proposition.

Proposition 7.1.6. *There exists a non-empty Zariski open set $\Omega_2 \subset \overline{\mathbb{K}}^{N+p}$ such that for $\sigma \in \Omega_2$, the following holds for any $\boldsymbol{e}$ in $\mathbb{Q}^{n+p}$: for $j = 1, \ldots, n+p$, the system obtained by setting the j-th variable to 1 in $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\mu}))$ has no solution in $(\overline{\mathbb{K}} - \{0\})^{n+p-1}$.*

The rest of the subsection is dedicated to proving this proposition. First note that although there is an infinite number of vectors $\boldsymbol{e}$ to take into account, there is only a finite number of possible systems $\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\mu})$. Thus, in what follows, we assume $\boldsymbol{e}$ is fixed. Similarly, without loss of generality, we assume $j = 1$, so that we are setting x_1 to 1.

Thus, we call $\bar{\boldsymbol{\mu}} = (\bar{\mu}_1, \ldots, \bar{\mu}_{n+p})$ the polynomials in $\mathbb{K}[\mathfrak{A}, \mathfrak{t}][x_2, \ldots, x_n, \ell_1, \ldots, \ell_p]$ obtained by setting x_1 to 1 in $\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\mu})$. We will prove that for a generic σ in $\overline{\mathbb{K}}^{N+p}$, the system $\Theta_\sigma(\bar{\boldsymbol{\mu}}) \subset \overline{\mathbb{K}}[x_2, \ldots, x_n, \ell_1, \ldots, \ell_p]$ has no solution in $(\overline{\mathbb{K}} - \{0\})^{n+p-1}$. This system is indeed the one mentioned in the statement of the proposition, since Θ_σ and variable evaluation commute by Lemma 7.1.4.

For $i = 1, \ldots, n+p$, denote by $\mathfrak{S}_i$ the subset of $(\mathfrak{A}, \mathfrak{t})$ consisting of those indeterminates that appear in the coefficients of μ_i, so it also contains those that appear in the coefficients of $\bar{\mu}_i$. With this convention, the sets $\mathfrak{S}_i$ are pairwise disjoint, and $(\mathfrak{S}_1, \ldots, \mathfrak{S}_{n+p})$ is the set of all indeterminate coefficients $(\mathfrak{A}, \mathfrak{t})$ that appear in $\boldsymbol{\mu}$. For all i, we let t_i be the cardinality of $\mathfrak{S}_i$, and we will write the elements of $\overline{\mathbb{K}}^{t_i}$ as r_i, so that a vector $\sigma \in \overline{\mathbb{K}}^{N+p}$ can be decomposed as $\sigma = (r_1, \ldots, r_{n+p})$. Given $(r_1, \ldots, r_i)$ in $\overline{\mathbb{K}}^{t_1+\cdots+t_i}$, $\Theta_{(r_1,\ldots,r_i)}$ denotes as usual the mapping that evaluates the $t_1+\cdots+t_i$ indeterminates $\mathfrak{S}_1, \ldots, \mathfrak{S}_i$ at $(r_1, \ldots, r_i)$. The key property we will use below is the following.

Lemma 7.1.7. *For any $\boldsymbol{\alpha}$ in $(\overline{\mathbb{K}} - \{0\})^{n+p-1}$, the polynomial $\gamma \in \overline{\mathbb{K}}[\mathfrak{S}_i]$ obtained by evaluating $x_2, \ldots, x_n, \ell_1, \ldots, \ell_p$ at the coordinates of $\boldsymbol{\alpha}$ in $\bar{\mu}_i$ is non-zero.*

Proof. For $i = 1, \ldots, s$ and $i = n+p$, the coefficients of $\bar{\mu}_i$ are sums of elements of $\mathfrak{S}_i$, no element in $\mathfrak{S}_i$ appears in two such coefficients, and all coordinates of $\boldsymbol{\alpha}$ are non-zero; so our claim holds.

For $i = s+1, \ldots, n+p-1$, since μ_i is $(\mathfrak{c}_{1,i-s}\ell_1 + \cdots + \mathfrak{c}_{p,i-s}\ell_p)\mathfrak{r}_{i-s}$, its initial form $\mathrm{init}_{\boldsymbol{e}}(\mu_i)$ is the product

$$\mathrm{init}_{\boldsymbol{e}}(\mu_i) = \mathrm{init}_{\boldsymbol{e}}(\mathfrak{c}_{1,i-s}\ell_1 + \cdots + \mathfrak{c}_{p,i-s}\ell_p)\,\mathrm{init}_{\boldsymbol{e}}(\mathfrak{r}_{i-s}).$$

By setting x_1 to 1, we deduce that $\bar{\mu}_i$ factors as $\bar{\mu}_i = f_i g_i$, where the coefficients of both f_i and g_i are sums of elements of $\mathfrak{S}_i$, and no element in $\mathfrak{S}_i$ appears in two such coefficients. Thus, the evaluations of f_i and g_i at $\boldsymbol{\alpha}$ are non-zero, so the same holds for $\bar{\mu}_i$. □

To describe algebraic sets in the torus $(\overline{\mathbb{K}} - \{0\})^{n+p-1}$, we work in $\overline{\mathbb{K}}^{n+p}$, using a new indeterminate y and taking into account the relation $x_2 \cdots x_n \ell_1 \cdots \ell_p y = 1$. Then, we will prove the following property.

Lemma 7.1.8. *For a generic choice of $(r_1, \ldots, r_i)$ in $\overline{\mathbb{K}}^{t_1+\cdots+t_i}$ (in the Zariski sense), the zero-set of $\Theta_{(r_1,\ldots,r_i)}(\bar{\mu}_1, \ldots, \bar{\mu}_i)$ and $x_2 \cdots x_n \ell_1 \cdots \ell_p y - 1$ has dimension at most $n+p-1-i$ in $\overline{\mathbb{K}}^{n+p}$.*

Proof. The proof is by induction on i. The conclusion is trivial for $i = 0$. Let us assume that our claim holds for $i-1$, for some index $i \geq 1$, and prove that it also holds at index i. We proceed by contradiction, assuming our claim does not hold. In this case, the vectors $r_1, \ldots, r_i$ for which the zero-set of $\Theta_{(r_1,\ldots,r_i)}(\bar{\mu}_1, \ldots, \bar{\mu}_i)$ and $x_2 \cdots x_n \ell_1 \cdots \ell_p y - 1$ has dimension at most $n + p - 1 - i$ in $\overline{\mathbb{K}}^{n+p}$ are contained in a hypersurface of the parameter space $\overline{\mathbb{K}}^{t_1+\cdots+t_i}$. Then, there exists a non-zero polynomial P in $\overline{\mathbb{K}}[\mathfrak{S}_1, \ldots, \mathfrak{S}_i]$ such that $P(r_1, \ldots, r_i) = 0$. Thus, take $(r_1, \ldots, r_{i-1})$ in $\overline{\mathbb{K}}^{t_1+\cdots+t_{i-1}}$ such that

- $P(r_1, \ldots, r_{i-1}, \mathfrak{S}_i)$ in $\overline{\mathbb{K}}[\mathfrak{S}_i]$ is not identically zero;
- the zero-set V of $\Theta_{(r_1,\ldots,r_{i-1})}(\bar{\mu}_1, \ldots, \bar{\mu}_{i-1})$ and $x_2 \cdots x_n \ell_1 \cdots \ell_p y - 1$ has dimension at most $n + p - i$ in $\overline{\mathbb{K}}^{n+p}$ (this is possible by the induction assumption). By Krull's theorem, all its irreducible components have dimension exactly $n + p - i$.

The first condition implies that for a generic r_i in $\overline{\mathbb{K}}^{t_i}$, the zero-set of $\Theta_{(r_1,\ldots,r_i)}(\bar{\mu}_1, \ldots, \bar{\mu}_i)$ and $x_2 \cdots x_n \ell_1 \cdots \ell_p y - 1$ has dimension at least $n + p - i$. Equivalently, this means that intersection of V and $\Theta_{(r_1,\ldots,r_i)}(\bar{\mu}_i)$ has dimension $n + p - i$. Let us see how to derive a contradiction.

Let $V_1, \ldots, V_d$ be the irreducible components of V. Pick $\boldsymbol{\alpha}_1$ in V_1, …, $\boldsymbol{\alpha}_d$ in V_d, and let $\gamma_1, \ldots, \gamma_d$ be the polynomials in $\overline{\mathbb{K}}[\mathfrak{S}_i]$ obtained by evaluating $x_2, \ldots, x_n, \ell_1, \ldots, \ell_p$ at the coordinates of $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_d$, respectively, in $\bar{\mu}_i$. As we pointed in Lemma 7.1.7, all γ_i's are non-zero, and thus so is $\Gamma := \gamma_1 \cdots \gamma_d \in \overline{\mathbb{K}}[\mathfrak{S}_i]$. In particular, for a generic choice of r_i in $\overline{\mathbb{K}}^{t_i}$, $\Theta_{(r_1,\ldots,r_i)}(\bar{\mu}_i)$ vanishes at none of $\{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_d\}$, and so it intersects each V_i (and thus V) in dimension $n + p - i - 1$. This contradicts the previous paragraph. □

Using Lemma 7.1.8 with $i = n + p$ ends our proof for Proposition 7.1.6.

7.1.5 The boundedness property

We finally establish the property C_2 needed for our homotopy algorithm. We prove that for a generic point ρ in $\overline{\mathbb{K}}^N$, the solutions of $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$ in $\overline{\mathbb{K}}\langle\langle t\rangle\rangle^n$ are bounded.

Proposition 7.1.9. *There exists a non-empty Zariski open set $\Omega_3 \subset \overline{\mathbb{K}}^N$ such that for $\rho \in \Omega_3$, writing $\boldsymbol{B} := \Theta_\rho(\mathfrak{B})$, all points in $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}\langle\langle t\rangle\rangle^n$ are bounded.*

Proof. Let us define the set Ω_3 first. By Proposition 7.1.6, there exists a non-empty Zariski open set $\Omega_2 \subset \overline{\mathbb{K}}^{N+p}$ such that for any $\sigma = (\rho, \kappa)$ in Ω_2, the following holds: for any $\boldsymbol{e}$ in $\mathbb{Q}^{n+p}$ and any j in $\{1, \ldots, n+p\}$, the system obtained by setting the j-th variable to 1 in $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\mu}))$ has no solution in $(\overline{\mathbb{K}} - \{0\})^{n+p-1}$. We then define a non-empty Zariski open $\Omega_2' \subset \overline{\mathbb{K}}^N$ be the image of Ω_2 through the projection $\pi : \sigma = (\rho, \kappa) \mapsto \rho$. Finally, we let Ω_3 be the intersection of Ω_2' with $(\overline{\mathbb{K}} - \{0\})^N \subset \overline{\mathbb{K}}^N$.

We take ρ in Ω_3 and we need to prove that all solutions of $\Theta_\rho(\mathfrak{B})$ in $\overline{\mathbb{K}}\langle\langle t\rangle\rangle^n$ are bounded. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \overline{\mathbb{K}}\langle\langle t\rangle\rangle^n$ be such a solution. By construction, there exists a non-zero $(\lambda_1, \ldots, \lambda_p) \in \overline{\mathbb{K}}\langle\langle t\rangle\rangle^p$ such that $[\lambda_1 \ \cdots \ \lambda_p]$ is in the left nullspace of $\mathfrak{L}(\boldsymbol{\alpha})$. Let $v \in \mathbb{Q}$ be the valuation of this vector, and let $(\lambda_1', \ldots, \lambda_p') \in \overline{\mathbb{K}}^p$ be the vector of coefficients of t^v in $(\lambda_1, \ldots, \lambda_p)$, so that $(\lambda_1', \ldots, \lambda_p')$ is not identically zero. Then we take $\kappa = (\kappa_1, \ldots, \kappa_p)$ such that $\sigma = (\rho, \kappa)$ is in Ω_2 and in addition $\kappa_1 \neq 0, \ldots, \kappa_p \neq 0$ and $\kappa_1\lambda_1' + \cdots + \kappa_p\lambda_p' \neq 0$. This is possible, since all these conditions are Zariski-open. In particular, $\kappa_1\lambda_1 + \cdots + \kappa_p\lambda_p$ is non-zero. We can then define $\bar{\boldsymbol{\lambda}} = (\bar\lambda_1, \ldots, \bar\lambda_p)$ by

$$\bar\lambda_i = \lambda_i/(\kappa_1\lambda_1 + \cdots + \kappa_p\lambda_p)$$

for all $i = 1, \ldots, p$. Let us write $\boldsymbol{\phi} = (\boldsymbol{\alpha}, \bar{\boldsymbol{\lambda}})$; our goal is then to prove that $\boldsymbol{\phi}$ is bounded, since it will imply that $\boldsymbol{\alpha}$ is bounded.

By construction, the vector $\bar{\boldsymbol{\lambda}} = (\bar\lambda_1, \ldots, \bar\lambda_p)$ is still in the left nullspace of $\mathfrak{L}(\boldsymbol{\alpha})$ and satisfies $\tau_1\bar\lambda_1 + \cdots + \tau_p\bar\lambda_p - 1 = 0$. Hence, the vector $\boldsymbol{\phi}$ is in $V(\Theta_\sigma(\mathfrak{H}))$. Let us then write

$$\boldsymbol{\phi} = (t^{e_1}c_1 + \cdots, \ldots, t^{e_{n+p}}c_{n+p} + \cdots)$$

with, for all $i = 1, \ldots, n+p$, e_i in $\mathbb{Q}$ and c_i in $\overline{\mathbb{K}} - \{0\}$. Since none of the coordinates of σ vanishes, we can apply Proposition 7.1.5, and deduce that $\boldsymbol{c} = (c_1, \ldots, c_{n+p})$ cancels $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$, with $\boldsymbol{e} = (e_1, \ldots, e_{n+p})$.

Suppose then by way contradiction that some e_i is negative, that is, $\boldsymbol{\phi}$ is unbounded; without loss of generality, we can assume that $e_1 < 0$. The polynomials $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$ are weighted-homogeneous, for the weight vector $\boldsymbol{e}$. In particular, the point

$$\tilde{\boldsymbol{c}} = \left(1, \frac{c_2}{\epsilon^{e_2}}, \ldots, \frac{c_{n+p}}{\epsilon^{e_{n+p}}}\right)$$

is also a solution of these equations, where ϵ denotes any element in $\overline{\mathbb{K}}$ such that $\epsilon^{e_1} = c_1$. Note that none of the coordinates of the vector $\tilde{\boldsymbol{c}}$ vanishes. However, by construction, σ

is in Ω_2, so Proposition 7.1.6 asserts that the system obtained by setting the first variable x_1 to 1 in $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$ has no solution in $(\overline{\mathbb{K}} - \{0\})^{n+p-1}$. This is the contradiction we wanted, so we have $e_i \geq 0$ for all i, as claimed. □

At this stage, in order to finish our proof of Proposition 7.1.2, it suffices to let Ω be the intersection of Ω_1 (from Proposition 7.1.3) and Ω_3 (from the proposition above).

7.1.6 Setting up parameters

Let the polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ and $\boldsymbol{F} = [f_{i,j}]_{1 \leq i \leq p, 1 \leq j \leq q}$ be as before. To find the isolated points in $V_p(\boldsymbol{F}, \boldsymbol{G})$, we take $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$ as in the previous subsections, for a randomly chosen ρ in $\mathbb{K}^N$ and apply the Homotopy algorithm of Proposition 5.2.11.

Proposition 7.1.2 established the basic properties needed for the correctness of our homotopy algorithm. To finish the analysis, and establish a cost bound, we now give upper bounds on the parameters that appear in the runtime reported in Proposition 5.2.11, such as the size of the input, the number of solutions to our start system and on the degree of the homotopy curve; we also have to give the cost of solving the start system.

We first consider the case of arbitrary sparse polynomials, for which we state our results in terms of certain mixed volumes. In the next section, we will discuss the particular case of weighted-degree polynomials. Some quantities will be defined similarly in both cases.

As before, for $i = 1, \ldots, s$, $\mathcal{A}_i \subset \mathbb{N}^n$ denotes the support of g_i, to which we add the origin $\mathbf{0} \in \mathbb{N}^n$, and for $j = 1, \ldots, q$, $\mathcal{B}_j \subset \mathbb{N}^n$ is the union of the supports of the polynomials in the j-th column of $\boldsymbol{F}$, to which we add $\mathbf{0}$ as well. For indices i, j as above, we let γ_i, respectively δ_j, be the cardinality of $\mathcal{A}_i$, respectively $\mathcal{B}_j$. As input, in either case, we are given $\boldsymbol{G}$ and $\boldsymbol{F}$ through the list of their non-zero terms; this involves $O(\gamma)$ elements in $\mathbb{K}$, with

$$\gamma := \gamma_1 + \cdots + \gamma_s + p(\delta_1 + \cdots + \delta_q). \tag{7.4}$$

Finally, we let d be the maximum degree of all the polynomials in $\boldsymbol{G}$ and $\boldsymbol{F}$.

Number of solutions of the start system.

For ρ in the non-empty open set $\Omega \subset \overline{\mathbb{K}}^N$ defined in Proposition 7.1.2, we have seen in the proof of Proposition 7.1.3 that the solutions of the start system $\boldsymbol{B}_{t=0}$ are the disjoint union of the solutions of the systems $\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}}, \mathfrak{M})$, where for a subset $\boldsymbol{i} = \{i_1, \ldots, i_{n-s}\}$ of $\{1, \ldots, q\}$ we write $\mathfrak{R}_{\boldsymbol{i}} = (\mathfrak{r}_{i_1}, \ldots, \mathfrak{r}_{i_{n-s}})$.

For $i = 1, \ldots, s$ and $j = 1, \ldots, q$, we let $\mathcal{C}_i$ and $\mathcal{D}_j$ be the convex hulls of respectively $\mathcal{A}_i$ and $\mathcal{B}_j$. Proposition 3.3.6 then implies that, for $\boldsymbol{i}$ as above, the number of solutions of $\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}}, \mathfrak{M})$ in $\overline{\mathbb{K}}^n$ equals the mixed volume

$$\chi_{\boldsymbol{i}} := \mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_s, \mathcal{D}_{i_1}, \ldots, \mathcal{D}_{i_{n-s}}),$$

for any ρ in a certain non-empty Zariski open set $\mathscr{O}_{\mathrm{BKK}\boldsymbol{i}} \subset \overline{\mathbb{K}}^N$. We define

$$\chi := \sum_{\boldsymbol{i}=\{i_1,\ldots,i_{n-s}\}\subset\{1,\ldots,q\}} \chi_{\boldsymbol{i}} = \sum_{\boldsymbol{i}=\{i_1,\ldots,i_{n-s}\}\subset\{1,\ldots,q\}} \mathsf{MV}(\mathcal{C}_1,\ldots,\mathcal{C}_s,\mathcal{D}_{i_1},\ldots,\mathcal{D}_{i_{n-s}}), \tag{7.5}$$

and let Ω' be the intersection of Ω with the finitely many $\mathscr{O}_{\mathrm{BKK}\boldsymbol{i}}$. Then, for ρ in Ω', the start system $\boldsymbol{B}_{t=0}$ has precisely χ solutions. As we pointed out after Proposition 7.1.2, this implies that the system $\boldsymbol{B}_{t=1}$ which we want to solve admits at most χ isolated solutions, counted with multiplicities.

Solving the start system.

We also need a zero-dimensional parametrization of $V(\boldsymbol{B}_{t=0})$ for the homotopy algorithms. To do it, it is enough to find the solutions of the systems $\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}}, \mathfrak{M})$, for all sequences $\boldsymbol{i} \subset \{1,\ldots,q\}$ of the cardinality $n-s$. To solve the systems $\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}}, \mathfrak{M})$, we rely on the sparse symbolic homotopy algorithm of [110, Section 5], which is, from now on, called SparseHomotopy. This algorithm finds the solutions of a sparse system of n equations in n unknowns, with arbitrary support and generic coefficients (in the Zariski sense). This means that in addition to the constraint $\rho \in \Omega$, our choice of ρ will also have to satisfy the constraints stated in that reference.

The runtime of this algorithm depends on some combinatorial quantities (we refer to the original reference for a more extensive discussion). We need a so-called *lifting function* $\boldsymbol{\omega}_{\boldsymbol{i}}$, and the associated *fine mixed subdivision* $M_{\boldsymbol{i}}$, for the support $\mathcal{A}_1,\ldots,\mathcal{A}_s,\mathcal{B}_{i_1},\ldots,\mathcal{B}_{i_{n-s}}$ of $\mathfrak{M}$ and $\mathfrak{R}_{\boldsymbol{i}}$ [104]. We then let $w_{\boldsymbol{i}}$ be the maximum value taken by $\boldsymbol{\omega}_{\boldsymbol{i}}$ on the support, and $\vartheta_{\boldsymbol{i}}$ be the maximum norm of the (primitive, integer) normal vectors to the cells of $M_{\boldsymbol{i}}$. Then, the SparseHomotopy algorithm in [110, Theorem 6.2] compute as zero-dimensional parametrization $\mathscr{R}_{\boldsymbol{i}}$ such that $Z(\mathscr{R}_{\boldsymbol{i}}) = V(\Theta_\rho(\mathfrak{R}_{\boldsymbol{i}}, \mathfrak{M}))$ using

$$\tilde{O}(n^5\gamma\log(d)\chi_{\boldsymbol{i}}^2\vartheta_{\boldsymbol{i}}w_{\boldsymbol{i}})$$

operations in $\mathbb{K}$.

Taking the union of all these parametrizations, using for example, [158, Lemma J.3], does not introduce any added cost. Thus we obtain a randomized algorithm to compute a zero-dimensional parametrization of $V_p(\Theta_\rho(\mathfrak{R}, \mathfrak{M}))$ using

$$\tilde{O}(n^5\gamma\log(d)\chi^2\vartheta w) \tag{7.6}$$

operations in $\mathbb{K}$, where we write

$$\vartheta := \max_{\boldsymbol{i}}(\vartheta_{\boldsymbol{i}}) \text{ and } w := \max_{\boldsymbol{i}}(w_{\boldsymbol{i}}) \tag{7.7}$$

An upper bound on the degree of the homotopy curve.

Similar to what we have done in Subsection 6.2.5 and Subsection 6.3.5, it suffices to find an upper bound ϱ for the number of isolated points defined by the equations in $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$ together with a generically chosen hyperplane.

Let $h = \zeta_0 + \zeta_1 x_1 + \cdots + \zeta_n x_n + \zeta_{n+1} t$ be a linear form defining such a hyperplane, for $\zeta_i \in \mathbb{K}$. Then we can rewrite t as

$$\wp(x_1, \ldots, x_n) = -(\zeta_0 + \zeta_1 x_1 + \cdots + \zeta_n x_n)/\zeta_{n+1}.$$

The isolated points in $V(\boldsymbol{B}) \cap V(h)$ are in one-to-one correspondence with the isolated solutions of the system $\boldsymbol{B}' = (b'_1, \ldots, b'_s, b'_{s+1}, \ldots, b'_m)$, where $b'_i = (1 - \wp)m_i + \wp g_i$, for $i = 1, \ldots, s$, and $(b'_{s+1}, \ldots, b'_m)$ are the p-minors of the matrix

$$\mathbf{V}' = [v'_{i,j}] = (1 - \wp) \cdot \boldsymbol{L} + \wp \cdot \boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}.$$

Hence it is sufficient to bound the number of isolated solutions of $V(\boldsymbol{B}')$.

For $1 \leq i \leq p$ and $1 \leq j \leq q$, let $\mathcal{B}'_{i,j}$ be the support of $v'_{i,j}$. We then define $\mathcal{B}'_j = \cup_{1 \leq i \leq p} \mathcal{B}'_{i,j}$, to which we add the origin if needed, and let $\mathcal{D}'_j$ be its Newton polytope. Similarly, for $i = 1, \ldots, s$ we let $\mathcal{C}'_i$ denote the Newton polytope of the support of b'_i. Then, the discussion on the number of solutions of the target system still applies, and shows that the system $\boldsymbol{B}'$ admits at most

$$\varrho = \sum_{\{i_1, \ldots, i_{n-s}\} \subset \{1, \ldots, q\}} \mathsf{MV}(\mathcal{C}'_1, \ldots, \mathcal{C}'_s, \mathcal{D}'_{i_1}, \ldots, \mathcal{D}'_{i_{n-s}}) \tag{7.8}$$

solutions.

A straight-line program for $\boldsymbol{B}$.

To obtain such a straight-line program, we fist compute the values of all monomials supported on $\mathcal{A}_1, \ldots, \mathcal{A}_s, \mathcal{B}_1, \ldots, \mathcal{B}_q$. Then we combine these values to obtain the polynomials $(1 - t) \cdot \Theta_\rho(\mathfrak{M}) + t \cdot \boldsymbol{G}$ and the matrix $(1 - t) \cdot \Theta_\rho(\mathfrak{L}) + t \cdot \boldsymbol{F}$, and take all p-minors in this matrix.

Computing the value of a single monomial supported on $\mathcal{A}_i$, respectively $\mathcal{B}_j$, can be done through repeated squaring, using $O(n \log(d))$ operations in $\mathbb{K}$. Therefore, we can obtain the values of all monomials supported on $\mathcal{A}_1, \ldots, \mathcal{A}_s, \mathcal{B}_1, \ldots, \mathcal{B}_q$ by using a straight-line program of length $O(n\gamma \log(d))$. Besides, combining these monomials to obtain

$$(1 - t) \cdot \Theta_\rho(\mathfrak{M}) + t \cdot \boldsymbol{F} \text{ and } (1 - t) \cdot \Theta_\rho(\mathfrak{L}) + t \cdot \boldsymbol{F}$$

takes another $O(\gamma)$ operations in $\mathbb{K}$. Finally, it takes $O(p^4 \binom{q}{p})$ operations to compute all p-minors of the latter matrix using a division-free determinant algorithm. Hence, a straight-line program of length

$$\beta \in O\left(n\gamma \log(d) + p^4 \binom{q}{p}\right) \tag{7.9}$$

to compute all entries of $\boldsymbol{B}$.

7.1.7 Completing the cost analysis

The previous discussion allows us to use the Homotopy algorithm from Proposition 5.2.11. In addition to the polynomials $\boldsymbol{G}$ and matrix $\boldsymbol{F}$, we also need the combinatorial information $\boldsymbol{\omega_i}, M_{\boldsymbol{i}}$ described previously. The sum of the costs of solving the start system, and of the Homotopy algorithm is as follow.

Theorem 7.1.10. *The set $V_p(\boldsymbol{F}, \boldsymbol{G})$ admits at most χ isolated solutions, counted with multiplicities. There exists a randomized algorithm called* ColumnSupport *which takes $\boldsymbol{G}$, $\boldsymbol{F}$, all lifting functions $\boldsymbol{\omega}_i$ and subdivisions $\boldsymbol{M_i}$ as input and computes a zero-dimensional parametrization of these isolated solutions using*

$$O^{\sim}\left(n^5 \left(\gamma \log(d)\chi^2 \vartheta w + \chi(\varrho + \chi^5)\binom{q}{p}\right)\right)$$

operations in $\mathbb{K}$, where γ, χ, ϱ are as in respectively (7.4), (7.5) and (7.8), and ϑ and w as in (7.7).

7.2 The weighted column-degree homotopy

Weighted domains arise naturally many applications, for example, in determining isolated critical points of a symmetric function ϕ defined over a variety $V(f_1, \ldots, f_s)$ defined by symmetric functions f_i. In the second part of the thesis, we will see that the orbits of these critical points can be described by domains of the form $\mathbb{K}[e_{1,1}, \ldots, e_{1,\ell_1}, e_{2,1}, \ldots, e_{2,\ell_2}, \ldots, e_{r,1}, \ldots, e_{r,\ell_r}]$ with $e_{i,k}$ the k-th elementary symmetric function on ℓ_i letters. Measured in terms of these letters, each $e_{i,k}$ has naturally weighted degree k.

Polynomials in weighted domains have a natural sparse structure when compared to polynomials in classic domains. For example, a polynomial $p \in \mathbb{K}[x_1, x_2, x_3]$ having total degree bounded by 10 has 286 possible terms in a classical domain. However in a weighted domain with weights $\boldsymbol{w} = (5, 3, 2)$ there are only 19 possible terms. Such a reduction also exists when considering bounds for solutions of polynomial systems when comparing classical to weighted domains. For instance, Bézout's theorem bounds the number of isolated solutions to polynomial systems of equations by the product of their degrees. With polynomial systems lying in a weighted polynomial domain $\mathbb{K}[x_1, \ldots, x_n]$ having weights

Algorithm 11 ColumnSupport($\boldsymbol{F}, \boldsymbol{G}$)

Input: a matrix $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with $p \leq q$; and polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$, with $n = q - p + s + 1$

Output: a zero-dimensional parametrization of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

1. construct $\mathfrak{L} = [\mathfrak{c}_{i,j}\mathfrak{r}_j]_{1 \leq i \leq p, 1 \leq j \leq q} \in \mathbb{K}[\mathfrak{A}][x_1, \ldots, x_n]^{p \times q}$ as in (7.2) and $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_s)$ in $\mathbb{K}[\mathfrak{A}][x_1, \ldots, x_n]^s$ as in (7.1)
2. take $\rho \in \Omega$, define $\boldsymbol{L} = \Theta_\rho(\mathfrak{L}) = [c_{i,j}r_j]_{1 \leq i \leq p, 1 \leq j \leq q} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ and $\boldsymbol{M} = \Theta_\rho(\mathfrak{M}) = (m_1, \ldots, m_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$
3. for any subsequence $\boldsymbol{i} = (i_1, \ldots, i_{n-s})$ of $(1, \ldots, q)$
   (a) $\mathscr{R}_{0,\boldsymbol{i}} \leftarrow$ SparseHomotopy$(r_{i_1}, \ldots, r_{i_{n-s}}, m_1, \ldots, m_s)$
   cost: $O^\sim(n^5 \gamma \log(d) \chi^2 \vartheta w)$
4. combine all $(\mathscr{R}_{0,\boldsymbol{i}})_{\boldsymbol{i}}$ into a zero-dimensional parametrization $\mathscr{R}_0$
   cost: $O^\sim(\varrho\, n)$
5. construct a straight-line program Δ' that computes all polynomials $\boldsymbol{B}$
   length of Δ' is β as in (7.9)
6. return Homotopy$(\Delta', \mathscr{R}_0, \varrho)$
   cost: $O^\sim\left(\chi^5(n + \binom{q}{p})n^2 + \chi(\varrho + \chi^5)n(\beta + n^3)\right)$,

---

$\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n_{>0}$, the weighted Bézout theorem (Theorem 3.4.1) states that the number of isolated points of $V(f_1, \ldots, f_n) \subset \overline{\mathbb{K}}^n$ is bounded by

$$\delta = \frac{d_1 \cdots d_n}{w_1 \cdots w_n} \quad \text{with} \quad d_i = \operatorname{wdeg}(f_i). \tag{7.10}$$

In this section we show how our sparse homotopy algorithm also allows us to describe the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$ where $\boldsymbol{F} = [f_{i,j}] \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ and $\boldsymbol{G} = (g_1, \ldots, g_s) \in \mathbb{K}[x_1, \ldots, x_n]^s$ with $n = q - p + s + 1$, assuming bounds on the weighted degrees of all polynomials $f_{i,j}$ and g_j. Without loss of generality, we will assume that $w_1 \leq \cdots \leq w_n$, and we will let $(\gamma_1, \ldots, \gamma_s)$ be the weighted degrees of $(g_1, \ldots, g_s)$ and $(\delta_1, \ldots, \delta_q)$ be the weighted column degrees of $\boldsymbol{F}$.

7.2.1 Setting up the systems

We construct the start matrix $\boldsymbol{L} \in \mathbb{K}[\boldsymbol{X}]^{p \times q}$ and start polynomials $\boldsymbol{M} = (m_1, \ldots, m_s)$ in $\mathbb{K}[\boldsymbol{X}]^s$. For $i = 1, \ldots, s$, let m_i be a generic polynomial of weighted degree γ_i. For

$j = 1, \ldots, q$, let r_j be a generic polynomial of weighted degree δ_j. Then we define

$$\boldsymbol{M} = (m_1, \ldots, m_s) \text{ and } \boldsymbol{L} = \begin{pmatrix} c_{1,1}r_1 & \cdots & c_{1,q}r_q \\ \vdots & & \vdots \\ c_{p,1}r_1 & \cdots & c_{p,q}r_q \end{pmatrix}, \tag{7.11}$$

for a generic choice $c_{i,j}$.

For $i = 1, \ldots, s$, let $\mathcal{A}'_i$ be a subset of $\mathbb{N}^n$

$$\mathcal{A}'_i = \{(e_1, \ldots, e_n) \in \mathbb{N}^n \,:\, w_1e_1 + \cdots + w_ne_n \leq \gamma_i\},$$

and for $j = 1, \ldots, q$, let

$$\mathcal{B}'_j = \{(e_1, \ldots, e_n) \in \mathbb{N}^n \,:\, w_1e_1 + \cdots + w_ne_n \leq \delta_j\}.$$

be a subset of $\mathbb{N}^n$. The sets $\mathcal{A}'_i$, respectively $\mathcal{B}'_j$, are the supports of generic polynomials of weighted degrees at most γ_i, respectively δ_j. In other words, they are supports of polynomials m_i and r_j, respectively. In particular, the monomial supports $\mathcal{A}_1, \ldots, \mathcal{A}_s$ of $g_1, \ldots, g_s$ are contained in the sets $\mathcal{A}'_1, \ldots, \mathcal{A}'_s$. Similarly, for $1 \leq j \leq q$, $\mathcal{B}_j \subset \mathbb{N}^n$ is contained in the set $\mathcal{B}'_j$. Therefore, all requirements C_1, C_2, and B_1, B_2 as well are satisfied.

7.2.2 Setting up parameters

Similar to what we followed, we need to ensure that we can prepare the inputs for the homotopy algorithms: straight-line program for $\boldsymbol{B}$, a zero-dimensional representation of the solutions of $\boldsymbol{A} = \boldsymbol{B}_{t=0}$ and an upper bound on the degree of the homotopy curve.

A straight-line program for $\boldsymbol{B}$.

We follow the same approach as in the last subsection to obtain a straight-line program for $\boldsymbol{B}$, simply by computing all monomials of respective weighted degrees at most $(\gamma_1, \ldots, \gamma_s)$ and $(\delta_1, \ldots, \delta_q)$, combining them to form the polynomials $(1-t)\cdot\boldsymbol{M} + t\cdot\boldsymbol{G}$ and the matrix $(1-t)\cdot\boldsymbol{L} + t\cdot\boldsymbol{F}$ and taking the p-minors of the latter.

We benefit from a minor improvement here, as for a fixed γ_i or δ_j we can compute all these monomials in an incremental manner, starting from the monomial 1, foregoing the use of repeated squaring: this saves a factor $n\log(d)$. Altogether, this results in a straight-line program of size

$$\Gamma \in O\left((\gamma'_1 + \cdots + \gamma'_s + p(\delta'_1 + \cdots + \delta'_q)) + p^4\binom{q}{p}\right)$$

to compute all entries of $\boldsymbol{B}$.

Recall that a term such as γ_i' denotes the number of monomials of weighted degree at most γ_i in n variables, with $\gamma_i \leq d$ for all i (and similarly for δ_j', for the weighted degree bound δ_j). A crude bound is thus $\gamma_i', \delta_j' \leq \binom{n+d}{n}$ for all i, j, resulting in the estimate

$$\Gamma \in O\left(n^2\binom{n+d}{n} + n^4\binom{q}{p}\right). \tag{7.12}$$

This is not the sharpest possible bound. Bounding a_i' by the volume of the non-negative simplex defined by

$$w_1(e_1 - 1) + \cdots + w_n(e_n - 1) \leq \gamma_i$$

results in the upper bound $a_i' \leq (\gamma_i + w_1 + \cdots + w_n)^n/(n! w_1 \cdots w_n)$. Using results from Proposition 3.4.4 gives more refined bounds for γ_i' and δ_j' and hence also for Γ.

A zero-dimensional parametrization $\mathscr{R}_0$ of $V(\boldsymbol{A})$.

As in the case of sparse polynomials, for a generic choice of $c_{i,j}$ and for polynomials m_i and r_j with generic coefficients, the solutions of the start system $\boldsymbol{A}$ are the disjoint union of the solutions of systems $(\boldsymbol{R}_i, \boldsymbol{M}) = (r_{i_1}, \ldots, r_{i_{n-s}}, m_1, \ldots, m_s)$, for $\boldsymbol{i} = (i_1, \ldots, i_{n-s}) \subset \{1, \ldots, q\}^{n-s}$.

By the weighted Bézout theorem, the system $(\boldsymbol{R}_i, \boldsymbol{M})$ has

$$c_{\boldsymbol{i}} = \frac{\gamma_1 \cdots \gamma_s \delta_{i_1} \cdots \delta_{i_{n-s}}}{w_1 \cdots w_n}$$

solutions in $\overline{\mathbb{K}}^n$. Taking the sum over all subsets $\boldsymbol{i}$ of $\{1, \ldots, q\}$ of cardinality $n - s$, we deduce that the number of solutions of $\boldsymbol{B}_{t=0}$ is at most

$$\tilde{c} = \sum_{\boldsymbol{i}} c_{\boldsymbol{i}} = \frac{\gamma_1 \cdots \gamma_s \, \eta_{n-s}(\delta_1, \ldots, \delta_q)}{w_1 \cdots w_n}, \tag{7.13}$$

where $\eta_{n-s}(\delta_1, \ldots, \delta_q)$ is the elementary symmetric polynomial of degree $n-s$ in $\delta_1, \ldots, \delta_q$. The discussion following Proposition 7.1.2 implies that the system $\boldsymbol{B}_{t=1}$ which we want to solve admits at most $\tilde{c}$ isolated solutions.

To find these solutions, as in the previous subsection, we solve all systems $(\boldsymbol{R}_{\boldsymbol{i}}, \boldsymbol{M})$ independently. We are not aware of a dedicated algorithm for weighted-degree polynomial systems whose complexity would be suitable; instead, we rely on the geometric resolution algorithm as presented in [87].

For a subset $\boldsymbol{i} = \{i_1, \ldots, i_{n-s}\} \subset \{1, \ldots, q\}$, let $(d_{\boldsymbol{i},1}, \ldots, d_{\boldsymbol{i},n})$ denote the sequence $(\gamma_1, \ldots, \gamma_s, \delta_{i_1}, \ldots, \delta_{i_{n-s}})$; we write

$$\kappa_{\boldsymbol{i}} = \max_{1 \leq k \leq n} (d_{\boldsymbol{i},1} \cdots d_{\boldsymbol{i},k} w_{k+1} \cdots w_n) \quad \text{and} \quad \kappa = \sum_{\boldsymbol{i} = \{i_1, \ldots, i_{n-s}\} \subset \{1, \ldots, q\}} \kappa_{\boldsymbol{i}}. \tag{7.14}$$

Recall as well that we set $d = \max(\gamma_1, \ldots, \gamma_s, \delta_1, \ldots, \delta_q)$ and we arrange $\boldsymbol{w} = (w_1, \ldots, w_n)$ as $w_1 \leq \cdots \leq w_n$.

Lemma 7.2.1. *Let $\boldsymbol{M} = (m_1, \ldots, m_s)$ and $\boldsymbol{R} = (r_1, \ldots, r_q)$ be generic polynomials (in the Zariski sense). For $\boldsymbol{i} = \{i_1, \ldots, i_{n-s}\} \subset \{1, \ldots, q\}$, one can solve $(\boldsymbol{R_i}, \boldsymbol{M})$ by a randomized algorithm that uses*

$$O^{\sim}\left(n^4 \Gamma d^2 \left(\frac{\kappa_i}{w_1 \cdots w_n}\right)^2\right)$$

operations in $\mathbb{K}$.

Proof. Since the supports of $\boldsymbol{R_i}$ and $\boldsymbol{M}$ contain the origin and they are generic polynomials, by Proposition 7.1.3, the equations $(\boldsymbol{R_i}, \boldsymbol{M})$ define a reduced regular sequence (possibly terminating early and thus defining the empty set). We can thus apply the geometric resolution algorithm, which is denoted by GeometricResolution, in Theorem 1.3.1. The polynomials $(\boldsymbol{R_i}, \boldsymbol{M})$ have weighted degrees at most $(\gamma_1, \ldots, \gamma_s, \delta_{i_1}, \ldots, \delta_{i_{n-s}})$; to simplify indexing, as above, we rewrite this sequence of degrees as $(d_{\boldsymbol{i},1}, \ldots, d_{\boldsymbol{i},n})$. For the same reason, we rewrite the polynomials $(\boldsymbol{R_i}, \boldsymbol{M})$ themselves as $h_1, \ldots, h_n$.

The GeometricResolution algorithm in Theorem 1.3.1 takes its input represented as a straight-line program that computes $(\boldsymbol{R_i}, \boldsymbol{M})$. To obtain one, we take our straight-line program of length Γ that computes $\boldsymbol{B}$ and set $t = 0$; the resulting straight-line program computes all $\boldsymbol{R}$ and $\boldsymbol{M}$, and in particular $(\boldsymbol{R_i}, \boldsymbol{M})$. We deduce that we can compute a zero-dimensional parametrization of the solutions of $(\boldsymbol{R_i}, \boldsymbol{M})$ using

$$O^{\sim}(n^4 \Gamma d^2 \boldsymbol{\Sigma_i}^2)$$

operations in $\mathbb{K}$. Here, $\boldsymbol{\Sigma_i}$ is the maximum of the degrees of the "intermediate varieties" $V_1, \ldots, V_n$, where V_i is defined by the first i equations in $(\boldsymbol{R_i}, \boldsymbol{M})$. Hence, to conclude, it suffices to prove that $\boldsymbol{\Sigma_i} \leq \kappa_{\boldsymbol{i}}/(w_1 \cdots w_n)$.

Fix an index ℓ in $\{1, \ldots, n\}$. We identify degree-one polynomials $P = p_0 + p_1 x_1 + \cdots + p_n x_n$ in $\overline{\mathbb{K}}[x_1, \ldots, x_n]$ with points in $\overline{\mathbb{K}}^{n+1}$. Then, there exists a non-empty Zariski open set $\mathscr{P} \subset \overline{\mathbb{K}}^{(n+1)(n-\ell)}$ such that for $(p_{i,j})_{0 \leq j \leq n, 1 \leq i \leq n-\ell} \in \mathscr{P}$, defining P_i as

$$P_i = p_{i,0} + p_{i,1} x_1 + \cdots + p_{i,n} x_n$$

implies that $V_\ell \cap V(P_1) \cdots \cap V(P_{n-\ell})$ has cardinality $\deg(V_\ell)$. Up to taking the $p_{i,j}$'s in the intersection of $\mathscr{P}$ with another non-empty Zariski open set, one can perform Gaussian elimination to rewrite $P_1, \ldots, P_{n-\ell}$ as

$$x_{\ell+1} - \wp_{\ell+1}(x_1, \ldots, x_\ell), \ldots, x_n - \wp_n(x_1, \ldots, x_\ell).$$

For $k = 1, \ldots, \ell$, let $g_k(x_1, \ldots, x_\ell) = h_k(x_1, \ldots, x_\ell, \wp_{\ell+1}(x_1, \ldots, x_\ell), \ldots, \wp_n(x_1, \ldots, x_\ell))$ in $\mathbb{K}[x_1, \ldots, x_\ell]$. Because the sequence of weights is non-decreasing, these have respective weighted degrees at most $d_1, \ldots, d_\ell$ and, by construction, $V(g_1, \ldots, g_\ell)$ is finite and $\deg(V_\ell) = \deg(V(g_1, \ldots, g_\ell))$. Using the weighted Bézout's theorem implies

$$\deg(V(g_1, \ldots, g_\ell)) \leq \frac{d_{\boldsymbol{i},1} \cdots d_{\boldsymbol{i},\ell}}{w_1 \cdots w_\ell} = \frac{d_{\boldsymbol{i},1} \cdots d_{\boldsymbol{i},\ell} w_{\ell+1} \cdots w_n}{w_1 \cdots w_n} = \frac{\kappa_{\boldsymbol{i}}}{w_1 \cdots w_n}.$$

Taking all possible $\boldsymbol{i}$ into account, we see that for a generic ρ we can compute zero-dimensional parametrizations for all $(\boldsymbol{R_i}, \boldsymbol{M})$ using

$$O^{\sim}\left(n^4\Gamma d^2\left(\frac{\kappa}{w_1\cdots w_n}\right)^2\right)$$

operations in $\mathbb{K}$. As in the previous subsection, taking the union of all these parametrizations does not introduce any added cost. □

An upper bound on the degree of the homotopy curve.

As before, a suitable upper bound is the number of isolated intersection points in $\overline{\mathbb{K}}^{n+1}$ between $V(\boldsymbol{B})$ and a generic hyperplane. Let $\zeta = \zeta_0 + \zeta_1 x_1 + \cdots + \zeta_n x_n + \zeta_{n+1} t$ be a linear form defining such a hyperplane (here, we take $\zeta_i \in \mathbb{K}$). We are interested in counting the isolated solutions of all equations $\boldsymbol{G'} = (\zeta, (1-t)\cdot\boldsymbol{M} + t\cdot\boldsymbol{G})$, and all p-minors of $\boldsymbol{F'} = (1-t)\cdot\boldsymbol{L} + t\cdot\boldsymbol{F}$, that is, of $V_p(\boldsymbol{F'}, \boldsymbol{G'})$.

Assign weight $w_t = 1$ to t, so the weighted degree of ζ is w_n. Then, the system above is of the kind considered in this section, but with $n+1$ variables instead of n, and $s+1$ equations $\boldsymbol{G'}$ instead of s. The weighted degrees of the equations $\boldsymbol{G'}$ are $(w_n, \gamma_1+1, \ldots, \gamma_s+1)$ and the weighted column degrees of $\boldsymbol{F'}$ are $(\delta_1+1, \ldots, \delta_q+1)$. As we pointed out when counting the solutions of the start system, this implies that our equations admit at most e isolated solutions, with

$$\tilde{e} = \frac{(\gamma_1+1)\cdots(\gamma_s+1)\,\eta_{n-s}(\delta_1+1, \ldots, \delta_q+1)}{w_1\cdots w_{n-1}}, \tag{7.15}$$

where η_{n-s} is the elementary symmetric polynomial of degree $n-s$.

7.2.3 Completing the weighted column-degree homotopy

The previous sections allow us to use the Homotopy algorithm from Proposition 5.2.11. We obtain the following result.

Theorem 7.2.2. *The set $V_p(\boldsymbol{F}, \boldsymbol{G})$ admits at most $\tilde{c}$ isolated solutions, counted with multiplicities. There exists a randomized algorithm which takes $\boldsymbol{G}$ and $\boldsymbol{F}$ as input and computes a zero-dimensional parametrization of these isolated solutions using*

$$O^{\sim}\Big(\Big(\tilde{c}(\tilde{e}+\tilde{c}^5) + d^2\left(\frac{\kappa}{w_1\cdots w_n}\right)^2\Big)n^4\Gamma\Big)$$

operations in $\mathbb{K}$, where $\Gamma, \tilde{c}, \kappa, \tilde{e}$ are as in respectively (7.12), (7.13), (7.14) and (7.15).

Algorithm 12 WeightedColumnDegree($\boldsymbol{F}, \boldsymbol{G}$)

Input: a matrix $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with $\mathrm{wdeg}(f_{i,j}) \leq \delta_j$ for all j and $p \leq q$; and polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$, with $\mathrm{wdeg}(g_i) = \gamma_i$ and $n = q - p + s + 1$
Output: a zero-dimensional parametrization of the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{G})$.

1. construct $\boldsymbol{L} = [c_{i,j} r_j]_{1 \leq i \leq p, 1 \leq j \leq q} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ and $\boldsymbol{M} = (m_1, \ldots, m_s)$ in $\mathbb{K}[x_1, \ldots, x_n]^s$ as in (7.11)
2. for any subsequence $\boldsymbol{i} = (i_1, \ldots, i_{n-s})$ of $(1, \ldots, q)$
   (a) construct a straight-line program $\Delta_{\boldsymbol{i}}$ that computes $(r_{i_1}, \ldots, r_{i_{n-s}}, m_1, \ldots, m_s)$
   length of $\Delta_{\boldsymbol{i}} = O(\Gamma)$ with Γ is given in (7.12)
   (b) $\mathscr{R}_{0,\boldsymbol{i}} \leftarrow$ GeometricResolution($\Delta_{\boldsymbol{i}}$)
   cost: $O^{\sim}(n^4 \Gamma d^2 \boldsymbol{\Sigma}_{\boldsymbol{i}}^2)$ with $\boldsymbol{\Sigma}_{\boldsymbol{i}} \leq \kappa_{\boldsymbol{i}} / (w_1 \cdots w_n)$ and $\kappa_{\boldsymbol{i}}$ is given in (7.14).
3. combine all $(\mathscr{R}_{0,\boldsymbol{i}})_{\boldsymbol{i}}$ into a zero-dimensional parametrization $\mathscr{R}_0$
   cost: $O^{\sim}(cn)$ with c is given in (7.13)
4. construct a straight-line program Δ' that computes all polynomials $\boldsymbol{B}$
   length of Δ' is Γ
5. return Homotopy($\Delta', \mathscr{R}_0, e$)
   cost: $O^{\sim}\left(c^5 m n^2 + c(e + c^5) n (\Gamma + n^3)\right)$, with e is given in (7.15)

7.2.4 Example

In this section we provide an example illustrating the steps of our column-support homotopy algorithms. Let

$$\boldsymbol{G} = (99x_1^3 + 92x_1^2 - 228x_1x_2 + 67x_1 - 140x_2 + 98x_3 + 25) \in \mathbb{Q}[x_1, x_2, x_3]$$

and $\boldsymbol{F} \in \mathbb{Q}[x_1, x_2, x_3]^{2 \times 3}$ be

$$\begin{pmatrix} 9x_1^2 + 65471x_1 + 59x_2 + 42308x_3 + 65504 & 86x_1^2 + 65460x_1 + 65414x_2 + 12381x_3 + 44 & 65477x_1 + 59898x_3 + 76 \\ 65501x_1^2 + 51x_1 + 65466x_2 + 57496x_3 + 35 & 16x_1^2 + 99x_1 + 65503x_2 + 17950x_3 + 31 & 65454x_1 + 41178x_3 + 65453 \end{pmatrix}.$$

The support of g is $\mathcal{A} = \{(3,0,0), (2,0,0), (1,1,0), (1,0,0), (0,1,0), (0,0,1), (0,0,0)\} \subset \mathbb{Z}^3$ with unions of the column supports of $\boldsymbol{F}$ being

$$\begin{aligned} \mathcal{B}_1 &= \{(2,0,0), (1,0,0), (0,1,0), (0,0,1), (0,0,0)\}, \\ \mathcal{B}_2 &= \{(2,0,0), (1,0,0), (0,1,0), (0,0,1), (0,0,0)\}, \\ \mathcal{B}_3 &= \{(1,0,0), (0,0,1), (0,0,0)\}. \end{aligned}$$

Start system. The start system for $(\boldsymbol{F}, \boldsymbol{G})$ is built as follows. Let $m_1 = 88x_1^3 - 82x_1^2 - 70x_1x_2 + 41x_1 + 91x_2 + 29x_3 + 70 \in \mathbb{Q}[x_1, x_2, x_3]$ a polynomial supported by $\mathcal{A}$ and define $r_1 = -78x_1^2 - 4x_1 + 5x_2 - 91x_3 - 44$, $r_2 = 63x_1^2 + 10x_1 - 61x_2 - 26x_3 - 20$, and $r_3 = 88x_1 + 95x_3 + 9$, polynomials in $\mathbb{Q}[x_1, x_2, x_3]$ supported by $(\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$. The start polynomials $\boldsymbol{M} = (m_1)$ and the start matrix is given as

$$\boldsymbol{L} = \begin{pmatrix} -62r_1 & 26r_2 & 10r_3 \\ -83r_1 & -3r_2 & -44r_3 \end{pmatrix} \in \mathbb{Q}[x_1, x_2, x_3]^{2\times 3}.$$

We remark that the coefficients in the start equation and start matrix for this example were chosen randomly, in this case with the help of the rand() command in Maple.

A parametrization of the start system. The set of 2-minors of $\boldsymbol{L}$ is given by $(2344r_1r_2, 3558r_1r_3, -1114r_2r_3)$ and hence $V_2(\boldsymbol{L}, m_1) = V_1 \cup V_2 \cup V_3$, where

$$V_1 = V(r_1, r_2, m_1),\ V_2 = V(r_1, r_3, m_1),\ \text{and}\ V_3 = V(r_2, r_3, m_1).$$

Parametrizations of V_1, V_2, and V_3 are given by

$$\begin{aligned}
\mathscr{R}_{0,1} = \ & \big((10671923044484y^3 + 1646504057122 64y^2 + 541980679674061y + 393540496795784, \\
& \frac{23707677043321206}{205138445880446701}y^2 + \frac{197994419338092137}{205138445880446701}y + \frac{3859258707817950}{205138445880446701}, \\
& \frac{2817387683743776}{205138445880446701}y^2 - \frac{334804957251324375}{205138445880446701}y - \frac{199554818581221524}{205138445880446701}, y), x_3\big), \\
\mathscr{R}_{0,2} = \ & \big((1076005625y^3 + 2749690925y^2 + 2278375403y + 797867887, \\
& -\frac{95}{88}y - \frac{9}{88}, \frac{70395}{3872}y^2 + \frac{201161}{9680}y + \frac{171943}{19360}, y), x_3\big), \\
\mathscr{R}_{0,3} = \ & \big((410682625y^3 + 773879025y^2 + 2045246267y - 666910765, \\
& -\frac{95}{88}y - \frac{9}{88}, \frac{568575}{472384}y^2 - \frac{88607}{236192}y - \frac{157697}{472384}, y), x_3\big).
\end{aligned}$$

Taking the union of $(\mathscr{R}_{0,i})_{1\le i\le 3}$ gives a parametrization $\mathscr{R}_0$ of $V_p(\boldsymbol{M}, r)$ with

$$\begin{aligned}
\mathscr{R}_0 = \ & ((q_0, v_{0,1}, v_{0,2}, v_{0,3}), \lambda) \\
= \ & \big((4715888798904593238258009062500y^9 + \cdots, \\
& \frac{1047634696676655387879016713234375 0}{205138445880446701}y^8 + \cdots, \\
& \frac{2265193491697540283699777221137124035318470625}{24226029904697233601296}y^8 + \cdots, \\
& 15866264491953179878625y^7 + \cdots), x_3\big).
\end{aligned}$$

Degree bounds. The mixed volumes associated to our sub-square systems are $\mathsf{MV}_1 = \mathsf{MV}(\mathrm{conv}(\mathcal{A}), \mathrm{conv}(\mathcal{B}_1), \mathrm{conv}(\mathcal{B}_2)) = 3$, $\mathsf{MV}_2 = \mathsf{MV}(\mathrm{conv}(\mathcal{A}), \mathrm{conv}(\mathcal{B}_1), \mathrm{conv}(\mathcal{B}_3)) = 3$, and finally $\mathsf{MV}_3 = \mathsf{MV}(\mathrm{conv}(\mathcal{A}),\ \mathrm{conv}(\mathcal{B}_2), \mathrm{conv}(\mathcal{B}_3)) = 3$. So $\chi = \mathsf{MV}_1 + \mathsf{MV}_2 + \mathsf{MV}_3 = 9$ which is a bound on the number of isolated solutions of $V_2(\boldsymbol{F}, \boldsymbol{G})$. Note that this number coincides with the actual number of isolated solutions of $V_2(\boldsymbol{L}, m_1)$ as the degree of q_0 equals 9.

A parametrization $\mathscr{R}_1$ of $V_2(\boldsymbol{F},\boldsymbol{G})$. We apply the Homotopy algorithm to the system $(M_2((1-t)\boldsymbol{F}+t\boldsymbol{L}),(1-t)m_1+tg)$ and $\mathscr{R}_0$ to obtain $\mathscr{R}_1$. As the coefficients of the result over $\mathbb{Q}$ are quite large we illustrate this calculation over $\mathbb{F}_{65521}$, a finite field of 65521 elements. In this case we obtain

$$\begin{aligned}\mathscr{R}_0 = \ & \big((y^9+42377y^8+63439y^7+23268y^6+1541y^5+21916y^4\\ & +24479y^3+1064y^2+47617y+765, 18447y^8+58286y^7+48619y^6\\ & +49312y^5+\ 42721y^4+44021y^3+47621y^2+39038y+13072,\\ & 9852y^8+30892y^7+\ 29236y^6+63043y^5+623y^4+8249y^3\\ & +22956y^2+23577y+41427,\ 3y^7+19233y^6+56323y^5+58151y^4\\ & +8939y^3+30577y^2+13156y), x_3\big)\end{aligned}$$

and

$$\begin{aligned}\mathscr{R}_1 = \ & \big((y^9+27502y^8+1022y^7+42474y^6+21370y^5+47501y^4\\ & +37694y^3+\ 13474y^2+49870y+26489, 19690y^8+28497y^7\\ & +23045y^6+29265y^5+\ 32212y^4+8948y^3+16460y^2\\ & +19357y+9600, 26426y^8+24119y^7+\ 48429y^6+34031y^5\\ & +32994y^4+13559y^3+34993y^2+59636y+64778, y), x_3\big).\end{aligned}$$

We note that using the Algorithm ColumnDegree from Section 6.2 produces a degree bound of 24, a considerable over estimate of the number of isolated zeros.

Part II

Invariant algebraic systems

Chapter 8

An overview

In this part of the thesis, we consider the problem of computing critical points of the restriction of a polynomial map to an algebraic variety. We study the important case where the input polynomials are all invariant under the action of the symmetric group $\mathcal{S}_n$. The problem of computing such points appears in many application areas including for example polynomial optimization and real algebraic geometry.

8.1 Problem statement and main results

Let $\boldsymbol{G} = (g_1, \ldots, g_s)$ and ϕ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$, with $\mathbb{K}$ a field of characteristic zero. Let $W(\phi, \boldsymbol{G})$ be an algebraic set defined by the following equations

$$\langle g_1, \ldots, g_s \rangle + \langle M_{s+1}(\mathrm{Jac}(\boldsymbol{G}, \phi)) \rangle \tag{8.1}$$

where, $\mathrm{Jac}(\boldsymbol{G}, \phi)$ is the Jacobian matrix of $(g_1, \ldots, g_s, \phi)$ with respect to $(x_1, \ldots, x_n)$, and $M_r(\boldsymbol{F})$ denotes the set of all r-minors of a matrix $\boldsymbol{F}$. If we assume that the Jacobian matrix $\mathrm{Jac}(\boldsymbol{G})$ has full rank s at any point of $V(\boldsymbol{G})$, then, Lemma 3.1.8 implies that the algebraic set $V(\boldsymbol{G})$ is smooth and $(n-s)$-equidimensional, and so that $W(\phi, \boldsymbol{G})$ is indeed the set of critical points of ϕ on $V(\boldsymbol{G})$ by Lemma 3.1.10.

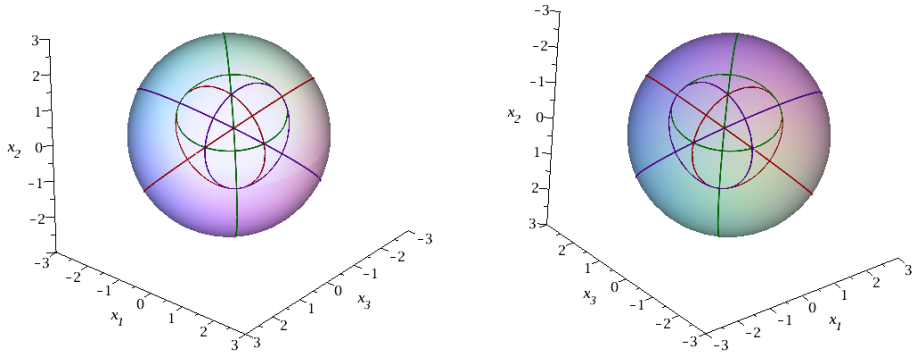
Let d be a bound for the degrees of $\boldsymbol{G}$ and ϕ. We provide a randomized algorithm to compute a representation for the set $W(\boldsymbol{G}, \phi)$ whose runtime is polynomial in $d^s, \binom{n+d}{n}, \binom{n}{s+1}$. This runtime is polynomial in the bound we give on the output size, as well as the number of maximal minors in the matrix $\mathrm{Jac}(\boldsymbol{G}, \phi)$.

Although $g_1, \ldots, g_s$ and ϕ are $\mathcal{S}_n$-invariant, the equations in (8.1) are usually not invariant. However, it can be shown that the system of equations in (8.1) is *globally invariant*. That is for all $\sigma \in \mathcal{S}_n$, and any f among either $g_1, \ldots, g_s$ or the $(s+1)$-minors of $\mathrm{Jac}(\boldsymbol{G}, \phi)$, either $\sigma(f)$ or $-\sigma(f)$ belongs again to the same set of equations. This implies that $W(\phi, \boldsymbol{G})$ is $\mathcal{S}_n$-invariant.

Example 8.1.1. Let $n = 3, s = 1$ and $\phi = x_1x_2x_3 - 3x_1 - 3x_2 - 3x_3$. The critical points of ϕ over the sphere defined by $g = x_1^2 + x_2^2 + x_3^2 - 6$ are solutions of the globally invariant system

$$(g\,,\, x_1^2x_3 - x_2^2x_3 - 3x_1 + 3x_2, x_1^2x_2 - x_2x_3^2 - 3x_1 + 3x_3, x_1x_2^2 - x_1x_3^2 - 3x_2 + 3x_3\,).$$

These critical points are the intersection of three different colors in Figure 8.1. From this figure, one can see that the set of these critical points is $\mathcal{S}_3$-invariant.



(a) First part. (b) Second part.

Figure 8.1: Critical points of $x_1x_2x_3 - 3x_1 - 3x_2 - 3x_3$ over the sphere $x_1^2 + x_2^2 + x_3^2 - 6$

The global invariance property allows us to split the set $W(\phi, \boldsymbol{G})$ into orbits under the action of the symmetric group with the size of the orbit of a point in $W(\phi, \boldsymbol{G})$ depending on the number of pairwise distinct coordinates of that point.

Example 8.1.2. For g and ϕ from Example 8.1.1, the points $(2, 1, 1), (0, \sqrt{3}, \sqrt{3}), (-2, -1, -1)$, and $(0, -\sqrt{3}, -\sqrt{3})$ each have three elements in their respective $\mathcal{S}_3$-orbits, while the points $(\sqrt{2}, \sqrt{2}, \sqrt{2})$ and $(-\sqrt{2}, -\sqrt{2}, -\sqrt{2})$ have only one point in their orbits. This is the entire decomposition of $W(\phi, g)$ into orbits, with the size of $W(\phi, g)$ being 14.

The different sizes of orbits needs to be considered for efficient computation. In order to study the structure of these orbits and take into consideration pairwise distinct coordinates, we make use of partitions of n. A sequence $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \ldots\, n_r^{\ell_r})$, with the ℓ_i and n_i positive integers and $n_1 < \cdots < n_r$, is called a *partition* of n if $n_1\ell_1 + n_2\ell_2 + \cdots + n_r\ell_r = n$. Partitions of n will be used to parameterize orbits, with λ as above parameterizing those points in $W(\phi, \boldsymbol{G})$ having ℓ_1 distinct sets of n_1 equal coordinates, ℓ_2 distinct sets of n_2 equal coordinates and so on. We will write W_λ for the set of such orbits contained in $W(\phi, \boldsymbol{G})$, so that $W(\phi, \boldsymbol{G})$ is the disjoint union of all W_λ, for all partitions λ of n.

Example 8.1.3. Let ϕ and g be defined in Example 8.1.1 and Example 8.1.2. The set $W_{(1^3)}$ of orbits parameterized by $\lambda = (1^3)$ corresponds to the orbits with all distinct coordinates (ξ_1, ξ_2, ξ_3). This set is the zero set of

$$(g,\ -4,\ -2(x_1 + x_2 + x_3),\ 2(x_1^2 + x_2^2 + x_3^2) + 8(x_1x_2 + x_2x_3 + x_1x_3) - 36).$$

The set $W_{(1^1\,2^1)}$ of orbits parameterized by $\lambda = (1^1\,2^1)$ is orbits of points of the form (ξ_1, ξ_2, ξ_2), with $\xi_1 \neq \xi_2$. It is the orbit of the zero set of

$$(x_1^2 + 2x_2^2 - 6,\ x_2^2 + x_1x_2 - 3,\ x_2 - x_3),$$

where the first polynomial is g restricted to the hyperplane $x_2 = x_3$. In particular, $W_{(1^1\,2^1)}$ is the union of the orbits of the points $(2, 1, 1), (0, \sqrt{3}, \sqrt{3}), (-2, -1, -1), (0, -\sqrt{3}, -\sqrt{3})$ seen in Example 8.1.2.

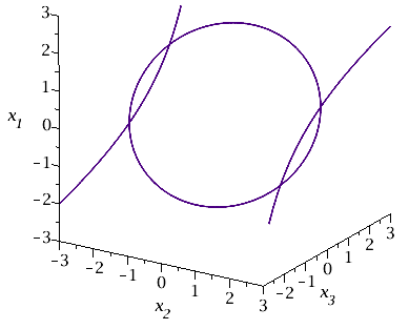


Figure 8.2: The zero set of $(x_1^2 + 2x_2^2 - 6, x_2^2 + x_1x_2 - 3, x_2 - x_3)$

Finally, the set $W_{(3^1)}$ of orbits parameterized by $\lambda = (3^1)$, which is orbit of points of the form (ξ_1, ξ_1, ξ_1), is the zero set of $3x_1^2 - 6 = 0$. This polynomial is g restricted to hyperplanes $x_2 = x_1$ and $x_3 = x_1$.

We provide a procedure to determine invariant polynomials that describe these $\mathcal{S}_n$-orbits. For an orbit parameterized by the partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \ldots\, n_r^{\ell_r})$, we work with points which have distinct coordinates $(\xi_{1,1}, \ldots, \xi_{1,\ell_1}, \xi_{2,1}, \ldots, \xi_{2,\ell_2}, \ldots, \xi_{r,1}, \ldots, \xi_{r,\ell_r})$. Instead of n coordinates, there are only $\ell = \ell_1 + \cdots + \ell_r$ distinct coordinates for points in this orbit. Invariance under permutations implies that single distinct points are permuted, groups of two points are permuted, etc. This will allow us to work with polynomials in $\mathbb{K}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r] = \mathbb{K}[e_{1,1}, \ldots, e_{1,\ell_1}, e_{2,1}, \ldots, e_{2,\ell_2}, \ldots, e_{r,1}, \ldots, e_{r,\ell_r}]$, in order to represent a certain "compressed" image $W'_\lambda \subset \overline{\mathbb{K}}^\ell$ of W_λ; here, $\boldsymbol{e}_k = (e_{k,1}, \ldots, e_{k,\ell_k})$ are variables standing for the elementary symmetric function in ℓ_k indeterminates.

Example 8.1.4. Continue previous examples, for $\lambda = (1^1\,2^1)$, we have $\ell = 2$ and $W'_\lambda = \{(2, 1), (0, \sqrt{3}), (-2, -1), (0, -\sqrt{3})\}$.

Throughout the thesis, we will assume that $W(\phi, \boldsymbol{G})$, and thus all W_λ and W'_λ, are finite. Then, for λ as above, the cardinality of W'_λ is smaller than that of W_λ by a factor

$$\nu_\lambda = \ell_1! \cdots \ell_r! \cdot \binom{n}{n_1, \ldots, n_1, \ldots, n_r, \ldots, n_r}, \tag{8.2}$$

where each n_i is repeated ℓ_i times in the multinomial term. We will prove some bounds, which will be denoted by $\mathfrak{c}_\lambda$ on the cardinality of W'_λ. The sum of the $\mathfrak{c}_\lambda$'s then gives us an upper bound on the size of the output of our main algorithm; we will see that, in practice (see Table 10.2), each of the $\mathfrak{c}_\lambda$ provides an accurate bound on the cardinality of the finite set W'_λ. Moreover, we can prove that this sum is bounded above by $\mathfrak{c}$, where

$$\mathfrak{c} = d^s \binom{n+d-1}{n}. \tag{8.3}$$

We will see that, in practice (see Table 10.1), this is a rather rough upper bound but in several cases, it compares well to the upper bound

$$\tilde{\mathfrak{c}} = d^s \, (d-1)^{n-s} \binom{n}{s} \tag{8.4}$$

from Nie and Ranestad [144, Theorem 2.2] on the size of $W(\phi, \boldsymbol{G})$. For example, when $d = 2$, we have $\mathfrak{c} = 2^s(n+1)$ while $\tilde{\mathfrak{c}} = 2^s\binom{n}{s}$. More generally, when d and s are fixed, $\mathfrak{c}$ is polynomial in n (since it is bounded above by $d^s(n+d-1)^d$) while $\tilde{\mathfrak{c}}$ is exponential in n (since it is greater than $(d-1)^n$). When s is fixed and $d = n$, $\mathfrak{c}$ is $n^{O(1)}2^n$, whereas $\tilde{\mathfrak{c}}$ is $n^{O(1)}(n-1)^{n-s}$.

The output of our algorithm will thus be a collection of zero-dimensional parameterizations, one for each of the sets W'_λ; we will call such a data structure a *symmetric representation* of $W(\phi, \boldsymbol{G})$ (precise definitions are in Section 9). Rather than using Gröbner bases to compute such descriptions, we will use a symbolic homotopy continuation, so as to control precisely the cost of the algorithm.

In our case we can make use of a sparse symbolic homotopy method given in Section 7 specifically designed to handle determinantal systems over weighted polynomial rings, that is, multivariate polynomial rings where each variable has a weighted degree, which is a positive integer. These domains arise naturally for our orbits: the domain arising from an orbit parameter λ has variables $e_{i,k}$ which are defined corresponding to elementary symmetric polynomials $\eta_{i,k}$; since $\eta_{i,k}$ has degree k, the variable $e_{i,k}$ will naturally be assigned weight k. The main result of this part is summarized in the following theorem.

Theorem 8.1.1. *Let $\boldsymbol{G} = (g_1, \ldots, g_s)$ and ϕ be $\mathcal{S}_n$-invariant polynomials in $\mathbb{K}[x_1, \ldots, x_n]$, with degree at most $d \geq 2$, and suppose that $W(\phi, \boldsymbol{G})$ is finite. Then, there exists a randomized algorithm that takes as input $\boldsymbol{G}, \phi$ and outputs a symmetric representation for the set $W(\phi, \boldsymbol{G})$, and whose runtime is polynomial in d^s, $\binom{n+d}{d}$, $\binom{n}{s+1}$. Moreover, the total number of points described by the output is at most $d^s\binom{n+d-1}{n}$.*

Note that the runtime is polynomial in the bound we give on the output size, as well as the number $\binom{n}{s+1}$ of maximal minors in the matrix $\mathrm{Jac}(\boldsymbol{G}, \phi)$. Section 10.2 gives a more precise estimate on the runtime of the algorithm.

8.2 Organization of part II

The second half of this thesis is organized as follows. In the next chapter, we provide several properties of invariant polynomials, discuss in detail the sets W_λ and W'_λ mentioned above, and describe the notion of a symmetric representation for the set $W(\phi, \boldsymbol{G})$. Chapter 10 contains our main algorithm, called Critical_Points_Per_Orbit, a proof of correctness, and the runtime of this algorithm, finishing the proof of Theorem 8.1.1. Experiments to validate our new algorithm is given in Section 10.4.

Chapter 9

Invariant algebraic representations

One of our key observations, formalized in the next chapter, is that the special nature of our set of critical points allows us to split $W(\phi, \boldsymbol{G})$ into subsystems defined by the orbits of the symmetric group $\mathcal{S}_n$.

Definition 9.0.1. *Let $\boldsymbol{\xi}$ be a point in $\overline{\mathbb{K}}^n$. The* orbit *of $\boldsymbol{\xi}$ which is denoted by $\mathcal{S}_n(\boldsymbol{\xi})$ is the set of form $\{\sigma(\boldsymbol{\xi}) \,|\, \sigma \in \mathcal{S}_n\}$.*

As mentioned in the previous chapter, the size of an orbit $\mathcal{S}_n(\boldsymbol{\xi})$ will depend on the number of pairwise distinct coordinates of $\boldsymbol{\xi}$. The general formula for this size is given in (9.2).

Example 9.0.1. With $n = 3$, a point of the form (ξ_1, ξ_2, ξ_2) with $\xi_1 \neq \xi_2$ will have an orbit of size 3.

As a result, we need to consider the separation of distinct coordinates in an orbit which is what we do in this chapter. We do this through a discussion of the geometry of (finite) $\mathcal{S}_n$-invariant subsets of $\overline{\mathbb{K}}^n$ and the data structures we can use to represent them. Much of what follows is preliminary for our description of orbits presented in the next section.

9.1 Partitions

Partitions play a major role in describing our orbits. In this section, we gather the basic definitions of partitions and of a few notions attached to them, which will be used throughout this chapter.

Definition 9.1.1. *A sequence $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \ldots\, n_r^{\ell_r})$, with ℓ_i's and n_i's positive integers and $n_1 < \cdots < n_r$, is called a* partition *of n if $n_1\ell_1 + n_2\ell_2 + \cdots + n_r\ell_r = n$. The number $\ell = \ell_1 + \cdots + \ell_r$ is called the* length *of the partition λ.*

Example 9.1.1. Partitions of 5 are $(1^5), (1^4\,2^1), (1^1\,2^2), (1^2\,3^1), (2^1\,3^1), (1^1\,4^1)$, and (5^1).

Sometimes it is convenient to use the ordered list $(n_1, \ldots, n_1, \ldots, n_r, \ldots, n_r)$ with each n_i repeated ℓ_i times to represent a partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \ldots\, n_r^{\ell_r})$.

Definition 9.1.2. *Consider integers n and n'. Let λ and λ' be partitions of n and n', respectively. The* union partition *of λ and λ' is $\lambda \cup \lambda'$ whose ordered list is obtained by merging those of λ and λ'.*

Note that if λ is a partition of n and λ' is a partition of n', then $\lambda \cup \lambda'$ is a partition of $n + n'$.

Example 9.1.2. Let $(2^1\,3^1)$ be a partition of 5 and $(1^1\,2^1)$ be a partition of 3. Then $(1^1\,2^2\,3^1)$, which is a partition of 8, is the union partition of $(2^1\,3^1)$ and $(1^1\,2^1)$.

We will make use of the *refinement order* on partitions (see [133, p. 103] or [31, p. 16]).

Definition 9.1.3. *Consider two partitions $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \ldots\, n_r^{\ell_r})$ and $\lambda' = (m_1^{k_1}\, m_2^{k_2}\, \ldots\, m_s^{k_s})$ of the same integer n. We say that λ* refines *λ', if λ is the union of some partitions $(\lambda_{i,j})_{1\leq i\leq s, 1\leq j\leq k_i}$, where $\lambda_{i,j}$ is a partition of m_i for all i, j.*

Example 9.1.3. For the partitions of $n = 3$, we have $(1^3) \leq (1^1 2^1) \leq (3^1)$.

Let $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \ldots\, n_r^{\ell_r})$ be a partition of n having length ℓ. For $k = 1, \ldots, r$, we will denote by $\boldsymbol{Z}_k = (z_{k,1}, \ldots, z_{k,\ell_k})$ a sequence of ℓ_k indeterminates. When convenient, we will also index the entire sequence of indeterminates

$$(\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r) = (z_{1,1}, \ldots, z_{r,\ell_r}) = (z_1, \ldots, z_\ell),$$

so that $z_1 = z_{1,1}, \ldots, z_\ell = z_{r,\ell_r}$. From this point of view, introducing $\tau_0 = 0$ and $\tau_k = \ell_1 + \cdots + \ell_k$, for $k = 1, \ldots, r$, any index i in $1, \ldots, \ell$ can be written uniquely as $i = \tau_{k-1} + u$, for some k in $1, \ldots, r$ and u in $1, \ldots, \ell_k$. Thus, the indeterminates $z_{k,1}, \ldots, z_{k,\ell_k}$ are numbered $z_{\tau_{k-1}+1}, \ldots, z_{\tau_k}$, with $\tau_r = \ell$.

Definition 9.1.4. *For a partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \ldots\, n_r^{\ell_r})$, we define the group*

$$\mathcal{S}_\lambda = \mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}.$$

The group $\mathcal{S}_\lambda$ acts naturally on $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]$, and we will denote by $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^{\mathcal{S}_\lambda}$ the $\mathbb{K}$-algebra of $\mathcal{S}_\lambda$-invariant polynomials. Note that $\mathcal{S}_\lambda$ can be seen as a subgroup of the permutation group $\mathcal{S}_\ell$ of $\{1, \ldots, \ell\}$, where $\mathcal{S}_{\ell_1}$ acts on the first ℓ_1 indices, $\mathcal{S}_{\ell_2}$ acts on the next ℓ_2 ones, etc.

9.2 Symmetric representations

In this section, we describe the geometry of $\mathcal{S}_\lambda$-orbits in $\overline{\mathbb{K}}^n$, and we define the data structure we will use to represent $\mathcal{S}_\lambda$-invariant sets, and present some basic algorithms related to it.

The mapping E_λ and its fibers. For a partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \dots\, n_r^{\ell_r})$ of n, we define the following two subsets of $\overline{\mathbb{K}}^n$:

(i) $\mathcal{C}_\lambda$: the set of all points $\boldsymbol{\xi}$ in $\overline{\mathbb{K}}^n$ that can be written as

$$\boldsymbol{\xi} = \Big(\underbrace{\xi_{1,1}, \dots, \xi_{1,1}}_{n_1}, \dots, \underbrace{\xi_{1,\ell_1}, \dots, \xi_{1,\ell_1}}_{n_1}, \dots, \underbrace{\xi_{r,1}, \dots, \xi_{r,1}}_{n_r}, \dots, \underbrace{\xi_{r,\ell_r}, \dots, \xi_{r,\ell_r}}_{n_r}\Big). \tag{9.1}$$

(ii) $\mathcal{C}_\lambda^{\text{strict}}$: the set of all $\boldsymbol{\xi}$ in $\mathcal{C}_\lambda$ for which the $\xi_{i,j}$'s in (9.1) are pairwise distinct.

To any point $\boldsymbol{\xi}$ in $\overline{\mathbb{K}}^n$ we can associate its *type*: this is the unique partition λ of n such that there exists σ in $\mathcal{S}_n$ for which $\sigma(\boldsymbol{\xi})$ lies in $\mathcal{C}_\lambda^{\text{strict}}$. Since all points in an orbit have the same type, we can then define the type of an orbit as the type of any point in it. Any orbit of type $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \dots\, n_r^{\ell_r})$ has size

$$\gamma_\lambda = \binom{n}{n_1, \dots, n_1, \dots, n_r, \dots, n_r} = \frac{n!}{n_1!^{\ell_1} \cdots n_r!^{\ell_r}} \tag{9.2}$$

since the stabilizer of a point in $\mathcal{C}_\lambda^{\text{strict}}$ is $\mathcal{S}_{n_1}^{\ell_1} \times \cdots \times \mathcal{S}_{n_r}^{\ell_r}$.

Clearly all points in $\mathcal{C}_\lambda^{\text{strict}}$ have type λ, but this is not necessarily true for all points in $\mathcal{C}_\lambda$. This can be understood with the help of the refinement order we introduced in Section 9.1, as $\mathcal{C}_\lambda$ contains points of type λ' for all $\lambda' \geq \lambda$. More precisely, $\mathcal{C}_\lambda$ is the disjoint union of all $\mathcal{C}_{\lambda'}^{\text{strict}}$ for all $\lambda' \geq \lambda$.

Example 9.2.1. For the partitions of $n = 3$, we have $(1^3) < (1^1 2^1) < (3^1)$. In addition,

(a) $\mathcal{C}_{(1^3)}$ is $\overline{\mathbb{K}}^3$, while $\mathcal{C}_{(1^3)}^{\text{strict}}$ is the set of all points $\boldsymbol{\xi}$ with pairwise distinct coordinates.

(b) $\mathcal{C}_{(1^1 2^1)}$ is the set of points that can be written $\boldsymbol{\xi} = (\xi_{1,1}, \xi_{2,1}, \xi_{2,1})$, while $\mathcal{C}_{(1^1 2^1)}^{\text{strict}}$ is the subset of it where $\xi_{1,1} \neq \xi_{2,1}$.

(c) $\mathcal{C}_{(3^1)} = \mathcal{C}_{(3^1)}^{\text{strict}}$ is the set of points $\boldsymbol{\xi}$ whose coordinates are all equal.

For λ as above, we define a mapping $E_\lambda : \mathcal{C}_\lambda \to \overline{\mathbb{K}}^\ell$ by

$$E_\lambda : \quad \boldsymbol{\xi} \text{ as in (9.1)} \quad \mapsto \quad (\eta_1(\boldsymbol{\xi}_1), \dots, \eta_{\ell_1}(\boldsymbol{\xi}_1), \dots, \eta_1(\boldsymbol{\xi}_r), \dots, \eta_{\ell_r}(\boldsymbol{\xi}_r)),$$

where for $i = 1, \ldots, r$ and $k = 1, \ldots, \ell_i$, $\eta_k(\boldsymbol{\xi}_i)$ is the degree k elementary symmetric function in $\boldsymbol{\xi}_i = (\xi_{i,1}, \ldots, \xi_{i,\ell_i})$. One should see this mapping as a means to compress orbits: through the application of E_λ, one can represent a whole orbit $\mathcal{O}$ of type λ, which has size $\nu_\lambda := \gamma_\lambda \times \ell_1! \cdots \ell_r!$, by the single point

$$E_\lambda(\mathcal{O} \cap \mathcal{C}_\lambda) = E_\lambda(\mathcal{O} \cap \mathcal{C}_\lambda^{\text{strict}}).$$

To put this into practice, we need to be able to recover an orbit from its image. Note that the mapping E_λ is onto: for $\boldsymbol{\varepsilon} = (\varepsilon_{1,1}, \ldots, \varepsilon_{r,\ell_r})$ in $\overline{\mathbb{K}}^\ell$, one can find a point $\boldsymbol{\xi}$ in the preimage $E_\lambda^{-1}(\boldsymbol{\varepsilon})$ by finding the roots $\xi_{i,1}, \ldots, \xi_{i,\ell_i}$ of

$$P_i(T) = T^{\ell_i} - \varepsilon_{i,1} T^{\ell_i - 1} + \cdots + (-1)^{\ell_i} \varepsilon_{i,\ell_i},$$

for $i = 1, \ldots, r$. Since we will use this idea often, we will write $E_\lambda^*(\boldsymbol{\varepsilon}) = \mathcal{S}_n(\boldsymbol{\xi})$ for the orbit of any such point $\boldsymbol{\xi}$ in $E_\lambda^{-1}(\boldsymbol{\varepsilon})$; this is well-defined, as all points in this fiber are $\mathcal{S}_n$-conjugate. More generally, for a set G in $\overline{\mathbb{K}}^\ell$, we will write $E_\lambda^*(G)$ for the union of the orbits $E_\lambda^*(\boldsymbol{\varepsilon})$, for $\boldsymbol{\varepsilon}$ in G, that is, $E_\lambda^*(G) = \bigcup_{\boldsymbol{\varepsilon} \in G} E_\lambda^*(\boldsymbol{\varepsilon})$.

The image $E_\lambda(\mathcal{C}_\lambda^{\text{strict}})$ of those points having type λ is an open subset $O_\lambda \subsetneq \overline{\mathbb{K}}^\ell$, defined by the conditions that the polynomials P_i above are pairwise coprime and square-free. For $\boldsymbol{\varepsilon}$ in $\overline{\mathbb{K}}^\ell \setminus O_\lambda$, the orbit $E_\lambda^*(\boldsymbol{\varepsilon})$ does not have type λ, but rather type λ', for some partition $\lambda' > \lambda$.

Example 9.2.2. With $n = 3$ and $\lambda = (1^1 2^1)$, we have $\ell = 2$ and E_λ maps points of the form $(\xi_{1,1}, \xi_{2,1}, \xi_{2,1})$ to $(\xi_{1,1}, \xi_{2,1})$. The polynomials P_1, P_2 defined in the previous paragraph are respectively given by $P_1(T) = T - \varepsilon_{1,1}$ and $P_2(T) = T - \varepsilon_{2,1}$, and O_λ is defined by $\varepsilon_{1,1} \neq \varepsilon_{2,1}$.

The point $\boldsymbol{\varepsilon} = (2, 3)$ is in O_λ; the orbit $E_\lambda^*(2, 3)$ is $\{(2, 3, 3), (3, 2, 3), (3, 3, 2)\}$. On the other hand, $\boldsymbol{\varepsilon} = (1, 1)$ is not in O_λ; the orbit $E_\lambda^*(1, 1)$ is the point $\{(1, 1, 1)\}$, and it has type $(3^1) > (1^1 2^1)$. Finally, if we define $G = \{(1, 1), (2, 3)\}$, then $E_\lambda^*(G)$ is the set $W = \{(1, 1, 1), (2, 3, 3), (3, 2, 3), (3, 3, 2)\}$.

We will need an algorithm that computes the type λ' of the orbit $E_\lambda^*(\boldsymbol{\varepsilon})$, for a given $\boldsymbol{\varepsilon}$ in $\mathbb{K}^\ell$, and also computes the value that the actual compression mapping $E_{\lambda'}$ takes at this orbit. The algorithm's specification assumes inputs in $\mathbb{K}$ (since our computation model is a RAM over $\mathbb{K}$) but the procedure makes sense over any field extension of $\mathbb{K}$. We will use this remark later in the proof of Lemma 9.2.3.

Lemma 9.2.1. *There exists an algorithm* $\mathsf{Type_Of_Fiber}(\lambda, \boldsymbol{\varepsilon})$ *which takes as input a partition λ of n with length ℓ and a point $\boldsymbol{\varepsilon}$ in $\mathbb{K}^\ell$, and returns a partition λ' of n of length k and a tuple $\boldsymbol{f}$ in $\mathbb{K}^k$, such that*

(i) *λ' is the type of the orbit $\mathcal{O} := E_\lambda^*(\boldsymbol{\varepsilon})$*

(ii) $E_{\lambda'}(\mathcal{O} \cap \mathcal{C}_{\lambda'}^{\mathrm{strict}}) = \{\boldsymbol{f}\}$.

The algorithm runs in time $O^{\sim}(n)$.

Proof. Write $\boldsymbol{\varepsilon} = (\varepsilon_{1,1}, \ldots, \varepsilon_{r,\ell_r})$. The points in $E_\lambda^{-1}(\boldsymbol{\varepsilon})$ are obtained as permutations of

$$\boldsymbol{\xi} = \Big(\underbrace{\xi_{1,1}, \ldots, \xi_{1,1}}_{n_1}, \quad \ldots, \quad \underbrace{\xi_{1,\ell_1}, \ldots, \xi_{1,\ell_1}}_{n_1}, \quad \ldots, \quad \underbrace{\xi_{r,1}, \ldots, \xi_{r,1}}_{n_r}, \quad \ldots, \quad \underbrace{\xi_{r,\ell_r}, \ldots, \xi_{r,\ell_r}}_{n_r}\Big),$$

where for $i = 1, \ldots, r$, $\xi_{i,1}, \ldots, \xi_{i,\ell_i}$ are the roots of

$$P_i(T) = T^{\ell_i} - \varepsilon_{i,1} T^{\ell_i - 1} + \cdots + (-1)^{\ell_i} \varepsilon_{i,\ell_i} = 0.$$

Finding the type of such a point $\boldsymbol{\xi}$ amounts to finding the duplicates among the $\xi_{i,j}$'s, and finding such duplicates can be done by computing the product

$$P = \Big(T^{\ell_1} - \varepsilon_{1,1} T^{\ell_1 - 1} + \cdots + (-1)^{\ell_1} \varepsilon_{1,\ell_1}\Big)^{n_1} \cdots \Big(T^{\ell_r} - \varepsilon_{r,1} T^{\ell_r - 1} + \cdots + (-1)^{\ell_r} \varepsilon_{r,\ell_r}\Big)^{n_r}$$

and its square-free factorization $P = Q_1^{m_1} \cdots Q_s^{m_s}$, with $m_1 < \cdots < m_s$ and all Q_i's square-free and pairwise coprime. If $k_i = \deg(Q_i)$ then $\boldsymbol{\xi}$ has type $\lambda' = (m_1^{k_1} m_2^{k_2} \ldots m_s^{k_s})$ with $\lambda' > \lambda$. If we write

$$Q_i = T^{k_i} - f_{i,1} T^{k_i - 1} + \cdots + (-1)^{k_i} f_{i,k_i}, \quad 1 \le i \le s,$$

then our output is $(\lambda', \boldsymbol{f})$, where $\boldsymbol{f} = (f_{1,1}, \ldots, f_{s,k_s})$.

Using sub-product tree techniques [80, Chapter 10] to compute P and fast GCD [80, Chapter 14], all computations take quasi-linear time $O^{\sim}(n)$. □

Example 9.2.3. Let $n = 3$ and $\lambda = (1^1 2^1)$, with $E_\lambda(\xi_{1,1}, \xi_{2,1}, \xi_{2,1}) = (\xi_{1,1}, \xi_{2,1})$. We saw that for $\boldsymbol{\varepsilon} = (1, 1)$ in $\mathbb{K}^2$, the orbit $E_\lambda^*(1, 1)$ is $\{(1, 1, 1)\}$, which has type $\lambda' = (3^1)$.

Since $n_1 = 1$ and $n_2 = 2$, the above algorithm first expands the product $(T-1)(T-1)^2$ as $T^3 - 3T^2 + 3T - 1$, then computes its square-free factorization as $(T-1)^3$. From this, we read off that $s = 1$, $m_1 = 3$ and $k_1 = 1$, so that λ' is indeed (3^1). The output is $(\lambda', E_{\lambda'}(1, 1, 1))$, the latter being equal to (1).

A data structure for $\mathcal{S}_n$-invariant sets. The previous setup allows us to represent invariant sets in $\overline{\mathbb{K}}^n$ as follows. Let W be a set in $\overline{\mathbb{K}}^n$, invariant under the action of $\mathcal{S}_n$. For a partition λ of n with ℓ, we write

$$W_\lambda = \mathcal{S}_n(W \cap \mathcal{C}_\lambda^{\mathrm{strict}}) \subset \overline{\mathbb{K}}^n \quad \text{and} \quad W'_\lambda = E_\lambda(W \cap \mathcal{C}_\lambda^{\mathrm{strict}}) \subset \overline{\mathbb{K}}^\ell, \tag{9.3}$$

where $\mathcal{S}_n(W \cap \mathcal{C}_\lambda^{\mathrm{strict}})$ is the orbit of $W \cap \mathcal{C}_\lambda^{\mathrm{strict}}$ under $\mathcal{S}_n$, or, equivalently, the set of points of type λ in W (so this matches the notation used in the introduction).

For two distinct partitions λ, λ' of n, W_λ and $W_{\lambda'}$ are disjoint, so that any invariant set W can be written as the disjoint union $W = \sqcup_{\lambda \vdash n} W_\lambda$. When W is finite, we then can represent W_λ by describing the image W'_λ. Indeed, the cardinality of the set W'_λ is smaller than that of the orbit W_λ by a factor of ν_λ, and we can recover W_λ as $W_\lambda = E_\lambda^*(W'_\lambda)$. Altogether, we are led to the following definition.

Definition 9.2.2. *Let W be a finite set in $\overline{\mathbb{K}}^n$, defined over $\mathbb{K}$ and $\mathcal{S}_n$-invariant. A* symmetric representation *of W is a sequence $(\lambda_i, \mathscr{R}_i)_{1\le i\le N}$, where the λ_i's are all the partitions of n for which W_{λ_i} is not empty, and, for each i, $\mathscr{R}_i$ is a zero-dimensional parametrization of W'_{λ_i}.*

Example 9.2.4. Suppose $n = 3$ and

$$W = \{(1,1,1), (2,3,3), (3,2,3), (3,3,2)\}.$$

Then with $\lambda = (1^1 2^1)$ we have $W_\lambda = \{(2,3,3), (3,2,3), (3,3,2)\}$, $W'_\lambda = \{(2,3)\} \subset \overline{\mathbb{K}}^2$ and $\gamma_\lambda = \nu_\lambda = 3$, while with $\lambda' = (3^1)$, we have $W_{\lambda'} = \{(1,1,1)\}$, $W'_{\lambda'} = \{(1)\} \subset \overline{\mathbb{K}}^1$ and $\gamma_{\lambda'} = \nu_{\lambda'} = 1$.

A symmetric representation of W would consist of $(\lambda, \mathscr{R}_\lambda)$ and $(\lambda', \mathscr{R}_{\lambda'})$, with $V(\mathscr{R}_\lambda) = \{(2,3)\}$ and $V(\mathscr{R}_{\lambda'}) = \{(1)\}$.

Our main algorithm will have to deal with the following situation. As input, we will be given a representation of the set G in $\overline{\mathbb{K}}^\ell$; possibly, some points in G will not be in the open set O_λ (that is, may correspond to orbits having type λ', for some $\lambda' > \lambda$). As usual, the finite set G will be described by means of a zero-dimensional parametrization. Our goal will then be to compute a symmetric representation of $E^*_\lambda(G)$.

Example 9.2.5. Take $n = 3$, and let again $\lambda = (1^1 2^1)$, with $E_\lambda(\xi_{1,1}, \xi_{2,1}, \xi_{2,1}) = (\xi_{1,1}, \xi_{2,1})$. Assume we are given $G = \{(1,1), (2,3)\} \subset \overline{\mathbb{K}}^2$. In this case, $E^*_\lambda(G)$ is the set W seen in Examples 9.2.2 and 9.2.4, and the output we seek is a distinct coordinates representation of W, as discussed in Example 9.2.4.

Lemma 9.2.3. *There exists a randomized algorithm* Decompose$(\lambda, \mathscr{R})$*, which takes as input a partition λ of n with length ℓ and a zero-dimensional parametrization $\mathscr{R}$ of a set $G \subset \overline{\mathbb{K}}^\ell$; it returns a symmetric representation of $E^*_\lambda(G)$. The expected runtime is $O^{\sim}(D^2 n)$ operations in $\mathbb{K}$, with $D = \deg(\mathscr{R}) = |G|$.*

Proof. In the first step, we apply our algorithm Type_Of_Fiber from Lemma 9.2.1 where the input fiber is given not with coefficients in $\mathbb{K}$, but as the points described by $\mathscr{R}$. A general algorithmic principle, known as *dynamic evaluation*, allows us to do this as follows. Let $\mathscr{R} = ((q, v_1, \ldots, v_\ell), \mu)$, with q and the v_i's in $\mathbb{K}[y]$. We then call Type_Of_Fiber with input coordinates $(v_1, \ldots, v_\ell)$, and attempt to run the algorithm over the residue class ring $\mathbb{K}[y]/q$, as if q were irreducible.

If q is irreducible, $\mathbb{K}[y]/q$ is a field, and we encounter no problem. However, in general, $\mathbb{K}[y]/q$ is only a product of fields, so the algorithm may attempt to invert a zero-divisor. When this occurs, a "splitting" of the computation occurs. This amounts to discovering a non-trivial factorization of q. A direct solution then consists of running the algorithm again modulo the two factors that were discovered. Overall, this computes a sequence $(\mathscr{R}_i, \lambda_i, \boldsymbol{f}_i)_{1\le i\le N}$, where for $i = 1, \ldots, N$,

(i) $\mathscr{R}_i = ((q_i, v_{i,1}, \ldots, v_{i,\ell}), \mu_i)$ is a zero-dimensional parametrization that describes a set $F_i \subset F$. In addition F is the disjoint union of $F_1, \ldots, F_N$;

(ii) λ_i is a partition of n, of length ℓ_i;

(iii) $\boldsymbol{f}_i$ is a sequence of ℓ_i elements with entries in the residue class ring $\mathbb{K}[y]/q_i$;

(iv) for any $\boldsymbol{\varepsilon}$ in F_i, corresponding to a root τ of q_i, $\mathsf{Type_Of_Fiber}(\lambda, \boldsymbol{\varepsilon}) = (\lambda_i, \boldsymbol{f}_i(\tau))$.

Since Type_Of_Fiber takes time $O^{\sim}(n)$, this process takes time $O^{\sim}(D^2 n)$, with $D = \deg(\mathscr{R})$. The overhead $O^{\sim}(D^2)$ is the penalty incurred by a straightforward application of dynamic evaluation techniques.

For $i = 1, \ldots, r$, let $V_i = E_\lambda^{-1}(F_i)$, so that $W = \mathcal{S}_n(V)$ is the union of the orbits $W_i = \mathcal{S}_n(V_i)$. Then, from (iv) above we see that all points in W_i have type λ_i and that $(W_i)'_{\lambda_i}$ is the set $G_i = \{\boldsymbol{f}_i(\tau) \mid q_i(\tau) = 0\} \subset \overline{\mathbb{K}}^{\ell_i}$. Using the algorithm of [146, Proposition 1], we can compute a zero-dimensional parametrization $\mathscr{S}_i$ of G_i in time $O^{\sim}(D_i^2 n)$, with $D_i = \deg(\mathscr{R}_i)$. The total cost is thus $O^{\sim}(D^2 n)$.

The λ_i's may not be pairwise distinct. Up to changing indices, we may assume that $\lambda_1, \ldots, \lambda_s$ are representatives of the pairwise distinct values among them. Then, for $i = 1, \ldots, s$, we compute a zero-dimensional parametrization $\mathscr{T}_i$ that describes the union of those $V(\mathscr{S}_j)$, for j such that $\lambda_j = \lambda_i$. Using algorithm [146, Lemma 3], this takes a total of $O^{\sim}(D^2 n)$ operations in $\mathbb{K}$. Finally, we return $(\lambda_i, \mathscr{T}_i)_{1 \le i \le s}$. □

9.3 Some useful algorithms

In this section, we design some important algorithms which are needed to construct our main algorithm in the next section. The first algorithm called Symmetric_Coordinates takes an $\mathcal{S}_\lambda$-invariant polynomial and outputs its representation in the elementary symmetric functions. The second algorithm called Symmetric which turns an $\mathcal{S}_\lambda$-equivariant system into an $\mathcal{S}_\lambda$-invariant polynomials and keeps the same variety upto a localization.

9.3.1 $\mathcal{S}_\lambda$-invariant polynomials: the Symmetric_Coordinates algorithm

Let $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \ldots\, n_r^{\ell_r})$ be a partition of n having length ℓ, and, for $i = 1, \ldots, r$, let $\boldsymbol{e}_i = (e_{i,1}, \ldots, e_{i,\ell_i})$ be a set of ℓ_i new variables. Then, by Theorem 3.5.2, for any f in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^{\mathcal{S}_\lambda}$, there exists a unique $\bar{f}$ in $\mathbb{K}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r]$ with

$$f(\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r) = \bar{f}(\boldsymbol{\eta}_1, \ldots, \boldsymbol{\eta}_r), \tag{9.4}$$

where $\boldsymbol{\eta}_i = (\eta_{i,1}, \ldots, \eta_{i,\ell_i})$ is the vector of elementary symmetric polynomials in variables $\boldsymbol{Z}_i$. The goal of this subsection is to give an estimate on the cost of computing $\bar{f}$ from f.

Lemma 9.3.1. *There exists an algorithm* Symmetric_Coordinates(λ, f) *which, given a partition* λ *of* n *and* f *of degree at most* d *in* $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^{\mathcal{S}_\lambda}$*, returns* $\overline{f}$ *such that* $f = \overline{f}(\boldsymbol{\eta}_1, \ldots, \boldsymbol{\eta}_r)$*, using* $O\tilde{}(\binom{\ell+d}{d}^2)$ *operations in* $\mathbb{K}$*.*

The rest of this subsection is devoted to prove Lemma 9.3.1. Algorithm Symmetric_Coordinates is a slight generalization of the procedure described in the proof of Bläser and Jindal's algorithm [32, Theorem 4], which was written only for the case of $r = 1$, and for polynomials represented as straight-line programs.

The key to the algorithm is the following. Assume we know an integral domain $\mathbb{L}$ containing $\mathbb{K}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r]$, and vectors $\boldsymbol{\zeta}_1, \ldots, \boldsymbol{\zeta}_r$ of elements in $\mathbb{L}$, where for each i, $\boldsymbol{\zeta}_i = (\zeta_{i,1}, \ldots, \zeta_{i,\ell_i}) \in \mathbb{L}^{\ell_i}$ are the ℓ_i pairwise distinct roots (with respect to T) of

$$P_i(T, \boldsymbol{e}_i) = T^{\ell_i} - (e_{i,1} + \rho_{i,1})T^{\ell_i - 1} + \cdots + (-1)^{\ell_i}(e_{i,\ell_i} + \rho_{i,\ell_i}), \tag{9.5}$$

and where $\rho_{i,1}, \ldots, \rho_{i,\ell_i}$ are the elementary symmetric polynomials evaluated at $1, \ldots, \ell_i$. Then, $\bar{f}$ satisfies

$$\bar{f}(e_{1,1} + \rho_{1,1}, \ldots, e_{r,\ell_r} + \rho_{r,\ell_r}) = f(\boldsymbol{\zeta}_1, \ldots, \boldsymbol{\zeta}_r). \tag{9.6}$$

As in Bläser and Jindal's algorithm, we take for $\mathbb{L}$ a ring of multivariate power series, namely $\mathbb{L} = \mathbb{K}[[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r]]$.

First, we need to show the existence of the power series $\boldsymbol{\zeta}_i$. The following Lemma gives a sufficient condition when the roots of a polynomial $P(T, \boldsymbol{e}_i)$ are elements of the power series ring $\mathbb{L}$.

Lemma 9.3.2. [32, Lemma 14] *Let* $P(T, \boldsymbol{e}_i)$ *be a square free and monic polynomial in* T *variable. If all roots of* $P(T, \boldsymbol{0})$ *have multiplicity one, then the roots* $\boldsymbol{\zeta}(\boldsymbol{e}_i)$ *of* $P(T, \boldsymbol{e}_i)$ *can be expressed into power series in* $\mathbb{L}$*.*

For polynomial $P_i(T)$ in (9.5), one has $P_i(T, \boldsymbol{0}) = (T-1)\cdots(T-\ell_i)$ which has ℓ_i distinct roots. Thus the ℓ_i roots of $P_i(T)$ in (9.5) can be expressed as power series in $\boldsymbol{e}_i$.

Corollary 9.3.3. *For* $i = 1, \ldots, r$*,* $P_i(T, \boldsymbol{e}_i)$ *are polynomials given in* (9.5)*. Then there exists power series* $\boldsymbol{\zeta}_i = (\zeta_{i,1}, \ldots, \zeta_{i,\ell_i}) \in \mathbb{L}^{\ell_i}$ *such that* $P_i(\zeta_{i,k}, \boldsymbol{e}_i) = 0$ *for all* $i = 1, \ldots, r$ *and* $k = 1, \ldots, \ell_i$*.*

Now we use Newton's iteration to compute the requested power series roots $\boldsymbol{\zeta}_i = (\zeta_{i,1}, \ldots, \zeta_{i,\ell_i})$. In order to obtain the polynomial $\bar{f}$, we only need truncations of these roots at precision d; and then by equation (9.6), it suffices to substitute these degree d truncations to f.

To finish our proof of Lemma 9.3.1, we analyze the complexity for Symmetric_Coordinates algorithm. For $i = 1, \ldots, r$, we can obtain the truncation of $\boldsymbol{\zeta}_i$ using $O\tilde{}(\ell_i\binom{\ell_i+d}{d})$ operations in $\mathbb{K}$, where the factor $\binom{\ell_i+d}{d}$ accounts for the cost of multivariate power series

Algorithm 13 Symmetric_Coordinates(λ, f)

Input: a partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2} \dots n_r^{\ell_2})$ and a polynomial f in $\mathbb{K}[\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r]^{\mathcal{S}_\lambda}$
Output: a polynomial $\bar{f}$ in $\mathbb{K}[\boldsymbol{e}_1, \dots, \boldsymbol{e}_r]$ with $f(\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r) = \bar{f}(\boldsymbol{\eta}_1, \dots, \boldsymbol{\eta}_r)$,

1. for any i in $\{1, \dots, r\}$
   (a) construct $\rho_{i,1}, \dots, \rho_{i,\ell_i}$ are the elementary symmetric functions of $\boldsymbol{\zeta}_i = (1, \dots, \ell_i)$
   (b) build the polynomial $P_i(T, \boldsymbol{e}_i) = T^{\ell_i} - (e_{i,1} + \rho_{i,1})T^{\ell_i - 1} + \cdots + (-1)^{\ell_i}\,(e_{i,\ell_i} + \rho_{i,\ell_i})$
   (c) applying a Newton-Hensel lifting (in parameter T) to $P_i(T, \boldsymbol{e}_i)$ to lift $\boldsymbol{\zeta}_i$ to the truncation $\boldsymbol{\zeta}_i^{(d)}$ of degree $d = \deg(f)$
2. evaluate f at $(\boldsymbol{\zeta}_1^{(d)}, \dots, \boldsymbol{\zeta}_r^{(d)})$ to get a power series g in $\mathbb{K}[[\boldsymbol{e}_1, \dots, \boldsymbol{e}_r]]$
3. compute $\bar{f} = g(e_{1,1} - \rho_{1,1}, \dots, e_{r,1} - \rho_{r,\ell_r})$

arithmetic [125]. Taking all i's into account, this adds up to $O^{\sim}(\ell\binom{\ell+d}{d})$ arithmetic operations. We then evaluate f at these truncated power series. Since f has degree at most d, this can be done using $O(\binom{\ell+d}{d})$ $(+, \times)$ operations on ℓ-variate power series truncated in degree d, for a total of $O^{\sim}(\binom{\ell+d}{d}^2)$ operations in $\mathbb{K}$. This gives us $\bar{f}(e_{1,1} + \rho_{1,1}, \dots, e_{r,\ell_r} + \rho_{r,\ell_r})$. We then apply the translation $(e_{i,j})_{i,j} \leftarrow (e_{i,j} - \rho_{i,j})_{i,j}$ in order to obtain the polynomial $\bar{f}$, also at a cost of $O^{\sim}(\binom{\ell+d}{d}^2)$ operations in $\mathbb{K}$. Through successive multiplications, we incrementally compute the translates of all monomials of degree up to d and then, before combining, using the coefficients of $\bar{f}(e_{1,1} + \rho_{1,1}, \dots, e_{r,\ell_r} + \rho_{r,\ell_r})$.

Example 9.3.1. Consider $r = 2$ and $f = z_{1,1}^3 + z_{1,2}^3 + 2z_{2,1}z_{2,2} - 5$ in $\mathbb{K}[z_{1,1}, z_{1,2}, z_{2,1}, z_{2,2}]^{\mathcal{S}_2 \times \mathcal{S}_2}$. Then

$$P_1 = T^2 - (e_{1,1} + 3)T + e_{1,2} + 2 \text{ and } P_2 = T^2 - (e_{2,1} + 3)T + e_{2,2} + 2.$$

After applying Newton's iteration and then truncating the roots at precision 3 for $(e_{1,1}, e_{1,2})$ and precision 2 for $(e_{2,1}, e_{2,2})$, we get

$$\begin{aligned}
z_{1,1} &= -6e_{1,1}^3 + 13e_{1,1}^2e_{1,2} - 9e_{1,1}e_{1,2}^2 + 2e_{1,2}^3 + 2e_{1,1}^2 - 3e_{1,1}e_{1,2} + e_{1,2}^2 - e_{1,1} + e_{1,2} + 1,\\
z_{1,2} &= 6e_{1,1}^3 - 13e_{1,1}^2e_{2,1} + 9e_{1,1}e_{1,2}^2 - 2e_{1,2}^3 - 2e_{1,1}^2 + 3e_{1,1}e_{1,2} - e_{1,2}^2 + 2e_{1,1} - e_{1,2} + 2,\\
z_{2,1} &= 2e_{2,1}^2 - 3e_{2,1}e_{2,2} + e_{2,2}^2 - e_{2,1} + e_{2,2} + 1,\\
z_{2,2} &= -2e_{2,1}^2 + 3e_{2,1}e_{2,2} - e_{2,2}^2 + 2e_{1,2} - e_{2,2} + 2.
\end{aligned}$$

We evaluate f at these truncated power series. Then truncating the result at precision 3 for $(e_{1,1}, e_{1,2})$ and precision 2 for $(e_{2,1}, e_{2,2})$ gives

$$\overline{f}(e_{1,1} + 3, e_{1,2} + 2, e_{2,1} + 3, e_{2,2} + 2) = e_{1,1}^3 + 9e_{1,1}^2 - 3e_{1,1}e_{1,2} + 21e_{1,1} - 9e_{1,2} + 2e_{2,2} + 10.$$

Finally, we use the substitution $e_{1,1} \leftarrow e_{1,1} - 3, e_{1,2} \leftarrow e_{1,2} - 2, e_{2,1} \leftarrow e_{2,1} - 3, e_{2,2} \leftarrow e_{2,2} - 2$ to obtain

$$\overline{f} = e_{1,1}^3 - 3e_{1,1}e_{1,2} + 2e_{2,2} - 5.$$

9.3.2 $\mathcal{S}_\lambda$-equivariant polynomials: the Symmetrize algorithm

As before we let $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \dots\, n_r^{\ell_r})$ denote a partition of n of length $\ell = \ell_1 + \cdots + \ell_r$. The aim of this subsection is to define $\mathcal{S}_\lambda$-*equivariant* systems of polynomials and give a detailed description of an algorithm, called Symmetrize, that turns an $\mathcal{S}_\lambda$-equivariant system into one which is $\mathcal{S}_\lambda$-invariant. Recall that the group $\mathcal{S}_\lambda$ is defined in Definition 9.1.4. The elements of $\mathcal{S}_\lambda$ are permutations of $\{1, \dots, \ell\}$, as explained in Section 9.1.

Definition 9.3.4. *Consider a sequence of polynomials $\boldsymbol{q} = (q_1, \dots, q_\ell)$ in $\mathbb{K}[\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r]$. We say that $\boldsymbol{q}$ is* $\mathcal{S}_\lambda$-equivariant *if for any σ in $\mathcal{S}_\lambda$ and i in $(1, \dots, \ell)$, we have $\sigma(q_i) = q_{\sigma(i)}$, or equivalently,*

$$q(z_{\sigma(1)}, \dots, z_{\sigma(\ell)}) = q_{\sigma(i)}(z_1, \dots, z_\ell).$$

In geometric terms, the zero-set $V(\boldsymbol{q}) \subset \overline{\mathbb{K}}^\ell$ of such a system is $\mathcal{S}_\lambda$-invariant, even though the equations themselves may not be invariant. In what follows, we describe how to derive equations $\boldsymbol{p} = (p_1, \dots, p_\ell)$ that generate the same ideal as $\boldsymbol{q}$ (in a suitable localization of $\mathbb{K}[\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r]$) and are actually $\mathcal{S}_\lambda$-invariant. We will need an assumption, discussed below, that $z_i - z_k$ divides $q_i - q_k$ for all pairwise distinct indices i, k.

Example 9.3.2. Let $n = 3$ and $\lambda = (1^2\, 2^1)$ so $r = 2$, $\ell_1 = 2$, $\ell_2 = 1$ and $\ell = 3$; we have $\mathcal{S}_\lambda = \mathcal{S}_2 \times \mathcal{S}_1$. We take $\boldsymbol{q} = (q_1, q_2, q_3)$, where

$$\begin{aligned} q_1 &= z_2 z_3^2 (z_1 + z_2 + 2z_3) + z_1 z_2 z_3^2, \\ q_2 &= z_1 z_3^2 (z_1 + z_2 + 2z_3) + z_1 z_2 z_3^2, \\ q_3 &= z_1 z_2 z_3 (z_1 + z_2 + 2z_3) + z_1 z_2 z_3^2. \end{aligned}$$

These polynomials satisfy both the equivariance property and the divisibility property.

Our procedure will produce the following polynomials:

$$\begin{aligned} p_1 &= (z_1 + z_2 + 2z_3) z_3, \\ p_2 &= (z_1 + z_2 + 2z_3) z_2 z_3 + (z_1 + z_2 + 2z_3) z_1 z_3, \\ p_3 &= z_1 z_2 z_3 (z_1 + z_2 + 2z_3) + z_1 z_2 z_3^2. \end{aligned}$$

The polynomials (p_1, p_2, p_3) are symmetric in (z_1, z_2) and (z_3), that is, are $\mathcal{S}_2 \times \mathcal{S}_1$-invariant, and they generate the same ideal as (q_1, q_2, q_3) in the localization $\mathbb{K}[z_1, z_2, z_3]_{(z_1 - z_2)(z_1 - z_3)(z_2 - z_3)}$.

In order to construct a set of invariant generators we make use of *divided differences* of $\boldsymbol{q} = (q_1, \dots, q_\ell)$.

Definition 9.3.5. *Consider a system $\boldsymbol{q} = (q_1, \dots, q_\ell)$ of $\mathcal{S}_\lambda$-equivariant. The* divided differences *are defined as $q_{\{i\}} = q_i$ for i in $\{1, \dots, \ell\}$, and for each set of k distinct integers $I := \{i_1, \dots, i_k\} \subset \{1, \dots, \ell\}$, with $k > 2$,*

$$q_I = \frac{q_{\{i_1, \dots, i_{r-1}, i_{r+1}, \dots, i_k\}} - q_{\{i_1, \dots, i_{q-1}, i_{q+1}, \dots, i_k\}}}{z_{i_r} - z_{i_q}}, \tag{9.7}$$

for any choice of i_r, i_q in I, with $i_r \neq i_q$.

It is known (see e.g. [69, Theorem 1]) that the recursive construction above defines q_I unambiguously (independently of the choice of i_r, i_q). Another useful property of divided differences is the following:

(i) if $z_i - z_k$ divides $q_i - q_k$ for all $1 \leq i < k \leq \ell$, then q_I is a polynomial for all $I \subset \{1, \ldots, \ell\}$.

The following proposition gives our construction of the polynomials $\boldsymbol{p}$. Recall from Section 3.5 that, for $i \geq 0$, $\eta_i(y_1, \ldots, y_s)$ is the degree i elementary symmetric function in variables $(y_1, \ldots, y_s)$. Before state our main result of this section, we start with some rather straightforward lemmas.

Lemma 9.3.6. *Consider an $\mathcal{S}_\lambda$-equivariant sequence $\boldsymbol{q} = (q_1, \ldots, q_\ell)$ in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]$. Then, for any $I \subset \{1, \ldots, \ell\}$ and any σ in $\mathcal{S}_\lambda$, we have $\sigma(q_I) = q_{\sigma(I)}$.*

Proof. By induction on the size of I. □

Lemma 9.3.7. *Consider a sequence $\boldsymbol{q} = (q_1, \ldots, q_\ell)$ in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]$, and suppose that*

(i) *$z_i - z_j$ divides $q_i - q_j$ for $1 \leq i < j \leq \ell$,*

(ii) *$\boldsymbol{q}$ is $\mathcal{S}_\lambda$-equivariant.*

Then, for k in $\{1, \ldots, r\}$ and s in $\{1, \ldots, \ell_k\}$, the polynomial $\sum_{i=\tau_k+1}^{\tau_k+s} q_{\{i,\tau_k+s+1,\ldots,\ell\}}$ is invariant under any permutation of $\{z_{\tau_k+1}, \ldots, z_{\tau_k+s}\}$.

Proof. For any $\sigma \in \mathcal{S}_\lambda$ permuting only $\{z_{\tau_k+1}, \ldots, z_{\tau_k+s}\}$, we have,

$$\sigma\Big(\sum_{i=1}^{\tau_k+s} q_{\{i,\tau_k+s+1,\ldots,\ell\}}\Big) = \sum_{i=\tau_k+1}^{\tau_k+s} \sigma\Big(q_{\{i,\tau_k+s+1,\ldots,\ell\}}\Big) = \sum_{i=\tau_k+1}^{\tau_k+s} q_{\{\sigma(i),\tau_k+s+1,\ldots,\ell\}},$$

by using the Lemma 9.3.6. Since σ permutes $\{z_{\tau_k+1}, \ldots, z_{\tau_k+s}\}$ and the last sum runs over all $i = \tau_k + 1, \ldots, \tau_k + s$, it equals $\sum_{i=\tau_k+1}^{\tau_k+s} q_{\{i,\tau_k+s+1,\ldots,\ell\}}$. □

We can now give one of our main result as the following.

Proposition 9.3.8. *Suppose the sequence $\boldsymbol{q} = (q_1, \ldots, q_\ell)$ in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^\ell$ is $\mathcal{S}_\lambda$-equivariant and satisfies $z_i - z_k$ divides $q_i - q_k$ for $1 \leq i < k \leq \ell$.*

For $0 \leq k \leq r-1$ and $1 \leq j < \ell_{k+1}$, define

$$p_{\tau_{k+1}} = \sum_{i=\tau_k+1}^{\tau_{k+1}} q_{\{i,\tau_{k+1}+1,\ldots,\tau_r\}},$$

$$p_{\tau_k+j} = \sum_{s=1}^{j} \eta_{j-s}(z_{\tau_k+s+2}, \ldots, z_{\tau_{k+1}}) \Big(\sum_{i=\tau_k+1}^{\tau_k+s} q_{\{i,\tau_k+s+1,\ldots,\tau_r\}} \Big).$$

Then the sequence

$$\boldsymbol{p} = \left(p_1, \ldots, p_{\tau_1},\, p_{\tau_1+1}, \ldots, p_{\tau_2},\ \ldots, p_{\tau_{r-1}+1}, \ldots, p_{\tau_r}\right)$$

is in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^{\mathcal{S}_\lambda}$. *If all* q_i*'s have degree at most* d, *then* $\deg(p_i) \leq d - \ell + i$ *holds for* $i = 1, \ldots, \ell$.

Proof. The degree bound comes by inspection. The fact that all entries of $\boldsymbol{p}$ are polynomials follows from our first assumption. Proving that they are $\mathcal{S}_\lambda$-invariant requires more work, as we have to deal with numerous cases. While most are straightforward, the last case does involve nontrivial calculations.

Fix $k \in \{0, \ldots, r-1\}$. We first prove that for

- $s \in \{1, \ldots, \ell_{k+1}\}$,
- $i \in \{\tau_k + 1, \ldots, \tau_k + s\}$, and
- $m \in \{0, \ldots, r-1\}$, with $m \neq k$,

the term $q_{\{i, \tau_k+s+1, \ldots, \tau_r\}}$ is symmetric in $\{z_{\tau_m+1}, \ldots, z_{\tau_{m+1}}\}$. Indeed, consider a permutation $\sigma \in \mathcal{S}_\lambda$ that acts on $\{z_{\tau_m+1}, \ldots, z_{\tau_{m+1}}\}$ only. By Lemma 9.3.6,

$$\sigma(q_{\{i, \tau_k+s+1, \ldots, \tau_r\}}) = q_{\{\sigma(i), \sigma(\tau_k+s+1), \ldots, \sigma(\tau_r)\}}.$$

If $m < k$, then all indices $i, \tau_k + s + 1, \ldots, \tau_r$ are left invariant by σ while for $m > k$, $[\sigma(i), \sigma(\tau_k + s + 1), \ldots, \sigma(\tau_r)]$ is a permutation of $[i, \tau_k + s + 1, \ldots, \tau_r]$. In both cases, $q_{\{\sigma(i), \sigma(\tau_k+s+1), \ldots, \sigma(\tau_r)\}} = q_{\{i, \tau_k+s+1, \ldots, \tau_r\}}$, as claimed.

Consider first the invariance of $p_{\tau_{k+1}}$. By Lemma 9.3.7, the sum $\sum_{i=\tau_k+1}^{\tau_{k+1}} q_{\{i, \tau_{k+1}+1, \ldots, \tau_r\}}$ is symmetric in $\{z_{\tau_k+1}, \ldots, z_{\tau_{k+1}}\}$. Next, for i in $\{\tau_k + 1, \ldots, \tau_{k+1}\}$ and m in $\{0, \ldots, r-1\}$, with $m \neq k$, each term $q_{\{i, \tau_{k+1}+1, \ldots, \tau_r\}}$ is symmetric in $\{z_{\tau_m+1}, \ldots, z_{\tau_{m+1}}\}$, making use of the previous paragraph with $s = \ell_{k+1}$. As a result, $p_{\tau_{k+1}}$ is $\mathcal{S}_\lambda$-invariant.

Now, for j in $\{1, \ldots, \ell_{k+1} - 1\}$ and σ in $\mathcal{S}_\lambda$, we prove that $\sigma(p_{\tau_k+j}) = p_{\tau_k+j}$. Assume first that σ acts only on $\{z_{\tau_m+1}, \ldots, z_{\tau_{m+1}}\}$, for some m in $\{0, \ldots, r-1\}$ with $m \neq k$. For s in $\{1, \ldots, j\}$, the polynomial $\eta_{j-s}(z_{\tau_k+s+2}, \ldots, z_{\tau_{k+1}})$ depends only on $\{z_{\tau_k+1}, \ldots, z_{\tau_{k+1}}\}$ and so is σ-invariant. Using our earlier argument we see that for i in $\{\tau_k + 1, \ldots, \tau_k + s\}$ the divided difference $q_{\{i, \tau_k+s+1, \ldots, \tau_r\}}$ is σ-invariant. As a result, p_{τ_k+j} itself is σ-invariant.

It remains to prove that p_{τ_k+j} is σ-invariant for a permutation σ of $\{\tau_k + 1, \ldots, \tau_{k+1}\}$. We do this first for $\sigma = (\tau_k + 1, \tau_k + 2)$, by proving that all summands in the definition of p_{τ_k+j} are σ-invariant. For any s in $\{2, \ldots, j\}$, $\eta_{j-s}(z_{\tau_k+s+2}, \ldots, z_{\tau_{k+1}})$ does not depend on $(z_{\tau_k+1}, z_{\tau_k+2})$, so it is σ-invariant. For s in $\{2, \ldots, j\}$, the sum $\sum_{i=\tau_k+1}^{\tau_k+s} q_{\{i, \tau_k+s+1, \ldots, \tau_r\}}$ is symmetric in $(\tau_k + 1, \tau_k + 2)$, since σ just permutes two terms in the sum while for $s = 1$, $q_{\{\tau_k+1, \tau_k+2, \ldots, \tau_r\}}$ is symmetric in $(z_{\tau_k+1}, z_{\tau_k+2})$ by Lemma 9.3.6. Thus, our claim is proved for $\sigma = (\tau_k + 1, \tau_k + 2)$.

It remains to prove that p_{τ_k+j} is invariant in $(z_{\tau_k+2},\dots,z_{\tau_{k+1}})$. For any $t=1,\dots,j$, set

$$p_{\tau_k+j,t}=\sum_{s=t}^{j}\eta_{j-s}(z_{\tau_k+t+2},\dots,z_{\tau_{k+1}})\Big(\sum_{i=\tau_k+1}^{\tau_k+s}q_{\{i,\tau_k+s+1,\dots,\tau_r\}}\Big). \tag{9.8}$$

Then $p_{\tau_k+j}=p_{\tau_k+j,1}$ and we have the recursive identity

$$p_{\tau_k+j,t-1}=p_{\tau_k+j,t}+\eta_{j-t+1}(z_{\tau_k+t+1},\dots,z_{\tau_{k+1}})\Big(\sum_{i=\tau_k+1}^{\tau_k+t-1}q_{\{i,\tau_k+t,\dots,\tau_r\}}\Big). \tag{9.9}$$

For any t, set $\boldsymbol{z}_{:t}=(z_{\tau_k+1},\dots,z_{\tau_k+t})$ and $\boldsymbol{z}_{t:}=(z_{\tau_k+t},\dots,z_{\tau_{k+1}})$. We will show that for $t=1,\dots,j$, the polynomial $p_{\tau_k+j,t}$ satisfies:

$$p_{\tau_k+j,t}\text{ is block symmetric in }\boldsymbol{z}_{:t}\text{ and }\boldsymbol{z}_{t+1:} \tag{9.10}$$

Taking $t=1$ implies that $p_{\tau_k+j}=p_{\tau_k+j,1}$ is symmetric in $\boldsymbol{z}_{2:}=(z_{\tau_k+2},\dots,z_{\tau_{k+1}})$, as claimed.

To prove statement (9.10) we use decreasing induction on $t=j,\dots,1$. The statement is true when $t=j$ since in this case

$$p_{\tau_k+j,j}=\sum_{i=\tau_k+1}^{\tau_k+j}q_{\{i,\tau_k+j+1,\dots,\tau_r\}},$$

which is symmetric in $\boldsymbol{z}_{:j}$ by Lemma 9.3.7, while each summand $q_{\{i,\tau_k+j+1,\dots,\tau_r\}}$ is symmetric in $\boldsymbol{z}_{j+1:}$ by Lemma 9.3.6. Assume now that (9.10) is true for some index t in $\{2,\dots,j\}$; we show that it also holds for $t-1$. That is, we have $p_{\tau_k+j,t}$ is block symmetric in $\boldsymbol{z}_{:t}$ and $\boldsymbol{z}_{t+1:}$ and need to show that $p_{\tau_k+j,t-1}$ is block symmetric in $\boldsymbol{z}_{:t-1}$ and $\boldsymbol{z}_{t:}$.

From Lemma 9.3.7, we have that $\sum_{i=\tau_k+1}^{\tau_k+t-1}q_{\{i,\tau_k+t,\dots,\tau_r\}}$ is symmetric in $\boldsymbol{z}_{:t-1}$. Furthermore, from our induction hypothesis, the polynomial $p_{\tau_k+j,t}$ is symmetric in $\boldsymbol{z}_{:t-1}$, while $\eta_{j-t+1}(z_{\tau_k+t+1},\dots,\tau_{k+1})$ depends only on $\boldsymbol{z}_{t:}$. Thus, in view of (9.9), we see that $p_{\tau_k+j,t-1}$ is symmetric in $\boldsymbol{z}_{:t-1}$. It remains to prove that it is also symmetric in $\boldsymbol{z}_{t:}$.

We will prove this by showing $\sigma(p_{\tau_k+j,t-1})=p_{\tau_k+j,t-1}$ for any $\sigma=(\tau_k+t+1,\tau_k+\epsilon)$ with $\epsilon\in\{t,t+2,\dots,\ell_{k+1}\}$. For any such σ with $t+2\le\epsilon\le\ell_{k+1}$, our induction hypothesis implies that $\sigma(p_{\tau_k+j,t})=p_{\tau_k+j,t}$, while $\sigma(\eta_{j-t+1}(z_{\tau_k+t+1},\dots,\tau_{k+1}))=\eta_{j-t+1}(z_{\tau_k+t+1},\dots,\tau_{k+1})$ and $\sigma\Big(q_{\{i,\tau_k+t,\dots,\tau_r\}}\Big)=q_{\{i,\tau_k+t,\dots,\tau_r\}}$ hold for all i. Together with (9.9), we get $\sigma(p_{\tau_k+j,t-1})=p_{\tau_k+j,t-1}$. Finally, if $\sigma=(\tau_k+t+1,\tau_k+t)$, then we have

$$\sigma(\eta_{j-t+1}(z_{\tau_k+t+1},\dots,\tau_{k+1}))=\eta_{j-t+1}(z_{\tau_k+t},z_{\tau_k+t+2},\dots,\tau_{k+1})$$

and $\sigma\Big(q_{\{i,\tau_k+t,\dots,\tau_r\}}\Big)=q_{\{i,\tau_k+t,\dots,\tau_r\}}$ for all $i=\tau_k+1,\dots,\tau_k+t-1$. Notice that

$$\eta_{j-t+1}(z_{\tau_k+t},z_{\tau_k+t+2},\dots,\tau_{k+1})-\eta_{j-t+1}(z_{\tau_k+t+1},\dots,\tau_{k+1})=\\(z_{\tau_k+t}-z_{\tau_k+t+1})\,\eta_{j-t}(z_{\tau_k+t+2},\dots,z_{\tau_{k+1}}).$$

Therefore,

$$\begin{aligned}\sigma(p_{\tau_k+j,t-1}) - p_{\tau_k+\hat{\imath},t-1} &= \sigma(p_{\tau_k+j,t}) - p_{\tau_k+j,t} \\ &\quad + (z_{\tau_k+t} - z_{\tau_k+t+1})\,\eta_{j-t}(z_{\tau_k+t+2},\ldots,z_{\tau_{k+1}})\Big(\sum_{i=\tau_k+1}^{\tau_k+t-1} q_{\{i,\tau_k+t,\ldots,\tau_r\}}\Big) \\ &= \sigma(p_{\tau_k+j,t}) - p_{\tau_k+j,t} + \eta_{j-t}(z_{\tau_k+t+2},\ldots,z_{\tau_{k+1}}) \\ &\quad \Big(\sum_{i=\tau_k+1}^{\tau_k+t-1} (q_{\{i,\tau_k+t+1,\tau_k+t+2,\ldots,\tau_r\}} - q_{\{i,\tau_k+t,\tau_k+t+2,\ldots,\tau_r\}})\Big), \end{aligned} \tag{9.11}$$

where the last equality follows from the definition of divided differences. In particular,

$$\sigma(p_{\tau_k+j,j-1}) - p_{\tau_k+j,j-1} = \sigma(p_{\tau_k+j,j}) - p_{\tau_k+j,j} + \sum_{i=\tau_k+1}^{\tau_k+j-1} (q_{\{i,\tau_k+j+1,\ldots,\tau_r\}} - q_{\{i,\tau_k+j,\tau_k+j+2,\ldots,\tau_r\}}).$$

Moreover, since $p_{\tau_k+j,j} = \sum_{i=\tau_k+1}^{\tau_k+j} q_{\{i,\tau_k+j+1,\ldots,\tau_r\}}$, then when $\sigma = (\tau_k+j+1, \tau_k+j)$, we have

$$\sigma(p_{\tau_k+j,j}) - p_{\tau_k+j,j} = \sum_{i=\tau_k+1}^{\tau_k+j-1} (q_{\{i,\tau_k+j,\tau_k+j+2,\ldots,\tau_r\}} - q_{\{i,\tau_k+j+1,\ldots,\tau_r\}}).$$

This implies that $\sigma(p_{\tau_k+j,j-1}) - p_{\tau_k+j,j-1} = 0$.

When $t \le j-1$, from equation (9.9), taken at index $t+1$, if $\sigma = (\tau_k+t+1, \tau_k+t)$, we also have

$$\sigma(p_{\tau_k+j,t}) = \sigma(p_{\tau_k+j,t+1}) + \eta_{j-t}(z_{\tau_k+t+2},\ldots,z_{\tau_{k+1}})\Big(\sum_{i=\tau_k+1}^{\tau_k+t-1} q_{\{i,\tau_k+t,\tau_k+t+2,\ldots,\tau_r\}} + q_{\{\tau_k+t,\tau_k+t+1,\ldots,\tau_{k+1}\}}\Big).$$

Then, by subtraction:

$$\begin{aligned}\sigma(p_{\tau_k+j,t}) - p_{\tau_k+j,t} = \sigma(p_{\tau_k+j,t+1}) - p_{\tau_k+j,t+1} + \eta_{j-t}(z_{\tau_k+t+2},\ldots,z_{\tau_{k+1}}) \\ \Big(\sum_{i=\tau_k+1}^{\tau_k+t-1} (q_{\{i,\tau_k+t,\tau_k+t+2,\ldots,\tau_r\}} - q_{\{i,\tau_k+t+1,\ldots,\tau_r\}})\Big)\end{aligned}$$

and so

$$\begin{aligned}\sigma(p_{\tau_k+j,t+1}) - p_{\tau_k+j,t+1} =& \sigma(p_{\tau_k+j,t}) - p_{\tau_k+j,t} + \eta_{j-t}(z_{\tau_k+t+2},\ldots,z_{\tau_{k+1}}) \\ & \Big(\sum_{i=\tau_k+1}^{\tau_k+t-1} (q_{\{i,\tau_k+t+1,\ldots,\tau_r\}} - q_{\{i,\tau_k+t,\tau_k+t+2,\ldots,\tau_r\}})\Big).\end{aligned} \tag{9.12}$$

Combining (9.11) and (9.12) gives $\sigma(p_{\tau_k+j,t-1}) - p_{\tau_k+j,t-1} = \sigma(p_{\tau_k+j,t+1}) - p_{\tau_k+j,t+1}$. By induction, we have that $p_{\tau_k+j,t+1}$ is symmetric in $\boldsymbol{z}_{:t+1}$ and so $\sigma(p_{\tau_k+j,t+1}) = p_{\tau_k+j,t+1}$ for $\sigma = (\tau_k+t+1, \tau_k+t)$ which in turn implies that $\sigma(p_{\tau_k+j,t-1}) = p_{\tau_k+j,t-1}$. This gives our result. □

In addition, we will show that $\boldsymbol{q}$ can be written as a linear combination of $\boldsymbol{p}$, that is, we can find an $\ell \times \ell$ matrix polynomial $\boldsymbol{U}$ such that $\boldsymbol{pU} = \boldsymbol{q}$. The construction of $\boldsymbol{U}$ proceeds as follows. Let $\boldsymbol{M}$ be the block-diagonal matrix with blocks $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_r$ given by,

$$\boldsymbol{M}_{k+1} = \begin{pmatrix} 1 & \eta_1(z_{\tau_k+3}, \ldots, z_{\tau_{k+1}}) & \eta_2(z_{\tau_k+3}, \ldots, z_{\tau_{k+1}}) & \cdots & \eta_{\ell_{k+1}-2}(z_{\tau_k+3}, \ldots, z_{\tau_{k+1}}) & 0 \\ 0 & 1 & \eta_1(z_{\tau_k+4}, \ldots, z_{\tau_{k+1}}) & \cdots & \eta_{\ell_{k+1}-3}(z_{\tau_k+4}, \ldots, z_{\tau_{k+1}}) & 0 \\ 0 & 0 & 1 & \cdots & \eta_{\ell_{k+1}-4}(z_{\tau_k+5}, \ldots, z_{\tau_{k+1}}) & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Note that $\det(\boldsymbol{M}_{k+1}) = 1$ for all $0 \leq k \leq r-1$ and hence $\det(\boldsymbol{M}) = 1$.

For a non-negative integer u, denote by $\boldsymbol{I}_u$ the identity matrix of size u and by $\boldsymbol{0}$ a zero matrix. Then for $k = 0, \ldots, r-1$ and $j = 1, \ldots, \ell_{k+1}$, we define the following $\tau_r \times \tau_r$ polynomial matrices. Set $\boldsymbol{B}_{\tau_0+1} = \boldsymbol{I}_{\tau_r}$, $\boldsymbol{C}_{\tau_0+1} = \boldsymbol{I}_{\tau_r}$, $\boldsymbol{D}_{\tau_0+j} = \boldsymbol{I}_{\tau_r}$, and

$$\boldsymbol{B}_{\tau_k+j} = \left(\begin{array}{c|c|c} \boldsymbol{I}_{\tau_k} & \boldsymbol{0} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{E}_{k,j} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{\tau_r - \tau_{k+1}} \end{array}\right), \text{ with } \boldsymbol{E}_{k,j} = \left(\begin{array}{c|c|c} & z_{\tau_k+j} - z_{\tau_k+1} & \\ \boldsymbol{I}_{j-1} & \vdots & \boldsymbol{0} \\ & z_{\tau_k+j} - z_{\tau_k+j-1} & \\ \hline 0 \quad \ldots \quad 0 & -1 & \boldsymbol{0} \\ \hline \boldsymbol{0} & 0 & \boldsymbol{I}_{\ell_{k+1}-j} \end{array}\right),$$

$$\boldsymbol{C}_{\tau_k+j} = \left(\begin{array}{c|c|c} \boldsymbol{I}_{\tau_k} & \boldsymbol{0} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{F}_{k,j} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{\tau_r - \tau_{k+1}} \end{array}\right), \text{ with } \boldsymbol{F}_{k,j} = \left(\begin{array}{c|c|c} \mathbf{diag}(z_{\tau_k+j} - z_{\tau_k+t})_{t=1}^{j-1} & \boldsymbol{0} & \boldsymbol{0} \\ \hline \frac{-1}{j} \quad \ldots \quad \frac{-1}{j} & \frac{-1}{j} & \boldsymbol{0} \\ \hline \boldsymbol{0} & 0 & \boldsymbol{I}_{\ell_{k+1}-j} \end{array}\right),$$

$$\boldsymbol{D}_{\tau_k+j} = \left(\begin{array}{c|c|c} \mathbf{diag}(z_{\tau_k+j} - z_t)_{t=1}^{\tau_k} & \boldsymbol{0} & \boldsymbol{0} \\ \hline \boldsymbol{G}_{k,j} & \boldsymbol{I}_{\ell_{k+1}} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{\tau_r - \tau_{k+1}} \end{array}\right), \ \boldsymbol{G}_{k,j} : j^{th} \text{ row is } (1, \ldots, 1), \text{ rest zeros.}$$

Then we have the following.

Proposition 9.3.9. *Suppose the sequence $\boldsymbol{q} = (q_1, \ldots, q_\ell)$ in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^\ell$ satisfies the conditions of Proposition 9.3.8. Let $\Delta = \prod_{1 \leq i < j \leq \ell}(z_i - z_j)$ be the Vandermonde determinant associated with $z_1, \ldots, z_\ell$. Then the matrix $\boldsymbol{U}$ in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^{\ell \times \ell}$, defined by*

$$\boldsymbol{M} \cdot \boldsymbol{U} = \left(\prod_{k=0}^{r-1} \prod_{j=1}^{\ell_{k+1}} \boldsymbol{B}_{\tau_k+j} \, \boldsymbol{C}_{\tau_k+j} \, \boldsymbol{D}_{\tau_k+j} \right)$$

has determinant a unit in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r, 1/\Delta]$ and satisfies $\boldsymbol{pU} = \boldsymbol{q}$.

Proof. The proof follows by induction. Define the row vector

$$\boldsymbol{h} = \left(h_{\tau_0+1}, \ldots, h_{\tau_1}, \ldots, h_{\tau_{r-1}+1}, \ldots, h_{\tau_r}\right)$$

where, for $k = 0, \ldots, r-1$ and $j = 1, \ldots, \ell_{k+1}$,

$$h_{\tau_k+j} = \sum_{i=\tau_k+1}^{\tau_k+j} q_{\{i,\tau_k+j+1,\ldots,\tau_r\}}. \tag{9.13}$$

Then, for all $i = 1, \ldots, m$, $k = 0, \ldots, r-1$, $p_{\tau_k+\ell_{k+1}} = h_{\tau_k+\ell_{k+1}}$, and for $j = 1, \ldots, \ell_{k+1}-1$,

$$p_{\tau_k+j} = \sum_{s=1}^{j} \eta_{j-s}(z_{\tau_k+s+2}, \ldots, z_{\tau_{k+1}})\, h_{\tau_k+s}.$$

Therefore, $\boldsymbol{h} = \boldsymbol{p}\,\boldsymbol{M}$. Furthermore, $\det(\boldsymbol{M}) = 1$ and $\boldsymbol{N} = \boldsymbol{M}^{-1}$ is also a polynomial matrix in $\mathbb{K}[\boldsymbol{Z}]$ with $\det(\boldsymbol{N}) = 1$.

We construct a matrix $\boldsymbol{J}$ which defines the column operations converting $\boldsymbol{h}$ into $\boldsymbol{q}$ as follows.

$$\boldsymbol{J} = \prod_{k=0}^{r-1} \prod_{j=1}^{\ell_{k+1}} \boldsymbol{B}_{\tau_k+j}\, \boldsymbol{C}_{\tau_k+j}\, \boldsymbol{D}_{\tau_k+j} \quad \in \quad \mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^{\tau_r \times \tau_r}.$$

We will prove that this matrix satisfies $\boldsymbol{q} = \boldsymbol{h}\,\boldsymbol{J}$. Note first that, for $k = 0, \ldots, r-1$ and $j = 1, \ldots, \ell_{k+1}$ we have

- $\det(\boldsymbol{B}_{\tau_k+j}) = \det(\boldsymbol{E}_{k,j}) = -1$,
- $\det(\boldsymbol{C}_{\tau_k+j}) = \det(\boldsymbol{F}_{k,j}) = \frac{-1}{j} \prod_{t=1}^{j-1} (z_{\tau_k+j} - z_t)$, and
- $\det(\boldsymbol{D}_{\tau_k+j}) = \prod_{t=1}^{\tau_k} (z_{\tau_k+j} - z_t)$.

This implies that

$$\det(\boldsymbol{J}) = \alpha \prod_{k=0}^{r-1} \prod_{j=1}^{\ell_{k+1}} \prod_{t=1}^{j-1} (z_{\tau_k+j} - z_t) \prod_{t=1}^{\tau_k} (z_{\tau_k+j} - z_t) = \alpha\Delta \text{ for some } \alpha \in \mathbb{K}_{\neq 0}.$$

Define $\boldsymbol{U} = \boldsymbol{N}\,\boldsymbol{J}$. Then $\boldsymbol{p} = \boldsymbol{q}\,\boldsymbol{U}$, and $\det(\boldsymbol{U})$ is a unit in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r, 1/\Delta]$, as claimed.

It remains to prove $\boldsymbol{q} = \boldsymbol{h}\,\boldsymbol{J}$. For $s = 0, \ldots, \tau_r$, define

$$\boldsymbol{q}_s = \left(q_{\{1,s+1,\ldots,\tau_r\}} \quad \ldots \quad q_{\{s,s+1,\ldots,\tau_r\}} \quad h_{s+1} \quad \ldots \quad h_{\tau_r}\right),$$

so that for $s = 0$ we have $\boldsymbol{q}_0 = \boldsymbol{h}$, whereas for $s = \tau_r$ we have $\boldsymbol{q}_{\tau_r} = \boldsymbol{q}$. We prove the following: for k in $\{0, \ldots, r-1\}$ and j in $\{1, \ldots, \ell_k\}$,

$$\boldsymbol{q}_{\tau_k+j} = \boldsymbol{q}_{\tau_k+j-1} \boldsymbol{B}_{\tau_k+j}\, \boldsymbol{C}_{\tau_k+j}\, \boldsymbol{D}_{\tau_k+j}. \tag{9.14}$$

Our claim $\boldsymbol{q} = \boldsymbol{h}\,\boldsymbol{J}$ then follows from a direct induction, taking into account the values of $\boldsymbol{q}_0$ and $\boldsymbol{q}_{\tau_r}$ given above.

Take k in $\{0, \dots, r-1\}$ and j in $\{1, \dots, \ell_k\}$. Right-multiplying $\boldsymbol{q}_{\tau_k+j-1}$ by $\boldsymbol{B}_{\tau_k+j}$ only affects the entry at index $\tau_k + j$. It replaces h_{τ_k+j} by

$$\sum_{i=1}^{j-1} q_{\{\tau_k+i,\tau_k+j,\dots,\tau_r\}}(z_{\tau_k+j} - z_{\tau_k+i}) \quad - \quad h_{\tau_k+j}.$$

Using the defining relation of divided differences, we get

$$q_{\{\tau_k+i,\tau_k+j,\dots,\tau_r\}}(z_{\tau_k+j} - z_{\tau_k+i}) = q_{\{\tau_k+i,\tau_k+j+1,\dots,\tau_r\}} - q_{\{\tau_k+j,\tau_k+j+1,\dots,\tau_r\}}.$$

The new entry at index $\tau_k + j$ simplifies as $-jq_{\{\tau_k+j,\tau_k+j+1,\dots,\tau_r\}}$ by using the definition of h_{τ_k+j} in (9.13). When we multiply the resulting vector by $\boldsymbol{C}_{\tau_k+j}$, we affect only entries from indices $\tau_k + 1$ to $\tau_k + j$. More precisely, the previous relation shows that we obtain the vector

$$\begin{pmatrix} q_{\{1,\tau_k+j,\dots,\tau_r\}} & \cdots & q_{\{\tau_k,\tau_k+j,\dots,\tau_r\}} & q_{\{\tau_k+1,\tau_k+j+1,\dots,\tau_r\}} & \cdots & q_{\{\tau_k+j,\tau_k+j+1,\dots,\tau_r\}} & h_{\tau_k+j+1} & \dots & h_{\tau_r} \end{pmatrix}.$$

Finally, right-multiplication by $\boldsymbol{D}_{\tau_k+j}$ affects entries of indices $1, \dots, \tau_k$. For $i = 1, \dots, \tau_k$, it replaces $q_{\{i,\tau_k+j,\dots,\tau_r\}}$ by

$$q_{\{i,\tau_k+j,\dots,\tau_r\}}(z_{\tau_k+j} - z_i) + q_{\{\tau_k+j,\tau_k+j+1,\dots,\tau_r\}} = q_{\{i,\tau_k+j+1,\dots,\tau_r\}}.$$

Thus, the resulting vector is

$$\begin{pmatrix} q_{\{1,\tau_k+j+1,\dots,\tau_r\}} & \cdots & q_{\{\tau_k,\tau_k+j+1,\dots,\tau_r\}} & q_{\{\tau_k+1,\tau_k+j+1,\dots,\tau_r\}} & \cdots & q_{\{\tau_k+j,\tau_k+j+1,\dots,\tau_r\}} & h_{\tau_k+j+1} & \dots & h_{\tau_r} \end{pmatrix}$$

which is precisely $\boldsymbol{q}_{\tau_k+j}$, as claimed in (9.14). □

Example 9.3.3. Consider again the polynomials $\boldsymbol{q} = (q_1, q_2, q_3)$ and $\boldsymbol{p} = (p_1, p_2, p_3)$ of Example 9.3.2. The matrix $\boldsymbol{U}$ which relates $\boldsymbol{p}$ to $\boldsymbol{q}$ is constructed as follows. For $k = 0$ and $j = 1, 2$ let

$$\boldsymbol{B}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \boldsymbol{C}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \boldsymbol{D}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\boldsymbol{B}_2 = \begin{pmatrix} 1 & z_2 - z_1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \boldsymbol{C}_2 = \begin{pmatrix} z_2 - z_1 & 0 & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \boldsymbol{D}_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

while for $k = 1$ and $j = 1$ we have

$$\boldsymbol{B}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \boldsymbol{C}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \boldsymbol{D}_3 = \begin{pmatrix} z_3 - z_1 & 0 & 0 \\ 0 & z_3 - z_2 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

In the case $\lambda = (1^2\,2^1)$,

$$\boldsymbol{M} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and hence

$$\boldsymbol{U} = (\boldsymbol{B}_1\boldsymbol{C}_1\boldsymbol{D}_1)(\boldsymbol{B}_2\boldsymbol{C}_2\boldsymbol{D}_2)(\boldsymbol{B}_3\boldsymbol{C}_3\boldsymbol{D}_3) = \begin{pmatrix} \frac{1}{2}(z_3 - z_1)(z_2 - z_1) & \frac{-1}{2}(z_2 - z_1)(z_3 - z_2) & 0 \\ \frac{1}{2}(z_3 - z_1) & \frac{1}{2}(z_3 - z_2) & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Note that $\det(\boldsymbol{U}) = \frac{1}{2}(z_3 - z_1)(z_3 - z_2)(z_2 - z_1)$.

The formulas defining $\boldsymbol{p}$ are straightforward to implement. Recall the expressions defining $\boldsymbol{p} = (p_1, \ldots, p_\ell)$: for $k = 0, \ldots, r-1$, we have

$$p_{\tau_k + \ell_{k+1}} = \sum_{i=\tau_k+1}^{\tau_{k+1}} q_{\{i, \tau_{k+1}+1, \ldots, \tau_r\}}$$

and for $j = 1, \ldots, \ell_{k+1} - 1$,

$$p_{\tau_k + j} = \sum_{s=1}^{j} \eta_{j-s}(z_{\tau_k+s+2}, \ldots, z_{\tau_{k+1}}) \Big(\sum_{i=1}^{s} q_{\{\tau_k+i, \tau_k+s+1, \ldots, \tau_r\}} \Big).$$

The main issue is to compute the divided differences $q_{\{\tau_k+i, \tau_k+s+1, \ldots, \tau_r\}}$ appearing in these expressions, for $k = 0, \ldots, r-1$ and $1 \le i \le s \le \ell_{k+1}$. Once this is done, the combinations necessary to obtain p_{τ_k+j} are easily carried out. The main ingredient in the proof is the following lemma which describes the computation of a single divided difference.

Lemma 9.3.10. *There exists an algorithm* Divided_Difference$(\boldsymbol{q}, I)$ *that takes as input* $\boldsymbol{q}$ *as in Proposition 9.3.8 and a subset* $I = \{i_1, \ldots, i_k\}$ *of* $\{1, \ldots, \ell\}$*, and returns* q_I*. For* $\boldsymbol{q}$ *of degree at most* d*, the runtime is* $O^{\sim}(\ell\binom{\ell+d}{d})$ *operations in* $\mathbb{K}$*.*

Proof. For $j = 1, \ldots, k-1$, we claim that given $q_{\{i_1, \ldots, i_{j-1}\}}$, we can obtain $q_{\{i_1, \ldots, i_j\}}$ using $O^{\sim}(\binom{\ell+d}{d})$ operations in $\mathbb{K}$.

To see this note that $q_{\{i_1, \ldots, i_{k-1}\}}$ has degree at most d. In order to compute $q_{\{i_1, \ldots, i_j\}}$, we use evaluation / interpolation. Choosing $\binom{\ell+d}{d}$ points as prescribed in [39], the algorithm given there allows us to compute the values of both numerator and denominator in (9.7) in $O^{\sim}(\binom{\ell+d}{d})$ operations, then compute their ratio, and finally interpolate $q_{\{i_1, \ldots, i_j\}}$ in the same asymptotic runtime. The result then follows. □

We finish this section by the following proposition which describes the resulting algorithm, called Symmetrize, and gives the cost of this procedure to compute the system $\boldsymbol{p}$ from $\boldsymbol{q}$.

Algorithm 14 Symmetrize$(\lambda, \boldsymbol{q})$

Input: a partition $\lambda = (n_1^{\ell_1} n_2^{\ell_2} \dots n_r^{\ell_2})$ and a sequence of $\mathcal{S}_\lambda$-equivariant polynomials $\boldsymbol{q} = (q_1, \dots, q_\ell)$ such that $z_i - z_k$ divides $q_i - q_k$ for $1 \le i < k \le \ell$
Output: an $\mathcal{S}_\lambda$-invariant sequence of polynomials $\boldsymbol{p} = (p_1, \dots, p_\ell)$ such that $\langle \boldsymbol{p} \rangle = \langle \boldsymbol{q} \rangle$ in $\mathbb{K}[\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r]_\Delta$, where Δ is the Vandermonde determinant associate with $(\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r)$

1. setting $\tau_0 = 0$ and $\tau_k = \sum_{i=1}^{k} \ell_i$ for $k = 1, \dots, r$
2. for $k \in \{0, \dots, r-1\}$
   (a) for $j \in \{1, \dots, \ell_{k+1} - 1\}$
      i. $p_{\tau_k + j} = \sum_{s=1}^{j} \eta_{j-s}(z_{\tau_k+s+2}, \dots, z_{\tau_{k+1}}) \left(\sum_{\tau_k+1}^{\tau_k+s} \mathsf{Divided_Difference}(q, \{i, \tau_k + s + 1, \dots, \tau_r\}) \right)$
      where $\eta_{j-s}(\cdot)$ is the $(j-s)$-th elementary symmetric function
   (b) $p_{\tau_{k+1}} = \sum_{i=\tau_k+1}^{\tau_{k+1}} \mathsf{Divided_Difference}(q, \{i, \tau_{k+1} + 1, \dots, \tau_r\})$
3. return $\boldsymbol{p} = (p_{\tau_0+1}, \dots, p_{\tau_0+\ell_1-1}, \dots, p_{\tau_{r-1}+1}, \dots, p_{\tau_r})$

Proposition 9.3.11. *There exists an algorithm* Symmetrize$(\lambda, \boldsymbol{q})$ *which takes as input* $\boldsymbol{q}$ *as in Proposition 9.3.8 and a partition* λ *of* n*, and returns* $\boldsymbol{p}$ *as defined in that proposition. For* $\boldsymbol{q}$ *of degree at most* d*, the runtime is* $O^{\sim}(\ell^3 \binom{\ell+d}{d})$ *operations in* $\mathbb{K}$*.*

Proof. Our Symmetrize algorithm proceeds as follows. Apply algorithm Divided_Difference from Lemma 9.3.10 to all $[\tau_k + i, \tau_k + s + 1, \dots, \tau_r]$, for $k = 0, \dots, r-1$ and $1 \le i \le s \le \ell_{k+1}$. There are $O(\ell^2)$ such indices, so this step takes $O^{\sim}(\ell^3 \binom{\ell+d}{d})$ operations in $\mathbb{K}$, allowing us to compute all sums $\sum_{i=1}^{s} q_{\{\tau_k+i, \tau_k+s+1, \dots, \tau_r\}}$ for the same asymptotic cost.

For $k = 0, \dots, r-1$, $j = 1, \dots, \ell_{k+1} - 1$ and $s = 1, \dots, j$, we then compute the elementary symmetric polynomial $\eta_{j-s}(z_{\tau_k+s+2}, \dots, z_{\tau_{k+1}})$, which does not involve any arithmetic operations. We multiply it by the above sum, with cost $O^{\sim}(\binom{\ell+d}{d})$, since the polynomials involved in the product have degree sum at most d and at most ℓ variables. Taking all indices k, j, s into account, this adds another $O^{\sim}(\ell^3 \binom{\ell+d}{d})$ steps to the total. □

Chapter 10

Computing critical points for invariant algebraic systems

We can now turn to the main question in this second half of the thesis. Let $\boldsymbol{G} = (g_1, \ldots, g_s)$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$, with $s \leq n$. Given a polynomial ϕ in $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$, we are interested in describing the algebraic set $W(\phi, \boldsymbol{G})$ defined by the simultaneous vanishing of the polynomials

$$g_1, \ldots, g_s, \quad M_{s+1}(\mathrm{Jac}(\boldsymbol{G}, \phi)) \tag{10.1}$$

where $M_{s+1}(\mathrm{Jac}(\boldsymbol{G}, \phi))$ is the set of $(s+1)$-minors of the Jacobian matrix $\mathrm{Jac}(\boldsymbol{G}, \phi) \in \mathbb{K}[x_1, \ldots, x_n]^{(s+1)\times n}$. Equivalently, this is the set of all $\boldsymbol{x}$ in $V(\boldsymbol{G})$ at which $\mathrm{Jac}(\boldsymbol{G}, \phi)$ has rank less than $s+1$.

If we assume that $\mathrm{Jac}(\boldsymbol{G})$ has full rank s at any point of $V = V(\boldsymbol{G})$, then V is smooth of codimension s (or empty) and $W(\phi, \boldsymbol{G})$ is the set of critical points of ϕ on it. However, most of our discussion can take place without this assumption. For the sake of simplicity, in any case, we will still refer to the solutions of (10.1) as critical points.

10.1 Description of the algebraic set $W(\phi, \boldsymbol{G})$

Fundamental to our results is the fact that $W(\phi, \boldsymbol{G})$ is invariant under the action of the symmetric group. This follows from the next lemma, being a direct consequence of the chain rule.

Lemma 10.1.1. *Let g be in $\mathbb{K}[x_1, \ldots, x_n]$ and σ in $\mathcal{S}_n$. Then for k in $\{1, \ldots, n\}$, we have*

$$\sigma\left(\frac{\partial g}{\partial x_k}\right) = \frac{\partial(\sigma(g))}{\partial x_{\sigma(k)}}. \tag{10.2}$$

Corollary 10.1.2. *The algebraic set $W(\phi, \boldsymbol{G})$ is $\mathcal{S}_n$-invariant.*

Proof. Let $\boldsymbol{\xi}$ be in $W(\phi, \boldsymbol{G})$ and σ be in $\mathcal{S}_n$. We need to show that $\sigma(\boldsymbol{\xi})$ is in $W(\phi, \boldsymbol{G})$, that is, $f_i(\sigma(\boldsymbol{\xi})) = 0$ for all i and $\mathrm{Jac}(\boldsymbol{G}, \phi)$ has rank at most s at $\sigma(\boldsymbol{\xi})$.

The first statement is clear, since $\boldsymbol{\xi}$ cancels $\boldsymbol{G}$ and $\boldsymbol{G}$ is $\mathcal{S}_n$-invariant. For the second claim, since all g_i's and ϕ are $\mathcal{S}_n$-invariant, Lemma 10.1.1 implies that the Jacobian matrix $\mathrm{Jac}(\boldsymbol{G}, \phi)$ at $\sigma(\boldsymbol{\xi})$ is equal to $(\mathrm{Jac}(\boldsymbol{G}, \phi)(\boldsymbol{\xi}))\boldsymbol{A}^{-1}$, where $\boldsymbol{A}$ is the matrix of σ. Therefore, as with $\mathrm{Jac}(\boldsymbol{G}, \phi)(\boldsymbol{\xi})$, it has rank at most s . □

Remark that the proof of the corollary implies a slightly stronger property, which we already mentioned in the introduction: the system $g_1, \ldots, g_s, M_{s+1}(\mathrm{Jac}(\boldsymbol{G}, \phi))$ is globally invariant (that is, applying any $\sigma \in \mathcal{S}_n$ permutes these equations, possibly changing signs). However, instead of using this fact directly, our algorithm will use our result from the previous section.

The corollary above also implies that the discussion in Section 9.2 applies to $W := W(\phi, \boldsymbol{G})$. In particular, for a partition λ of n, the set W_λ and W'_λ of (9.3) are well-defined. In what follows, we fix a partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2} \ldots n_r^{\ell_r})$ of n and we let ℓ be its length; we explain how to compute a description of W'_λ along the lines of Section 9.2. For this, we let $\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r$ be the indeterminates associated to λ, as defined in Section 9.1, with $\boldsymbol{Z}_i = (z_{i,1}, \ldots, z_{i,\ell_i})$. As in that section, we also write all indeterminates $(z_{1,1}, \ldots, z_{r,\ell_r})$ as $(z_1, \ldots, z_\ell)$.

Definition 10.1.3. *With λ and $\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r$ as above, we define $\mathbb{T}_\lambda$, the $\mathbb{K}$-algebra homomorphism $\mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]$ mapping $x_1, \ldots, x_n$ to*

$$\underbrace{z_{1,1}, \ldots, z_{1,1}}_{n_1},\ \ldots,\ \underbrace{z_{1,\ell_1}, \ldots, z_{1,\ell_1}}_{n_1}\ \ldots,\ \underbrace{z_{r,1}, \ldots, z_{r,1}}_{n_r},\ \ldots,\ \underbrace{z_{r,\ell_r}, \ldots, z_{r,\ell_r}}_{n_r}. \tag{10.3}$$

The operator $\mathbb{T}_\lambda$ extends to vectors or matrices of polynomials entry-wise.

We can now define

$$\boldsymbol{G}^{[\lambda]} = \mathbb{T}_\lambda(\boldsymbol{G}) = (g_1^{[\lambda]}, \ldots, g_s^{[\lambda]}) \quad \text{and} \quad \boldsymbol{J}^{[\lambda]} = \mathbb{T}_\lambda(\mathrm{Jac}(\boldsymbol{G}, \phi)) = \left[J_{i,j}^{[\lambda]}\right]_{1 \le i \le s+1, 1 \le j \le n}. \tag{10.4}$$

Notice that for f in $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$, and for any indices j, k in $\{1, \ldots, n\}$ for which $\mathbb{T}_\lambda(x_j) = \mathbb{T}_\lambda(x_k)$, we have

$$\mathbb{T}_\lambda\left(\frac{\partial f}{\partial x_j}\right) = \mathbb{T}_\lambda\left(\frac{\partial f}{\partial x_k}\right); \tag{10.5}$$

this follows by applying Lemma 10.1.1 to f and the transposition $(j\,k)$. Thus

$$\mathbb{T}_\lambda\left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) = \Big(\underbrace{f_{1,1}^{[\lambda]}, \ldots, f_{1,1}^{[\lambda]}}_{n_1}, \ldots, \underbrace{f_{1,\ell_1}^{[\lambda]}, \ldots, f_{1,\ell_1}^{[\lambda]}}_{n_1}, \ldots, \underbrace{f_{r,1}^{[\lambda]}, \ldots, f_{r,1}^{[\lambda]}}_{n_r}, \ldots, \underbrace{f_{r,\ell_r}^{[\lambda]}, \ldots, f_{r,\ell_r}^{[\lambda]}}_{n_r}\Big), \tag{10.6}$$

where $f_{i,j}^{[\lambda]}$ are polynomials in the variables $(\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r)$.

Lemma 10.1.4. *The columns of the transformed Jacobian matrix $\boldsymbol{J}^{[\lambda]}$ have the form:*

$$\boldsymbol{J}^{[\lambda]} = \Big(\underbrace{J_{1,1}^{[\lambda]}, \dots, J_{1,1}^{[\lambda]}}_{n_1}, \dots, \underbrace{J_{1,\ell_1}^{[\lambda]}, \dots, J_{1,\ell_1}^{[\lambda]}}_{n_1}, \dots, \underbrace{J_{r,1}^{[\lambda]}, \dots, J_{r,1}^{[\lambda]}}_{n_r}, \dots, \underbrace{J_{r,\ell_r}^{[\lambda]}, \dots, J_{r,\ell_r}^{[\lambda]}}_{n_r} \Big), \tag{10.7}$$

Proof. This follows directly from (10.6), since

$$(J_{s+1,1}^{[\lambda]}, \dots, J_{s+1,n}^{[\lambda]}) = \mathbb{T}_\lambda \left(\frac{\partial \phi}{\partial x_1}, \dots, \frac{\partial \phi}{\partial x_n} \right) \quad \text{and} \quad (J_{i,1}^{[\lambda]}, \dots, J_{i,n}^{[\lambda]}) = \mathbb{T}_\lambda \left(\frac{\partial g_i}{\partial x_1}, \dots, \frac{\partial g_i}{\partial x_n} \right)$$

for $i = 1, \dots, s$, and all polynomials $g_1, \dots, g_s, \phi$ are in $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{S}_n}$. □

We will then let $\boldsymbol{F}^{[\lambda]} = [F_{i,j}^{[\lambda]}]_{1 \le i \le s+1, 1 \le j \le \ell}$ be the matrix with entries in $\mathbb{K}[\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r]$ obtained from $\mathrm{Jac}(\boldsymbol{G}, \phi)$ by first applying $\mathbb{T}_\lambda$ and then keeping only one representative among all repeated columns highlighted in the previous lemma.

Example 10.1.1. Let $s = 1$ and $n = 5$, so we consider two polynomials g_1, ϕ in $\mathbb{K}[x_1, \dots, x_5]$, and take $\lambda = (1^1\, 2^2)$. Then

$$g_1^{[\lambda]}(z_{1,1}, z_{2,1}, z_{2,2}) = \mathbb{T}_\lambda(g_1) = g_1(z_{1,1}, z_{2,1}, z_{2,1}, z_{2,2}, z_{2,2}),$$

and

$$\boldsymbol{F}^{[\lambda]} = \begin{pmatrix} \mathbb{T}_\lambda(\frac{\partial g_1}{\partial x_1}) & \mathbb{T}_\lambda(\frac{\partial g_1}{\partial x_2}) & \mathbb{T}_\lambda(\frac{\partial g_1}{\partial x_4}) \\ \\ \mathbb{T}_\lambda(\frac{\partial \phi}{\partial x_1}) & \mathbb{T}_\lambda(\frac{\partial \phi}{\partial x_2}) & \mathbb{T}_\lambda(\frac{\partial \phi}{\partial x_4}) \end{pmatrix} \in \mathbb{K}[z_{1,1}, z_{2,1}, z_{2,2}]^{2 \times 3}.$$

It is easy to see that the polynomials $\boldsymbol{G}^{[\lambda]}$ are $\mathcal{S}_\lambda$-invariant, where $\mathcal{S}_\lambda$ is the permutation group $\mathcal{S}_{\ell_1} \times \cdots \times \mathcal{S}_{\ell_r}$ introduced in the previous section. However, this is generally not the case for the entries of $\boldsymbol{F}^{[\lambda]}$.

Lemma 10.1.5. *Let $\boldsymbol{f}^{[\lambda]} = (f_1^{[\lambda]}, \dots, f_\ell^{[\lambda]})$ be a row of $\boldsymbol{F}^{[\lambda]}$. Then*

(i) *$z_i - z_j$ divides $f_i^{[\lambda]} - f_j^{[\lambda]}$ for $1 \le i < j \le \ell$;*

(ii) *$\boldsymbol{f}^{[\lambda]}$ is $\mathcal{S}_\lambda$-equivariant.*

Proof. For the sake of definiteness, let us assume that $\boldsymbol{f}^{[\lambda]}$ is the row corresponding to the gradient of g_1, with the other cases treated similarly.

For statement (i), we start from indices i, j as in the lemma and let S be the $\mathbb{K}$-algebra homomorphism $\mathbb{K}[\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r] \to \mathbb{K}[\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r]$ that maps z_i to z_j, leaving all other variables unchanged. Let u, v in $\{1, \dots, n\}$ be indices such that $f_i^{[\lambda]} = \mathbb{T}_\lambda(\partial f_1/\partial x_u)$ and $f_j^{[\lambda]} = \mathbb{T}_\lambda(\partial f_1/\partial x_v)$ and $\sigma \in \mathcal{S}_n$ the transposition $(u\, v)$. From Lemma 10.1.1, we have that $\sigma(\partial f_1/\partial x_u) = \partial g_1/\partial x_v$ and applying $S \circ \mathbb{T}_\lambda$ gives $S(\mathbb{T}_\lambda(\sigma(\partial g_1/\partial x_u))) = S(\mathbb{T}_\lambda(\partial g_1/\partial x_v))$. For any $h \in \mathbb{K}[x_1, \dots, x_n]$ we have, by construction, $S(\mathbb{T}_\lambda(\sigma(h))) = S(\mathbb{T}_\lambda(h))$. Applying

this on the left-hand side of the previous equality gives $S(f_i^{[\lambda]}) = S(f_j^{[\lambda]})$. As a result, $z_i - z_j$ divides $f_i^{[\lambda]} - f_j^{[\lambda]}$, as claimed.

For statement (ii), we take indices k in $\{1, \ldots, r\}$ and j, j' in $\{1, \ldots, \ell_k\}$. We let $\sigma \in \mathcal{S}_\lambda$ be the transposition that maps (k, j) to (k, j') and prove that $\sigma(f_{k,j}^{[\lambda]}) = f_{k,j'}^{[\lambda]}$. As before, there exist indices u, v in $\{1, \ldots, n\}$ such that $f_{k,j}^{[\lambda]} = \mathbb{T}_\lambda(\partial g_1/\partial x_u)$ and $f_{k,j'}^{[\lambda]} = \mathbb{T}_\lambda(\partial g_1/\partial x_v)$. Without loss of generality, assume that u and v are the smallest such indices. Then $\mathbb{T}_\lambda$ maps $x_u, \ldots, x_{u+\ell_k-1}$ to $z_{k,j}$ and $x_v, \ldots, x_{v+\ell_k-1}$ to $z_{k,j'}$.

Let $\tau \in \mathcal{S}_n$ be permutation that permutes $(u, \ldots, u+\ell_k-1)$ with $(v, \ldots, v+\ell_k-1)$. From Lemma 10.1.1, we get $\tau(\partial g_1/\partial x_v) = \partial g_1/\partial x_u$. Then $\mathbb{T}_\lambda(\tau(\partial g_1/\partial x_u)) = \mathbb{T}_\lambda(\partial g_1/\partial x_v) = f_{k,j'}^{[\lambda]}$. By construction, the left-hand side is equal to $\sigma(\mathbb{T}_\lambda(\partial g_1/\partial x_u))$, that is, $\sigma(f_{k,j}^{[\lambda]})$. □

Lemma 10.1.5 implies that we can apply Algorithm Symmetrize from Section 9.3.2 to each row of $\boldsymbol{F}^{[\lambda]}$. The result is a polynomial matrix $\boldsymbol{H}^{[\lambda]}$ in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]$, whose entries are all $\mathcal{S}_\lambda$-equivariant, and such that $\boldsymbol{H}^{[\lambda]} = \boldsymbol{F}^{[\lambda]}\boldsymbol{U}^{[\lambda]}$, for some polynomial matrix $\boldsymbol{U}^{[\lambda]}$ in $\mathbb{K}[\boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_r]^{\ell\times\ell}$. Applying Algorithm Symmetric_Coordinates from Lemma 9.3.1 to the entries of both $\boldsymbol{G}^{[\lambda]}$ and $\boldsymbol{H}^{[\lambda]}$ gives polynomials $\bar{\boldsymbol{G}}^{[\lambda]}$ and a matrix $\bar{\boldsymbol{H}}^{[\lambda]}$, all with entries in $\mathbb{K}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r]$, with variables $\boldsymbol{e}_i = (e_{i,1}, \ldots, e_{i,\ell_1})$ for all i, and such that

$$\boldsymbol{G}^{[\lambda]} = \bar{\boldsymbol{G}}^{[\lambda]}(\boldsymbol{\eta}_1, \ldots, \boldsymbol{\eta}_r) \text{ and } \boldsymbol{H}^{[\lambda]} = \bar{\boldsymbol{H}}^{[\lambda]}(\boldsymbol{\eta}_1, \ldots, \boldsymbol{\eta}_r)$$

The following summarizes the main properties of this construction. For the definitions of the sets $\mathcal{C}_\lambda$, $\mathcal{C}_\lambda^{\text{strict}}$, the mapping E_λ and the open set $O_\lambda \subset \overline{\mathbb{K}}^\ell$, we refer to Section 9.2. From now on, we will denote by $W = W(\phi, \boldsymbol{G})$.

Proposition 10.1.6. *Let λ be a partition of n of length ℓ.*

(i) *If $\ell \leq s$, then $E_\lambda(W \cap \mathcal{C}_\lambda)$ is the zero-set of $\bar{\boldsymbol{G}}^{[\lambda]}$ in $\overline{\mathbb{K}}^\ell$.*

(ii) *If $\ell > s$, then $W'_\lambda = E_\lambda(W_\lambda^{\text{strict}})$ is the zero-set of $\bar{\boldsymbol{G}}^{[\lambda]}$ and all $(s+1)$-minors of $\bar{\boldsymbol{H}}^{[\lambda]}$ in $O_\lambda \subset \overline{\mathbb{K}}^\ell$.*

Proof. Let $\boldsymbol{\xi}$ be in the set $\mathcal{C}_\lambda$ defined in Section 9.2, and write

$$\boldsymbol{\xi} = \big(\underbrace{\xi_{1,1}, \ldots, \xi_{1,1}}_{n_1}, \ldots, \underbrace{\xi_{1,\ell_1}, \ldots, \xi_{1,\ell_1}}_{n_1}, \ldots, \underbrace{\xi_{r,1}, \ldots, \xi_{r,1}}_{n_r}, \ldots, \underbrace{\xi_{r,\ell_r}, \ldots, \xi_{r,\ell_r}}_{n_r}\big).$$

Set $\boldsymbol{\zeta} = (\xi_{1,1}, \xi_{1,2}, \ldots, \xi_{r,\ell_r}) \in \overline{\mathbb{K}}^\ell$ and $\boldsymbol{\varepsilon} = E_\lambda(\boldsymbol{\xi}) \in \overline{\mathbb{K}}^\ell$. By definition, we have $\boldsymbol{G}(\boldsymbol{\xi}) = \boldsymbol{G}^{[\lambda]}(\boldsymbol{\zeta})$ and $\mathrm{Jac}(\boldsymbol{G}, \phi)(\boldsymbol{\xi}) = \boldsymbol{J}^{[\lambda]}(\boldsymbol{\zeta})$; recall that the definition of the matrix $\boldsymbol{J}^{[\lambda]}$ is given in (10.4).

Thus, $\boldsymbol{\xi}$ is in $W \cap \mathcal{C}_\lambda$ if and only if it cancels $\boldsymbol{G}$ and $\mathrm{Jac}(\boldsymbol{G}, \phi)$ has rank at most s at $\boldsymbol{\xi}$, that is, if $\boldsymbol{G}^{[\lambda]}(\boldsymbol{\zeta}) = 0$ and $\boldsymbol{J}^{[\lambda]}(\boldsymbol{\zeta})$ has rank at most s. The point $\boldsymbol{\xi}$ is in $W \cap \mathcal{C}_\lambda^{\text{strict}}$ if all

the entries of $\boldsymbol{\zeta}$ are also pairwise distinct. In addition, we have $\boldsymbol{G}^{[\lambda]}(\boldsymbol{\zeta}) = \bar{\boldsymbol{G}}^{[\lambda]}(\boldsymbol{\varepsilon})$ and, by construction, $\operatorname{rank}(\boldsymbol{J}^{[\lambda]}(\boldsymbol{\zeta})) = \operatorname{rank}(\boldsymbol{F}^{[\lambda]}(\boldsymbol{\zeta}))$. If $\ell \leq s$ then, since $\boldsymbol{F}^{[\lambda]}$ has ℓ columns, we see that $\boldsymbol{\xi}$ is in $W \cap \mathcal{C}_\lambda$ if and only if $\boldsymbol{\varepsilon} = E_\lambda(\boldsymbol{\xi})$ cancels $\bar{\boldsymbol{G}}^{[\lambda]}$. Since $E_\lambda : \mathcal{C}_\lambda \to \overline{\mathbb{K}}^\ell$ is onto, this implies our first claim.

Suppose further that $\boldsymbol{\xi}$ is in $\mathcal{C}_\lambda^{\text{strict}}$, so that $\boldsymbol{\varepsilon}$ is in O_λ. From Proposition 9.3.8, we have $\boldsymbol{H}^{[\lambda]} = \boldsymbol{F}^{[\lambda]}\boldsymbol{U}^{[\lambda]}$. Our assumption on $\boldsymbol{\xi}$ implies that $\boldsymbol{U}^{[\lambda]}(\boldsymbol{\zeta})$ is invertible, so that $\boldsymbol{F}^{[\lambda]}$ and $\boldsymbol{H}^{[\lambda]}$ have the same rank at $\boldsymbol{\zeta}$. Finally, we have $\boldsymbol{H}^{[\lambda]}(\boldsymbol{\zeta}) = \bar{\boldsymbol{H}}^{[\lambda]}(\boldsymbol{\varepsilon})$. All this combined shows that $\boldsymbol{\xi}$ is in $W'_\lambda = E_\lambda(W \cap \mathcal{C}_\lambda^{\text{strict}})$ if and only if $\boldsymbol{\varepsilon} = E_\lambda(\boldsymbol{\xi})$ cancels $\bar{\boldsymbol{G}}^{[\lambda]}$ and all $(s+1)$-minors of $\bar{\boldsymbol{H}}^{[\lambda]}$. Since the restriction $E_\lambda : \mathcal{C}_\lambda^{\text{strict}} \to O_\lambda$ is onto, this implies the second claim. □

10.2 Algorithms for computing critical points

In this subsection, we present the main algorithm which is called Critical_Points_Per_Orbit. Consider symmetric polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ and ϕ in $\mathbb{K}[\boldsymbol{X}]$ such that the set $W(\phi, \boldsymbol{G})$ is finite.

Critical_Points_Per_Orbit algorithm takes $\boldsymbol{G}$ and ϕ as input and outputs a symmetric representation of $W = W(\phi, \boldsymbol{G})$. Using our notation from Chapter 9, this means that we want to compute zero-dimensional parametrizations of $W'_\lambda = E_\lambda(W \cap \mathcal{C}_\lambda^{\text{strict}})$, for all partitions λ of n for which this set is not empty. The algorithm is based on Proposition 10.1.6, with a minor modification, as we will see that it is enough to consider partitions of n of length ℓ either exactly equal to s, or at least $s+1$.

10.2.1 Some subroutines

We first present some subroutines we use in our main algorithm.

- Prepare_G$(\boldsymbol{G}, \lambda)$ takes as input $\boldsymbol{G}$ and a partition λ and returns the sequence of polynomials $\bar{\boldsymbol{G}}^{[\lambda]}$.
- Prepare_G_H$(\boldsymbol{G}, \phi, \lambda)$ takes as input $\boldsymbol{G}, \phi$ as above and a partition λ and returns the sequence of polynomials $\bar{\boldsymbol{G}}^{[\lambda]}$ and the matrix $\bar{\boldsymbol{H}}^{[\lambda]}$.
- WeightedColumnDegree$(\boldsymbol{G})$ takes as input polynomials $\boldsymbol{G}$ and returns a zero-dimensional parametrization of the isolated points of $V(\boldsymbol{G})$.
- WeightedColumnDegree$(\boldsymbol{H}, \boldsymbol{G})$ takes as input polynomials $\boldsymbol{G}$, a polynomial matrix $\boldsymbol{H}$ of size $p \times q$, and returns a zero-dimensional parametrization of the isolated points of $V_p(\boldsymbol{H}, \boldsymbol{G})$.
- Decompose$(\lambda, \mathscr{R})$ takes as input a partition λ and a zero-dimensional parametrization $\mathscr{R}$ of a set G and returns a symmetric representation of $E_\lambda^*(G)$.

- Remove_Duplicates(S) inputs a list $S = (\lambda_i, \mathscr{R}_i)_{1 \leq i \leq N}$, where each λ_i is a partition of n and $\mathscr{R}_i$ a zero-dimensional parametrization, and removes pairs $(\lambda_i, \mathscr{R}_i)$ from S so as to ensure that all resulting partitions are pairwise distinct.

Note that the WeightedColumnDegree($\boldsymbol{G}$) procedure can be seen as a particular case of the WeightedColumnDegree($\boldsymbol{H}, \boldsymbol{G}$), where we take $\boldsymbol{H}$ to be a matrix with no row. The choice of which entries to remove in the Remove_Duplicates(S) subroutine is arbitrary; it does not affect correctness of the overall algorithm

10.2.2 The main algorithm

Our Critical_Points_Per_Orbit algorithm is given as Algorithm 15. The goal of the algorithm is to compute zero-dimensional representations of $W'_\lambda = E_\lambda(W \cap \mathcal{C}_\lambda^{\text{strict}})$ for all partitions λ of n for which this set is not empty. Recall that $W = W(\phi, \boldsymbol{G})$.

Algorithm 15 Critical_Points_Per_Orbit($\boldsymbol{G}, \phi$)

Input: $\boldsymbol{G} = (g_1, \ldots, g_s)$ and ϕ in $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$ such that $W(\phi, \boldsymbol{G})$ is finite

Output: a symmetric representation of $W(\phi, \boldsymbol{G})$

1. $S = [\,]$
2. for $\lambda \vdash n$ of length s
   (a) $\bar{\boldsymbol{G}}^{[\lambda]} =$ Prepare_G($\boldsymbol{G}, \lambda$)
   (b) $\mathscr{R}_\lambda =$ WeightedColumnDegree($\bar{\boldsymbol{G}}^{[\lambda]}$)
   (c) append the output of Decompose($\mathscr{R}_\lambda$) to S
3. for $\lambda \vdash n$ of length in $\{s+1, \ldots, n\}$
   (a) $\bar{\boldsymbol{G}}^{[\lambda]}, \bar{\boldsymbol{H}}^{[\lambda]} =$ Prepare_G_H($\boldsymbol{G}, \phi, \lambda$)
   (b) $\mathscr{R}_\lambda =$ WeightedColumnDegree($\bar{\boldsymbol{H}}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]}$)
   (c) $(\lambda_i, \mathscr{R}_i)_{1 \leq i \leq N} =$ Decompose($\mathscr{R}_\lambda$)
   (d) append $(\lambda_{i_0}, \mathscr{R}_{i_0})$ to S, where i_0 is such that $\lambda_{i_0} = \lambda$, if such an i_0 exists
4. return Remove_Duplicates(S)

Proposition 10.2.1. *Algorithm* Critical_Points_Per_Orbit *is correct.*

Proof. Recall first that W is assumed to be finite. Hence this also holds for all $W \cap \mathcal{C}_\lambda$, and thus for all $E_\lambda(W \cap \mathcal{C}_\lambda)$. As a result, for λ of length s, Proposition 10.1.6(i) implies that at Step 2b, WeightedColumnDegree($\bar{\boldsymbol{G}}^{[\lambda]}$) returns a zero-dimensional parametrization of $G := E_\lambda(W \cap \mathcal{C}_\lambda)$. Moreover, from Lemma 9.2.3, the output of Decompose($\lambda, \mathscr{R}_\lambda$) is a symmetric representation of $E^*_\lambda(G)$. This representation is the orbit of $W \cap \mathcal{C}_\lambda$, that is, the set of all orbits contained in W whose type λ' satisfies $\lambda' \geq \lambda$. Taking into account all partitions λ of length s, the set of partitions $\lambda' \geq \lambda$ covers all partitions of length $\ell \in \{1, \ldots, s\}$, so that at the end of Step 2, we have zero-dimensional parametrizations of W'_λ for all partitions of length $\ell \in \{1, \ldots, s\}$ (with possible repetitions). Calling Remove_Duplicates(S) will remove any duplicates among this list.

The second loop deals with partitions λ of length at least $s+1$. Since we assume that W is finite, W'_λ is finite for any such λ. Proposition 10.1.6(ii) then implies that the points in W'_λ are isolated points of the zero-set of $\bar{\boldsymbol{G}}^{[\lambda]}$ and of the $(s+1)$-minors of $\bar{\boldsymbol{H}}^{[\lambda]}$. As a result, W'_λ is a subset of $V(\mathscr{R}_\lambda)$, for $\mathscr{R}_\lambda$ computed in Step 3b with all other points in $V(\mathscr{R}_\lambda)$ corresponding to points in W with type $\lambda' > \lambda$. In particular, after the call to Decompose, it suffices to keep the entry in the list corresponding to the partition λ, to obtain a description of W'_λ. □

10.3 Cost of the main algorithm

In this subsection we provide a complexity analysis of our Critical_Points_Per_Orbit algorithm by estimating the runtimes of all subroutines.

10.3.1 The Prepare procedure

For any partition λ, we first need to transform $\boldsymbol{G}$ and ϕ, in order to obtain the polynomials $\bar{\boldsymbol{G}}^{[\lambda]}$ and the matrix $\bar{\boldsymbol{H}}^{[\lambda]}$ in Proposition 10.1.6.

Algorithm 16 Prepare_G($\boldsymbol{G}, \lambda$)

Input: a partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2} \ldots n_r^{\ell_2})$ and a sequence of polynomials $\boldsymbol{G}$ in $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$ of degree at most d

Output: the polynomials $\bar{\boldsymbol{G}}^{[\lambda]}$ in $\mathbb{K}[\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r]$ as defined in Proposition 10.1.6

1. construct $\boldsymbol{G}^{[\lambda]} = \mathbb{T}_\lambda(\boldsymbol{G})$, where $\mathbb{T}_\lambda$ is the morphism defined in Definition 10.1.3
2. compute $\bar{\boldsymbol{G}}^{[\lambda]} =$ Symmetric_Coordinates($\lambda, \boldsymbol{G}^{[\lambda]}$)

Lemma 10.3.1. *There exists an algorithm* Prepare_G($\boldsymbol{G}, \lambda$) *which takes as input* $\boldsymbol{G}$ *as above and a partition* λ*, and returns* $\bar{\boldsymbol{G}}^{[\lambda]}$*. If* $\boldsymbol{G}$ *has degree at most* d*, the algorithm takes* $O^{\sim}(n\binom{n+d}{d}^2)$ *operations in* $\mathbb{K}$*.*

Algorithm 17 Prepare_G_H$(\boldsymbol{G}, \phi, \lambda)$

Input: a partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2} \dots n_r^{\ell_2})$ and a sequence of polynomials $\boldsymbol{G}$ and a polynomial map ϕ in $\mathbb{K}[x_1, \dots, x_n]^{\mathcal{S}_n}$ of degree at most d
Output: the polynomials $\bar{\boldsymbol{G}}^{[\lambda]}$ and the matrix $\bar{\boldsymbol{H}}$ in $\mathbb{K}[\boldsymbol{e}_1, \dots, \boldsymbol{e}_r]$ as defined in Proposition 10.1.6

1. construct $\boldsymbol{G}^{[\lambda]} = \mathbb{T}_\lambda(\boldsymbol{G})$
2. compute the Jacobian matrix $\mathrm{Jac}(\boldsymbol{G}, \phi)$ with respect to $(x_1, \dots, x_n)$
3. apply $\mathbb{T}_\lambda$ to all rows of $\mathrm{Jac}(\boldsymbol{G}, \phi)$ and remove all redundant columns to get the matrix $\boldsymbol{F}^{[\lambda]}$ in $\mathbb{K}[\boldsymbol{Z}_1, \dots, \boldsymbol{Z}_r]^{(s+1)\times \ell}$
4. for $i \in \{1, \dots, s+1\}$
   (a) compute $\boldsymbol{H}_{:i}^{[\lambda]} = \mathsf{Symmetrize}(\lambda, \boldsymbol{F}_{:i}^{[\lambda]})$, where $A_{:i}$ is the i-th row of the matrix A
   (b) for $j \in \{1, \dots, \ell\}$
   compute $\bar{\boldsymbol{H}}_{i,j}^{[\lambda]} = \mathsf{Symmetric_Coordinates}(\lambda, \boldsymbol{H}_{i,j}^{[\lambda]})$, the (i,j)-th entry of $\bar{\boldsymbol{H}}^{[\lambda]}$

Similarly, there exists an algorithm Prepare_G_H$(\boldsymbol{G}, \phi, \lambda)$ *which takes as input* $\boldsymbol{G}, \phi$ *as above and a partition* λ*, and returns* $\bar{\boldsymbol{G}}^{[\lambda]}$ *and* $\bar{\boldsymbol{H}}^{[\lambda]}$*. If* $\boldsymbol{G}$ *and* ϕ *have degree at most* d*, then the algorithm takes* $O^{\sim}(n^4\binom{n+d}{d}^2)$ *operations in* $\mathbb{K}$*.*

Proof. In the first case, applying $\mathbb{T}_\lambda$ to $\boldsymbol{G}$ takes linear time in the number of monomials $O(n\binom{n+d}{d})$ and gives us $\boldsymbol{G}^{[\lambda]}$. We then invoke $\mathsf{Symmetric_Coordinates}(\lambda, \boldsymbol{G}^{[\lambda]})$, using Lemma 9.3.1, in order to obtain $\bar{\boldsymbol{G}}^{[\lambda]}$ with the cost being $O^{\sim}(n\binom{n+d}{d})^2$ operations in $\mathbb{K}$.

In the second case, we obtain $\boldsymbol{G}^{[\lambda]}$ as above. We also compute the matrix $\mathrm{Jac}(\boldsymbol{G}, \phi)$, which takes $O(n^2\binom{n+d}{d})$ operations. For the same cost, we apply $\mathbb{T}_\lambda$ to all its entries and remove redundant columns, as specified in Lemma 10.1.4, so as to yield the matrix $\boldsymbol{F}^{[\lambda]}$. We then apply Algorithm Symmetrize from Proposition 9.3.11 to all $(s+1)$ rows of $\boldsymbol{F}^{[\lambda]}$, which takes $O^{\sim}(n^4\binom{n+d}{d})$ operations, and returns $\boldsymbol{H}^{[\lambda]}$. Finally, we apply Symmetric_Coordinates to all entries of this matrix which gives $\bar{\boldsymbol{H}}^{[\lambda]}$ and takes $O^{\sim}(n^2\binom{n+d}{d}^2)$ operations in $\mathbb{K}$. □

10.3.2 The complexity of the WeightedColumnDegree procedure

Recall that on input polynomials $\boldsymbol{G}$, a polynomial matrix $\boldsymbol{H}$ and an integer k, Algorithm WeightedColumnDegree returns a zero-dimensional parametrization of the isolated points of $V(\boldsymbol{G}, M_k(\boldsymbol{H}))$, where $M_k(\boldsymbol{H})$ denotes the set of k-minors of $\boldsymbol{H}$. We apply this procedure to polynomials with entries in $\mathbb{K}[\boldsymbol{e}_1, \dots, \boldsymbol{e}_r] = \mathbb{K}[e_{1,1}, \dots, e_{1,\ell_1}, e_{2,1}, \dots, e_{2,\ell_2}, \dots, e_{r,1}, \dots, e_{r,\ell_r}]$. Estimating the runtimes for the WeightedColumnDegree algorithms follows from Theorem

7.2.2, for the weighted domains associated to various partitions of n. Thus we let $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \dots\, n_r^{\ell_r})$ be a partition of length ℓ, with $\ell \geq s$.

The parameters that appear in Theorem 7.2.2 can be determined as follows. The weights of variables $(\boldsymbol{e}_1, \dots, \boldsymbol{e}_r)$ are $\boldsymbol{w} = (1, \dots, \ell_1, \dots, 1, \dots, \ell_r)$. For $i = 1, \dots, s$, the weighted degree of $\bar{g}_i^{[\lambda]}$ is the same as the degree of $g_i^{[\lambda]}$ and so is at most d.

Note that all entries of the Jacobian matrix of $\boldsymbol{G}, \phi$ have degree at most $d-1$, then using Proposition 9.3.8, for $j = 1, \dots, \ell$, the weighted column degree of the j-th column of $\bar{\boldsymbol{H}}^{[\lambda]}$ is at most $\delta_j = d - 1 - \ell + j$. In particular, if $\ell > d$, then all entries on the j-th column of $\bar{\boldsymbol{H}}^{[\lambda]}$ equal zero for $j = 1, \dots, \ell - d$. Finally, in what follows, we let

$$\Gamma = n^2 \binom{n+d}{d} + n^4 \binom{n}{s+1}.$$

Partitions of length s. We recall that when the length ℓ of the partition λ equals s, we do not need to deal with a matrix $\bar{\boldsymbol{H}}^{[\lambda]}$. In this situation, one only needs to compute the isolated points of $V(\bar{\boldsymbol{G}}^{[\lambda]})$.

Consider a partition $\lambda = (n_1^{\ell_1}\, n_2^{\ell_2}\, \dots\, n_r^{\ell_r})$ and the corresponding variables $(\boldsymbol{e}_1, \dots, \boldsymbol{e}_r)$, with $\mathrm{wdeg}(e_{i,k}) = k$ for all $i = 1, \dots, r$ and $k = 1, \dots, \ell_i$. We make the following claim: *if there exists i such that $\ell_i > d$, then there is no isolated point in $V(\bar{\boldsymbol{G}}^{[\lambda]})$.* Indeed, in such a case, variable e_{i,ℓ_i} does not appear in $\bar{\boldsymbol{G}}^{[\lambda]}$, for weighted degree reasons, so that the zero-set of this system is invariant with respect to translations along the e_{i,ℓ_i} axis. In particular, it admits no isolated solution.

Therefore we can suppose that all ℓ_i's are at most d. In this case, the quantities c, e, κ used in Theorem 7.2.2 become respectively

$$\mathfrak{c}_\lambda = \frac{d^s}{w_\lambda}, \quad \mathfrak{e}_\lambda = \frac{n(d+1)^s}{w_\lambda}, \quad \kappa_\lambda = d^s = w_\lambda \mathfrak{c}_\lambda,$$

with $w_\lambda = \ell_1! \cdots \ell_r!$. In this case Theorem 7.2.2 implies that $V(\bar{\boldsymbol{G}}^{[\lambda]})$ contains at most $\mathfrak{c}_\lambda$ isolated points, and one can compute all of them using

$$O^{\sim}\left(\left(\mathfrak{c}_\lambda(\mathfrak{e}_\lambda + \mathfrak{c}_\lambda^5) + d^2\mathfrak{c}_\lambda^2\right) n^4 \Gamma_\lambda\right) \subset O^{\sim}\left(d^2 \mathfrak{c}_\lambda (\mathfrak{e}_\lambda + \mathfrak{c}_\lambda^5) n^4 \Gamma\right)$$

operations in $\mathbb{K}$.

Partitions of length greater than s. For a partition λ of length ℓ greater than s, we have to take into account the minors of the matrix $\bar{\boldsymbol{H}}^{[\lambda]}$. Note that the assumptions of Theorem 7.2.2 are satisfied: the matrix $\bar{\boldsymbol{H}}^{[\lambda]}$ is in $\mathbb{K}[\boldsymbol{e}_1, \dots, \boldsymbol{e}_r]^{(s+1)\times \ell}$, with $\ell \geq s+1$, and we have s equations $\bar{\boldsymbol{G}}^{[\lambda]}$ in $\mathbb{K}[\boldsymbol{e}_1, \dots, \boldsymbol{e}_r]$, so the number of variables ℓ does indeed satisfy $\ell = \ell - (s+1) + s + 1$.

We claim that if $\ell > d$, then the algebraic set $V_{s+1}(\bar{\boldsymbol{H}}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]})$ does not have any isolated point. Indeed, in this case, we pointed out above that the columns of indices 1 to $\ell - d$

in $\bar{\boldsymbol{H}}^{[\lambda]}$ are identically zero. After discarding these zero-columns from $\bar{\boldsymbol{H}}^{[\lambda]}$, we obtain a matrix $\boldsymbol{L}^{[\lambda]}$ of size $(s+1)\times d$ such that $V_{s+1}(\bar{\boldsymbol{H}}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]}) = V_{s+1}(\boldsymbol{L}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]})$, and using Remark 4.1.1 with $p = s+1, q = d$, $s+1$ extra polynomials and $n \geq \ell$ shows that this algebraic set has no isolated points.

Thus, let us now assume that $\ell \leq d$. The matrix $\bar{\boldsymbol{H}}^{[\lambda]}$ has weighted column degrees $(\delta_1, \ldots, \delta_\ell) = (d-\ell, \ldots, d-1)$, whereas the weighted degrees of all polynomials in $\bar{\boldsymbol{G}}^{[\lambda]}$ is at most d. To estimate the runtime of $\mathsf{WeightedColumnDegree}(\bar{\boldsymbol{H}}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]})$, we will need the following property.

Lemma 10.3.2. *Let κ be defined as in (7.14) with $n = \ell$, $p = s+1$, $q = \ell$, $s+1$ extra polynomials, $(\delta_1, \ldots, \delta_\ell) = (d-1-\ell, \ldots, d-1)$, and $(\gamma_1, \ldots, \gamma_s) = (d, \ldots, d)$. Then, for partitions of length ℓ at most d, one has*

$$\kappa = d^s \eta_{\ell-s}(d-1, \ldots, d-\ell).$$

Proof. Without loss of generality, we reorder the weights $\boldsymbol{w}$ as $\boldsymbol{w}' = (w'_1, \ldots, w'_\ell)$ such that $w'_1 \leq \cdots \leq w'_\ell$.

Take $\boldsymbol{i} = (i_1, \ldots, i_{\ell-s}) \subset \{1, \ldots, \ell\}$, and let $d_{\boldsymbol{i}} = (d_{\boldsymbol{i},1}, \ldots, d_{\boldsymbol{i},\ell})$ be the sequence obtained by reordering $(\delta_{i_1}, \ldots, \delta_{i_{\ell-s}}, d, \ldots, d)$; we first compute the value of $\kappa_{\boldsymbol{i}}$ from (7.14). If $d_{\boldsymbol{i},1} = 0$ (which can happen only if $\ell = d$), then $\kappa_{\boldsymbol{i}} = 0$. Otherwise, the sequence $d_{\boldsymbol{i}}$ starts with $d_{\boldsymbol{i},1} \geq 1$ and increases until index $\ell - s$, after which it keeps the value d. On the other hand, the ordered sequence of weights never increases by more than 1, so that for all $k = 1, \ldots, \ell$, we have $w'_k \leq d_{\boldsymbol{i},k}$. In this case,

$$\kappa_{\boldsymbol{i}} = \max_{1\leq k\leq \ell}(d_{\boldsymbol{i},1} \cdots d_{\boldsymbol{i},k} w_{k+1} \cdots w_m) = d_{\boldsymbol{i},1} \cdots d_{\boldsymbol{i},\ell} = d^s \delta_{i_1} \cdots \delta_{i_{\ell-s}};$$

note that this equality also holds if $d_{\boldsymbol{i},1} = 0$, since then both sides vanish. Since $\kappa = \sum_{\boldsymbol{i}=\{i_1,\ldots,i_{\ell-s}\}\subset\{1,\ldots,q\}} \kappa_{\boldsymbol{i}}$, we get

$$\kappa = \sum_{\boldsymbol{i}=\{i_1,\ldots,i_{\ell-s}\}\subset\{1,\ldots,\ell\}} d^s \delta_{i_1} \cdots \delta_{i_{\ell-s}} = d^s \eta_{\ell-s}(d-1, \ldots, d-\ell). \tag{10.8}$$

as claimed. □

The procedure $\mathsf{WeightedColumnDegree}\big(\bar{\boldsymbol{H}}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]}\big)$ then uses the algorithm in Theorem 7.2.2 with input $\big(\bar{\boldsymbol{H}}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]}\big)$. Writing as before $w_\lambda = \ell_1! \cdots \ell_r!$, the quantities used in the theorem become

$$\begin{aligned}
\mathfrak{c}_\lambda &= \frac{d^s \eta_{\ell-s}(d-1, \ldots, d-\ell)}{w_\lambda}, \\
\mathfrak{e}_\lambda &= \frac{n(d+1)^s \eta_{\ell-s}(d, \ldots, d-\ell+1)}{w_\lambda}, \\
\kappa_\lambda &= d^s \eta_{\ell-s}(d-1, \ldots, d-\ell) = w_\lambda \mathfrak{c}_\lambda.
\end{aligned}$$

This implies that running $\mathsf{WeightedColumnDegree}\left(\bar{\boldsymbol{H}}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]}\right)$ uses

$$O^{\sim}\left(\left(\mathfrak{c}_\lambda(\mathfrak{e}_\lambda + \mathfrak{c}_\lambda^5) + d^2\mathfrak{c}_\lambda^2\right)n^4\Gamma\right)$$

operations which is again in

$$O^{\sim}\left(d^2\mathfrak{c}_\lambda(\mathfrak{e}_\lambda + \mathfrak{c}_\lambda^5)n^4\Gamma\right).$$

As before, the number of solutions in the output is at most $\mathfrak{c}_\lambda$.

10.3.3 Finishing the proof of Theorem 8.1.1

We can now finish estimating the runtime of the Critical_Points_Per_Orbit Algorithm. For partitions of length s, at Step 2a, we only need to compute $\bar{\boldsymbol{G}}^{[\lambda]}$ which takes $O^{\sim}(n\binom{n+d}{d}^2)$ operations in $\mathbb{K}$ as per Lemma 10.3.1. At Step 2b, the procedure $\mathsf{WeightedColumnDegree}(\bar{\boldsymbol{G}}^{[\lambda]})$ takes at most $O^{\sim}\left(d^2\mathfrak{c}_\lambda(\mathfrak{e}_\lambda + \mathfrak{c}_\lambda^5)n^4\Gamma\right)$ operations in $\mathbb{K}$, as we saw in Subsection 10.3.2. The output of this procedure contains at most $\mathfrak{c}_\lambda$ points; then, by Lemma 9.2.3, the cost of the call to Decompose at Step 2c is $O^{\sim}(\mathfrak{c}_\lambda^2\, n)$, which is negligible compared to the previous costs.

For partitions of length greater than s, computing $\bar{\boldsymbol{G}}^{[\lambda]}$ and $\bar{\boldsymbol{H}}^{[\lambda]}$ at Step 3a takes $O^{\sim}(n^4\binom{n+d}{d}^2)$ operations in $\mathbb{K}$, by Lemma 10.3.1. At Step 3b, the procedure $\mathsf{WeightedColumnDegree}\left(\bar{\boldsymbol{H}}^{[\lambda]}, \bar{\boldsymbol{G}}^{[\lambda]}\right)$ requires at most $O^{\sim}\left(d^2\mathfrak{c}_\lambda(\mathfrak{e}_\lambda + \mathfrak{c}_\lambda^5)n^4\Gamma\right)$ operations in $\mathbb{K}$, as we saw in Subsection 10.3.2. Again, since the number of solutions in the output is at most $\mathfrak{c}_\lambda$, the cost of Decompose at Step 3c is still $O^{\sim}(\mathfrak{c}_\lambda^2\, n)$ which, as before, is negligible in comparison to the other costs. To complete our analysis, we need the following lemma.

Lemma 10.3.3. *With all notation being as above, the following holds*

$$\sum_{\lambda\vdash n, \ell_\lambda \geq s} \mathfrak{c}_\lambda \leq \mathfrak{c} \quad \text{and} \quad \sum_{\lambda\vdash n, \ell_\lambda \geq s} \mathfrak{e}_\lambda \leq \mathfrak{e},$$

where $\mathfrak{c} = d^s\binom{n+d-1}{n}$ *and* $\mathfrak{e} = n\,(d+1)^s\binom{n+d}{n}$.

Proof. The proof relies on the combinatorics of integer partitions and properties of elementary symmetric functions. To simplify our notation, for all $1 \leq s \leq \ell$, we abbreviate $\eta_{\ell-s}(d-1, \ldots, d-\ell)$ to $g_{\ell-s}$. Then, we claim that one has

$$g_{\ell-s} < d(d-1)\cdots(d-\ell+1).$$

Indeed, let $f(t) = (t+d-1)(t+d-2)\cdots(t+d-\ell)$, so that $f(1) = d(d-1)\cdots(d-\ell+1)$. From Vieta's formula we have

$$f(t) = \sum_{s=0}^{\ell} g_{\ell-s}\, t^s$$

and so we also have $f(1) = \sum_{s=0}^{\ell} g_{\ell-s}$. Therefore,

$$d(d-1)\cdots(d-\ell+1) = \sum_{s=0}^{\ell} g_{\ell-s}$$

and so $g_{\ell-s} < d(d-1)\cdots(d-\ell+1)$ for all $1 \le s \le \ell$.

Now, for any partition $\lambda = (n_1^{\ell_1} \ \dots \ n_r^{\ell_r}) \vdash n$ of length ℓ_λ, we have

$$\begin{aligned} \mathfrak{c}_\lambda &= d^s \frac{g_{\ell_\lambda - s}}{w_\lambda} \quad \text{with} \quad w_\lambda = \prod_{i=1}^{r} \ell_i! \\ &= d^s \frac{\ell_\lambda!}{\prod_{i=1}^r \ell_i!} \frac{g_{\ell_\lambda - s}}{\ell_\lambda!} \\ &= d^s h(\lambda)\, \mathscr{F}_{d,\ell_\lambda,s}, \end{aligned}$$

where $h(\lambda) = \frac{\ell_\lambda!}{\prod_{i=1}^r \ell_i!} = \binom{\ell_\lambda}{\ell_1,\dots,\ell_r}$ and $\mathscr{F}_{d,\ell_\lambda,s} = \frac{g_{\ell_\lambda - s}}{\ell_\lambda!}$. From our previous inequality we have

$$\mathscr{F}_{d,\ell_\lambda,s} \le \frac{d(d-1)\cdots(d-\ell_\lambda+1)}{\ell_\lambda!} = \binom{d}{\ell_\lambda}$$

and so

$$\sum_{\lambda\vdash n,\, \ell_\lambda \ge s} \mathfrak{c}_\lambda \le d^s \left(\sum_{\lambda\vdash n,\, \ell_\lambda \ge s} h(\lambda) \binom{d}{\ell_\lambda} \right). \tag{10.9}$$

Let $\mathbf{a}$ be a sequence of $m+1$ numbers $(a_0, a_1, \dots, a_m)$ and let $p_{\mathbf{a}}(t) = \sum_{i=0}^m a_i\, t^i$ be its generating polynomial. The *polynomial coefficients* associated to $\mathbf{a}$ are defined by

$$\binom{k}{n}_{\mathbf{a}} = \begin{cases} [t^n]\,(p_{\mathbf{a}}(t)^k), & \text{if } 0 \le n \le mk \\ 0, & \text{if } n < 0 \text{ or } n > mk \end{cases}$$

where $[t^n] \sum_i c_i t_i = c_n$ is the coefficient of t^n in the series $\sum_i c_i t_i$. For any partition λ of n, let further λ' be its conjugate partition. By [57, Lemma 2.1], we have

$$\binom{k}{n}_{\boldsymbol{a}} = \sum_{\substack{\lambda\vdash n, \\ \ell_{\lambda'} \le n}} a_0^{k-\ell_{\lambda'}}\, h(\lambda) w_{\boldsymbol{a}}(\lambda) \binom{k}{\ell_\lambda}, \tag{10.10}$$

where $w_{\boldsymbol{a}}(\lambda)$ is the function $w_{\boldsymbol{a}}(\lambda) = \prod_{i=1}^m a_i^{\ell_i}$, and $\ell_\lambda, \ell_{\lambda'}$ are the respective lengths of λ and λ'. If we consider $m = n$, $\boldsymbol{a} = (1, \dots, 1) = \mathbf{1}$ and $k = d$, then equation (10.10) becomes

$$\binom{d}{n}_{\mathbf{1}} = \sum_{\substack{\lambda\vdash n, \\ \ell_{\lambda'} \le n}} h(\lambda) \binom{d}{\ell_{\lambda'}}.$$

For any partition λ of n, the length of its conjugate satisfies $\ell_{\lambda'} \leq n$ and so

$$[t^n](1+t+\cdots+t^n)^d = \binom{d}{n}_{\mathbf{1}} = \sum_{\lambda \vdash n} h(\lambda)\binom{d}{\ell_\lambda}. \tag{10.11}$$

Furthermore,

$$(1+t+\cdots+t^n)^d \;=\; (1-t^{n+1})^d\,(1-t)^d = \Big(\sum_{k=0}^{d}(-1)^k\binom{d}{k}t^{(n+1)k}\Big)\Big(\sum_{i=0}^{\infty}\binom{d+i-1}{i}t^i\Big),$$

where t^n appears only when $k=0$ and $i=n$. In other words,

$$[t^n]\,(1+t+\cdots+t^n)^d = \binom{n+d-1}{n}. \tag{10.12}$$

Combining (10.9), (10.11) and (10.12), gives

$$\sum_{\lambda\vdash n,\,\ell_\lambda \geq s} \mathfrak{c}_\lambda \leq d^s\left(\sum_{\lambda\vdash n} h(\lambda)\binom{d}{\ell_\lambda}\right) \leq d^s\binom{n+d-1}{n}.$$

We prove the inequality $\sum_{\lambda\vdash n,\,\ell_\lambda\geq s}\mathfrak{e}_\lambda \leq n(d+1)^s\binom{n+d}{n}$ similarly. □

As a result, the total cost of

$$O^{\sim}\left(\mathfrak{c}(\mathfrak{e}+\mathfrak{c}^5)n^9d^2\left(\binom{n+d}{d}+\binom{n}{s+1}\right)\right)$$

is incurred by our calls to WeightedColumnDegree and Decompose. Since $\binom{n+d}{d} \leq (n+1)\binom{n+d-1}{d}$, we will simplify this further, by noticing that for $d\geq 2$ we have

$$\mathfrak{e} = n\,(d+1)^s\binom{n+d}{n} \leq n(n+1)d^{5s}\binom{n+d-1}{n}^5 = n(n+1)\mathfrak{c}^5$$

so this is

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

For the remaining operations, the total cost of Prepare_G and Prepare_G_H is

$$n^4\sum_{\lambda\vdash n,\ell_\lambda\geq s}\binom{n+d}{d}^2.$$

Since $\binom{n+d}{d} \leq (n+1)\binom{n+d-1}{d}$, the binomial term in the sum is in $O(n^2\mathfrak{c}^2)$, so the total is $O(n^5\mathfrak{c}^3)$, and can be neglected. Similarly, the cost of Remove_Duplicates is negligible. Therefore, the total complexity of Critical_Points_Per_Orbit is then in

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

Finally, the total number of solutions reported by our algorithm is at most $\sum_{\lambda\vdash n,\ell_\lambda\geq s}\mathfrak{c}_\lambda$, which itself is at most $\mathfrak{c}$.

10.4 Experimental results

In this section, we report on an implementation and set of experimental runs supporting the results in this paper. We compare our Critical_Points_Per_Orbit algorithm from Section 10.2 with a naive algorithm which computes a zero-dimensional parametrization of $V(I)$, where I is the ideal generated by $\boldsymbol{G}$ and the $(s+1)$-minors of $\mathrm{Jac}(\boldsymbol{G}, \phi)$. Since no implementation of the weighted determinantal homotopy algorithms is available at the moment, both algorithms use Gröbner bases computations to solve polynomial systems. Furthermore, using Gröbner bases computations is sufficient to see the advantage of our algorithm when the symmetric structure is exploited in our algorithm.

Our experiments are run using the Maple computer algebra system running on a computer with 16 GB RAM; the Gröbner basis computation in Maple uses the implementation of the F_4 and FGLM algorithms from the FGb package [60]. The symmetric polynomials $\boldsymbol{G}$ and ϕ are chosen uniformly at random in $\mathbb{K}[x_1, \ldots, x_n]$, with $\mathbb{K} = \mathrm{GF}(65521)$, and have the same degree n as the number of variables, that is, $\deg(g_1) = \cdots = \deg(g_s) = \deg(\phi) = n$; the number s of equations $\boldsymbol{G}$ ranges from 2 to $n-1$.

Our experimental results support the theoretical advantage gained by exploiting the symmetric structure of the input polynomials. In Table 10.1, we first report the number of points, denoted by D, that we compute using our algorithm; that is, D is the sum of the degrees $\deg(\mathscr{R}_\lambda)$ that we obtain for all partitions λ of length at least s. The next column is $\left\lceil \sum_{\ell_\lambda \geq s} \mathfrak{c}_\lambda \right\rceil$, which is an upper bound on D (here, $\mathfrak{c}_\lambda$ is as in Subsection 10.3.2); as we can see, this bound is quite sharp in general. We next give the upper bound $\mathfrak{c}$ from (8.3), which we proved in Lemma 10.3.3. While this bound is sufficient to prove asymptotic results (for fixed input degree, for instance, see the discussion in the introduction), we see that it is far from sharp.

Finally, we give the number of points $\deg(I)$ computed by the naive algorithm, together with the upper bound $\tilde{\mathfrak{c}}$ from (8.4); in some cases, we did not complete computations with the naive algorithm, so $\deg(I)$ was unavailable. We see that in all cases, the output of our algorithm is significantly smaller than the one from the direct approach.

n	s	D	$\lceil \sum_{\ell_\lambda \geq s} \mathfrak{c}_\lambda \rceil$	$\mathfrak{c}$	$\deg(I)$	$\tilde{\mathfrak{c}}$
4	2	79	80	560	856	864
4	3	47	48	2240	744	768
5	2	425	432	3150	15575	16000
5	3	357	370	15750	18760	20000
5	4	143	157	78750	11160	12500
6	2	2222	2227	16632	-	337500
6	3	2439	2453	99792	-	540000
6	4	1482	1503	598752	-	486000
6	5	470	486	3592512	-	233280

Table 10.1: Degrees and bounds

In Table 10.2, we report on our timings in a detailed fashion. Here, we give the time needed to compute the zero-dimensional representations $\deg(\mathscr{R}_\lambda)$ obtained by our algorithm, together with their degrees; Time(total) denotes the total time spent in our algorithm. On the other hand, Time(naive) is the time to compute a zero-dimensional parametrization for the algebraic set $V(I)$ using the naive algorithm. Experiments are stopped once the computation has gone past 24 hours, with the corresponding time marked with a dash.

In our experiments, the output $\mathscr{R}_\lambda$ was always empty for partitions of length less than s. Indeed, for any partition λ of length at most $s-1$, $Z(\mathscr{R}_\lambda) = V(\bar{g}_1^{[\lambda]}, \ldots, \bar{g}_s^{[\lambda]})$, where the $\bar{g}_i^{[\lambda]}$ are s polynomials in less than variables derived from the input $\boldsymbol{G}$. Since the polynomials $\boldsymbol{G}$ are chosen at random, the evaluated block symmetric polynomials $g_1^{[\lambda]}, \ldots, g_s^{[\lambda]}$ are generic. Furthermore, it is also possible to prove that in this case, $V(\bar{g}_1^{[\lambda]}, \ldots, \bar{g}_s^{[\lambda]})$ is empty in $\overline{\mathbb{K}}^\ell$. Therefore, $Z(\mathscr{R}_\lambda)$ to be empty for such partitions λ of length less than s. However, we point out that this output can be non-trivial in the general, non-generic case.

n	s	Partition(λ)	Time($\mathscr{R}_\lambda$)	deg($\mathscr{R}_\lambda$)	$\lceil \mathfrak{c}_\lambda \rceil$	Time(total)	Time(naive)	deg(I)
4	2	$\lambda = (1^4)$	1.524s	7	8	3.136s	0.905s	856
		$\lambda = (1^2\,2^1)$	0.684s	48	48			
		$\lambda = (2^2)$	0.200s	8	8			
		$\lambda = (1^1 3^1)$	0.380s	16	16			
4	3	$\lambda = (1^4)$	2.497s	15	16	4.468s	0.577s	744
		$\lambda = (1^2\,2^1)$	0.772s	32	32			
5	2	$\lambda = (1^5)$	9.236s	9	11	34.944s	2143.144s	15575
		$\lambda = (1^3\,2^1)$	6.832s	142	146			
		$\lambda = (1^2\,3)$	2.128s	112	113			
		$\lambda = (1^1\,2^2)$	2.816s	112	113			
		$\lambda = (1^1\,4^1)$	0.316s	25	25			
		$\lambda = (2^1\,3^1)$	0.392s	25	25			
5	3	$\lambda = (1^5)$	18.829s	31	37	48.019s	3423.660s	18760
		$\lambda = (1^3\,2^1)$	18.120s	202	209			
		$\lambda = (1^2\,3)$	4.607s	62	63			
		$\lambda = (1^1\,2^2)$	5.316s	62	63			
5	4	$\lambda = (1^5)$	17.080s	44	53	37.372s	969.396s	11160
		$\lambda = (1^3\,2^1)$	12.024s	99	105			
6	2	$\lambda = (1^6)$	44.979s	13	14	861.888s	-	-
		$\lambda = (1^4\,2^1)$	94.240s	334	338			
		$\lambda = (1^3\,3)$	110.615s	426	426			
		$\lambda = (1^2\,2^2)$	413.351s	639	639			
		$\lambda = (2^3)$	7.241s	72	72			
		$\lambda = (1^2\,4^1)$	15.208s	216	216			
		$\lambda = (1^1\,2^1\,3^1)$	92.589s	432	432			
		$\lambda = (1^1\,5^1)$	0.756s	36	36			
		$\lambda = (2^1\,4^1)$	1.072s	36	36			
		$\lambda = (3^2)$	0.956s	18	18			
6	3	$\lambda = (1^6)$	92.881s	63	68	1658.071s	-	-
		$\lambda = (1^4\,2^1)$	773.924s	756	765			
		$\lambda = (1^3\,3)$	114.064s	504	504			
		$\lambda = (1^2\,2^2)$	495.432s	756	756			
		$\lambda = (2^3)$	7.356s	36	36			
		$\lambda = (1^2\,4^1)$	9.236s	108	108			
		$\lambda = (1^1\,2^1\,3^1)$	17.908s	216	216			
6	4	$\lambda = (1^6)$	98.312s	142	153	842.256s	-	-
		$\lambda = (1^4\,2^1)$	591.78s	800	810			
		$\lambda = (1^3\,3)$	26.196s	216	216			
		$\lambda = (1^2\,2^2)$	46.420s	324	324			
6	5	$\lambda = (1^6)$	154.808s	150	162	251.752s	-	-
		$\lambda = (1^4\,2^1)$	121.768s	320	324			

Table 10.2: Algorithm timings

Chapter 11

Conclusions and Topics for Future Research

11.1 Conclusions

In the first part of the thesis, we have provided determinantal homotopy algorithms to compute the isolated and simple points of the set of the points at which a given sequence of polynomials $\boldsymbol{G}$ and a polynomial matrix $\boldsymbol{F}$ is not full rank. Our algorithms take into account all structures of the inputs such as when

- all polynomials $\boldsymbol{G}$ and entries of $\boldsymbol{F}$ are dense and belong to classical polynomial rings;
- all polynomials $\boldsymbol{G}$ and entries of $\boldsymbol{F}$ are sparse;
- all polynomials $\boldsymbol{G}$ and entries of $\boldsymbol{F}$ are in weighted domains.

For each situation, we also give a bound for the sum of the multiplicities of the isolated points that our algorithm needs to compute. While in the dense case, we study two degree measures for the matrix $\boldsymbol{F}$, the row-degree and the column-degree, in the sparse case (resp. the weighted case), we consider only one measure which is called the column-support (resp. the weighed column-degree). Note that our column supported homotopy algorithm is used to the case where our entries come from a weighted polynomial domain. Such weighted domains arise when we determine the isolated critical points of a symmetric function ϕ defined over a variety $V(\boldsymbol{G})$ generated by symmetric functions in $\boldsymbol{G}$.

In the second half of the thesis, we have provided a new algorithm for efficiently describing the critical point set of a function ϕ a variety $V(\boldsymbol{G})$ with ϕ and the defining functions of the variety all symmetric. The algorithm takes advantage of the symmetries and lower bounds for describing the generators of the set of critical points and as a result is more efficient than previous approaches.

When $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{R}[x_1, \ldots, x_n]$, with $\mathbb{R}$ is a real field, then computing the critical points of polynomial maps restricted to $V(\boldsymbol{G})$ finds numerous applications in computational real algebraic geometry. In particular such computations provide an effective Morse-theoretic approach to many problems such as real root finding, quantifier elimination or answering connectivity queries (see [20]). We view the complexity estimates in our result as a possible first step towards better algorithms for studying real algebraic sets defined by $\mathcal{S}_n$-invariant polynomials.

For instance, let d be the maximum degree of the entries in $\boldsymbol{G} = (g_1, \ldots, g_s)$ and assume that $\boldsymbol{G}$ generates an $(n-s)$-equidimensional ideal whose associated algebraic set is smooth. Then under these assumptions, we observe that the set $W(\phi_u, \boldsymbol{G})$ with

$$\phi_u : (x_1, \ldots, x_n) \to (x_1 - u)^2 + \cdots + (x_n - u)^2$$

and $u \in \mathbb{R}$, has a non-empty intersection with all connected components of $V(\boldsymbol{G}) \cap \mathbb{R}^n$. Hence, when $W(\phi_u, \boldsymbol{G})$ is finite for a generic choice of u, then one can use our algorithm to decide whenever $V(\boldsymbol{G}) \cap \mathbb{R}^n$ is empty. This is done in time polynomial in $d^s, \binom{n+d}{d}, \binom{n}{s+1}$.

In such cases, for d, s fixed, we end up with a runtime which is polynomial in n as in [172, 149, 150]. These latter references are restricted to situations when $d < n$ is fixed. If now, one takes families of systems where $d = n$ and s is fixed, we obtain a runtime which is polynomial in 2^n. This is an exponential speed-up with the best previous possible alternatives which run in time $2^{O(n \log(n))}$ as in for example [20, Chapter 13] (but note that these algorithms are designed for general real algebraic sets).

Obtaining an algorithm to decide whether $V(\boldsymbol{G}) \cap \mathbb{R}^n$ is empty in time polynomial in $d^s, \binom{n+d}{d}, \binom{n}{s+1}$, without assuming that $W(\phi_u, \boldsymbol{G})$ is finite for a generic $u \in \mathbb{R}$, is still an open problem.

11.2 Topics for future work

Row supported homotopy algorithms. Still regarding critical point computations, but for non symmetric input $\boldsymbol{F}, \boldsymbol{G}$ the natural bounds for a sparse homotopy would come from considering the row support rather than the column support of $\boldsymbol{F}$. An interesting approach would be the follow the algorithm given in Section 6.3. for dense polynomials using the row-homotopy algorithms. However, proving that in the sparse case, the corresponding start systems satisfy the genericity properties we need is not straightforward.

Infinite number of critical points of invariant systems. When our algorithm is applied in the deciding the emptiness of an invariant algebraic set over real fields, we have assumed that the set $W(\phi_u, \boldsymbol{G})$ is finite. It would be nice if we can remove this assumption in the future work.

Computing critical points for invariant systems under some other groups. Our results for computing critical points for invariant systems hold when the systems are invariant under the action of the symmetric group $\mathcal{S}_n$. A nice property in the symmetric polynomial ring $\mathbb{K}[x_1, \ldots, x_n]^{\mathcal{S}_n}$ is that any polynomial f lying on this ring can be represented by using unique polynomial $\bar{f}$ in $\mathbb{K}[e_1, \ldots, e_n]$ such that $\bar{f}(\eta_1(\boldsymbol{X}), \ldots, \eta_n(\boldsymbol{X})) = f(\boldsymbol{X})$, where $\eta_k(\boldsymbol{X})$ is the k-th elementary symmetric function in $\boldsymbol{X} = (x_1, \ldots, x_n)$. Therefore, instead of working with polynomials in $\mathbb{K}[\boldsymbol{X}]$, we can do our computation on the ring $\mathbb{K}[e_1, \ldots, e_n]$, which some how help us to reduce the number of computations by $n!$. However, when polynomial f is invariant under the action of other groups, in general, the process of working with a new polynomial $\bar{f}$ might not be hold. Our next goal is to study how can we exploit the invariance properties of some other groups rather than the symmetric group $\mathcal{S}_n$.

Homotopy algorithms for the MinRank problem. Consider a matrix $\boldsymbol{F}$ of size $p \times q$, with all entries are in $\mathbb{K}[x_1, \ldots, x_n]$, and a positive integer r. The MinRank problem is finding points in $\overline{\mathbb{K}}^n$ at which the matrix $\boldsymbol{F}$ has rank at most r. Our results in Part I, in the case there are no extra polynomials $\boldsymbol{G}$, of the thesis study a particular case of the MinRank problem with $r = \min(p, q) - 1$. Faugère et al. [66] give new complexity bounds for solving the MinRank problem using Gröbner bases algorithms under genericity assumptions on the input matrix $\boldsymbol{F}$. One of our next goals is to study how to use the homotopy continuation methods in order to solve the MinRank problem, without any genericity assumptions on the input. A primary goal is studying the case when $n = (p-r)(q-r)$. Recall that, in this case, when all entries of $\boldsymbol{F}$ are generic, the ideal generated by its r-minors is zero-dimensional.

Gröbner basis computation for sparse and weighted determinantal ideals. Given a matrix $\boldsymbol{F}$ in classical polynomial rings. Gröbner basis computation is well understood for dense determinantal ideals and the ideals define critical points (see [65, 66, 167] and references therein). However, to the best of our knowledge, there is no previous work which study Gröbner bases algorithms for the determinantal ideals of $\boldsymbol{F}$ when all entries of $\boldsymbol{F}$ are either sparse or in a weighted polynomial ring. We consider this problem as one of topics for future work.

References

[1] G. Agnarsson. On the Sylvester denumerants for general restricted partitions. *Congressus numerantium*, pages 49–60, 2002.

[2] M. K Agoston. *Computer Graphics and Geometric Modeling*, volume 1. Springer, 2005.

[3] G. B.-D. Aharon. Lower and upper bounds for the number of lattice points in a simplex. *SIAM Journal on Applied Mathematics*, 22(1):106–108, 1972.

[4] E. L. Allgower and K. Georg. *Numerical Continuation Methods: An Introduction*, volume 13. Springer Science & Business Media, 2012.

[5] M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In *Algorithms in Algebraic Geometry and Applications*, pages 1–15. Springer, 1996.

[6] M. Atiyah and I. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. Addison-Wesley, 1969.

[7] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[8] J. L. Balcázar, J. Diaz, and J. Gabarró. *Structural Complexity II*, volume 22. Springer Science & Business Media, 2012.

[9] 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.

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

[11] B. Bank, M. Giusti, J. Heintz, and G.M. Mbakop. Polar varieties, real equation solving, and data structures. *Journal of Complexity*, 13(1):5–27, March 1997.

[12] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties: geometry and algorithms. *Journal of Complexity*, 21(4):377–412, 2005.

[13] 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.

[14] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and É. Schost. On the geometry of polar varieties. *Applicable Algebra in Engineering, Communication and Computing*, pages 33–83, 2010.

[15] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* PhD thesis, Université Pierre et Marie Curie - Paris VI, 2004.

[16] M. Bardet. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. *MEGA'05*, 2005.

[17] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

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

[19] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier elimination and cylindrical algebraic decomposition*, pages 341–350. Springer, 1998.

[20] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics).* Springer-Verlag, Berlin, Heidelberg, 2006.

[21] S. Basu, M.-F. Roy, M. Safey El Din, and É. Schost. A baby-step giant-step roadmap algorithm for general real algebraic sets. *Foundations of Computational Mathematics*, 14(6):1117–1172, 2014.

[22] D. J. Bates, D. A. Brake, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. On computing a cell decomposition of a real surface containing infinitely many singularities. In *Mathematical software—ICMS 2014*, volume 8592 of *Lecture Notes in Comput. Sci.*, pages 246–252. Springer, Heidelberg, 2014.

[23] D. J. Bates, J. D. Hauenstein, C. Peterson, and A. J. Sommese. A numerical local dimension test for points on the solution set of a system of polynomial equations. *SIAM Journal on Numerical Analysis*, 47(5):3608–3623, 2009.

[24] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoretical computer science*, 22(3):317–330, 1983.

[25] D. Bayer and D. Mumford. What can be computed in algebraic geometry? *arXiv preprint alg-geom/9304003*, 1993.

[26] B. Beckermann and G. Labahn. A uniform approach for the fast computation of matrix-type padé approximants. *SIAM Journal on Matrix Analysis and Applications*, 15(3):804–823, 1994.

[27] D. N. Bernstein. The number of roots of a system of equations. *Funkcional. Anal. i Priložen.*, 9(3):1–4, 1975.

[28] G. M. Besana, S. Di Rocco, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. Cell decomposition of almost smooth real algebraic surfaces. *Numer. Algorithms*, 63(4):645–678, 2013.

[29] L. Bettale, J.-C. Faugère, and L. Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, 2013.

[30] E. Bézout. *Théorie générale des équations algébriques*. Ph.-D. Pierres, 1779.

[31] G. Birkhoff. *Lattice Theory*. American Mathematical Society, 1967.

[32] M. Bläser and G. Jindal. On the Complexity of Symmetric Polynomials. In A. Blum, editor, *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 47:1–47:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[33] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag, Berlin, Heidelberg, 2012.

[34] A. Bompadre, G. Matera, R. Wachenchauzer, and A. Waissbein. Polynomial equation solving by lifting procedures for ramified fibers. *Theoretical computer science*, 315(2-3):335–369, 2004.

[35] D. A. Brake, D. J. Bates, W. Hao, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. Algorithm 976: `{B}ertini_real`: numerical decomposition of real algebraic curves and surfaces. *ACM Trans. Math. Software*, 44(1):Art. 10, 30, 2017.

[36] B. Bruno. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41(3):475 – 511, 2006. Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday).

[37] W. Bruns and U. Vetter. *Determinantal Rings*, volume 1327. Springer, 2006.

[38] J. Canny and I. Emiris. An efficient algorithm for the sparse mixed resultant. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 89–104. Springer, 1993.

[39] J. Canny, E. Kaltofen, and Y. Lakshman. Solving systems of non-linear polynomial equations faster. In *Proceedings of the 1989 International Symposium on Symbolic and Algebraic Computation*, ISSAC'89, pages 121–128. ACM, 1989.

[40] J. F. Canny and I. Z. Emiris. A subdivision-based algorithm for the sparse resultant. *Journal of the ACM (JACM)*, 47(3):417–451, 2000.

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

[42] L. Comtet. Advanced Combinatorics, enlarged ed., D, 1974.

[43] A. Conca and J. Herzog. On the Hilbert function of determinantal rings and their canonical module. *Proceedings of the American Mathematical Society*, 122(3):677–681, 1994.

[44] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 1–6, 1987.

[45] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3rd ed.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[46] D.A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*, volume 185. Springer Science & Business Media, 2006.

[47] Y. Dai, S. Kim, and M. Kojima. Computing all nonsingular solutions of cyclic-n polynomial using polyhedral homotopy continuation methods. *Journal of Computational and Applied Mathematics*, 152(1-2):83–97, 2003.

[48] J. Della Dora, C. Discrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *EUROCAL'85*, volume 204 of *LNCS*, pages 289–290. Springer, 1985.

[49] H. Derksen and G. Kemper. *Computational Invariant Theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopedia of Mathematical Sciences, 130.

[50] J. Ding, R. Perlner, A. Petzoldt, and D. Smith-Tone. Improved cryptanalysis of HFEv-via projection. In *International Conference on Post-Quantum Cryptography*, pages 375–395. Springer, 2018.

[51] A. L. Dixon. The eliminant of three quantics in two independent variables. *Proceedings of the London Mathematical Society*, 2(1):49–69, 1909.

[52] J. Eagon and D. Northcott. Ideals defined by matrices and a certain complex associated with them. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, 269(1337):188–204, 1962.

[53] D. Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, New York, Berlin, Heildelberg, 1995.

[54] I. Z. Emiris and J. F. Canny. A practical method for the sparse resultant. In *Proceedings of the 1993 international symposium on Symbolic and algebraic computation*, pages 183–192, 1993.

[55] I. Z Emiris and J. F Canny. Efficient incremental algorithms for the sparse resultant and the mixed volume. *Journal of Symbolic Computation*, 20(2):117–149, 1995.

[56] I. Z. Emiris and J. Verscheide. How to count efficiently all affine roots of a polynomial system. *Discrete Applied Mathematics*, 93(1):21–32, 1999.

[57] N.-E. Fahssi. Polynomial triangles revisited. https://arxiv.org/abs/1202.0228, 2012.

[58] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.

[59] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.

[60] J.-C. Faugère. FGb: A Library for Computing Gröbner Bases. In Komei Fukuda, Joris Hoeven, Michael Joswig, and Nobuki Takayama, editors, *Mathematical Software - ICMS 2010*, volume 6327 of *Lecture Notes in Computer Science*, pages 84–87, Berlin, Heidelberg, September 2010. Springer Berlin / Heidelberg.

[61] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[62] J.-C. Faugère, M. Hering, and J. Phan. The membrane inclusions curvature equations. *Advances in Applied Mathematics*, 31(4):643 – 658, 2003.

[63] J.-C. Faugère and C. Mou. Fast algorithm for change of ordering of zero-dimensional Gröbner bases with sparse multiplication matrices. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, pages 115–122, 2011.

[64] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, ISSAC '09, pages 151–158, New York, NY, USA, 2009. ACM.

[65] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Critical points and Gröbner bases: The unmixed case. In *Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 162–169, New York, NY, USA, 2012. ACM.

[66] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. On the complexity of the generalized MinRank problem. *Journal of Symbolic Computation*, 55:30 – 58, 2013.

[67] J.-C. Faugère, M. Safey El Din, and T. Verron. On the complexity of computing Gröbner bases for quasi-homogeneous systems. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, pages 189–196, 2013.

[68] J.-C. Faugère, M. Safey El Din, and T. Verron. On the complexity of computing Gröbner bases for weighted homogeneous systems. *Journal of Symbolic Computation*, 76:107–141, 2016.

[69] 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 the 2012 International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 170–178, New York, NY, USA, 2012. ACM.

[70] P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009.

[71] A. S. Fraenkel and Y. Yesha. Complexity of problems in games, graphs and algebraic equations. *Discrete Applied Mathematics*, 1(1-2):15–30, 1979.

[72] W. Fulton. Flags, Schubert polynomials, degeneracy loci, and determinantal formulas. *Duke Mathematical Journal*, 65(3):381–420, 1992.

[73] W. Fulton. *Introduction to Toric Varieties*. Princeton University Press, 1993.

[74] W. Fulton and P. Pragacz. *Schubert varieties and degeneracy loci*. Springer, 2006.

[75] T. Gao and T. Y. Li. Mixed volume computation via linear programming. *Taiwanese Journal of Mathematics*, 4(4):599–619, 2000.

[76] T. Gao and T.-Y. Li. Mixed volume computation for semi-mixed systems. *Discrete & Computational Geometry*, 29(2):257–277, 2003.

[77] T. Gao, T.-Y. Li, and X. Wang. Finding all isolated zeros of polynomial systems in $\mathbb{C}^n$ via stable mixed volumes. *Journal of Symbolic Computation*, 28(1-2):187–211, 1999.

[78] T. Gao, T.-Y. Li, and M. Wu. Algorithm 846: MixedVol: a software package for mixed-volume computation. *ACM Transactions on Mathematical Software (TOMS)*, 31(4):555–560, 2005.

[79] M. R. Garey and D. S. Johnson. *Computers and intractability*, volume 29. WH Freeman New York, 2002.

[80] J. V. Z. Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, New York, NY, USA, 2 edition, 2003.

[81] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for computer algebra*. Springer Science & Business Media, 1992.

[82] I. Gelfand, M. Kapranov, and A. Zelevinsky. *Discriminants, resultants and multidimensional determinants*. Birkhäuser Boston, Inc., Boston, MA, 1994.

[83] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using Gröbner bases. In *AAECC*, volume 356 of *LNCS*, pages 247–257. Springer, 1989.

[84] M. Giusti, J. Heintz, K. Hägele, J. E. Morais, L. M. Pardo, and J. L. Montana. Lower bounds for diophantine approximations. *Journal of Pure and Applied Algebra*, 117:277–317, 1997.

[85] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.

[86] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

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

[88] L. Goubin and N. T. Courtois. Cryptanalysis of the TTM cryptosystem. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 44–57. Springer, 2000.

[89] O. Grellier, P. Comon, B. Mourrain, and P. Trébuchet. Analytical blind channel identification. *IEEE Transactions on Signal Processing*, 50(9):2196–2207, 2002.

[90] A. Greuet and M. Safey El Din. Probabilistic algorithm for polynomial optimization over a real algebraic set. *SIAM Journal on Optimization*, 24(3):1313–1343, 2014.

[91] D. Grigorév and N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *Journal of Symbolic Computation*, 5(1-2):37–64, 1988.

[92] F. Guo, M. Safey El Din, and L. Zhi. Global optimization of polynomials using generalized critical values and sums of squares. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, pages 107–114, New York, NY, USA, 2010. ACM.

[93] J. Harris. *Algebraic geometry: a first course*, volume 133. Springer Science & Business Media, 2013.

[94] R. Hartshorne. *Algebraic Geometry*, volume 52. Springer Science & Business Media, 2013.

[95] J. D. Hauenstein. Numerically computing real points on algebraic sets. *Acta Appl. Math.*, 125:105–119, 2013.

[96] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein. Deformation techniques for efficient polynomial equation solving. *Journal of complexity*, 16(1):70–109, 2000.

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

[98] J. Heintz and M. Sieveking. Absolute primality of polynomials is decidable in random polynomial time in the number of variables. In *International Colloquium on Automata, Languages, and Programming*, pages 16–28. Springer, 1981.

[99] J. Heintz, P. Solernó, and M.-F. Roy. On the complexity of semi-algebraic sets. In *IFIP Congress*, pages 293–298. San Francisco, 1989.

[100] M. I. Herrero, G. Jeronimo, and J. Sabia. Computing isolated roots of sparse polynomial systems in affine space. *Theoretical Computer Science*, 411(44):3894 – 3904, 2010.

[101] M. I. Herrero, G. Jeronimo, and J. Sabia. Affine solution sets of sparse polynomial systems. *Journal of Symbolic Computation*, 51:34 – 54, 2013.

[102] M. I. Herrero, G. Jeronimo, and J. Sabia. Elimination for generic sparse polynomial systems. *Discrete and Computational Geometry*, 51(3):578–599, 2014.

[103] Hoon Hong and Mohab Safey El Din. Variant quantifier elimination. *Journal of Symbolic Computation*, 47(7):883–901, July 2012.

[104] B. Huber and B. Sturmfels. A polyhedral method for solving sparse polynomial systems. *Mathematics of computation*, 64(212):1541–1555, 1995.

[105] B. Huber and B. Sturmfels. Bernstein's theorem in affine space. *Discrete & Computational Geometry*, 17(2):137–141, 1997.

[106] B. Huber and J. Verschelde. Pieri homotopies for problems in enumerative geometry applied to pole placement in linear systems control. *SIAM Journal on Control and Optimization*, 38(4):1265–1287, 2000.

[107] S. G. Hyun, V. Neiger, H. Rahkooy, and É. Schost. Block-Krylov techniques in the context of sparse-FGLM algorithms. *Journal of Symbolic Computation*, 98:163–191, 2020.

[108] D. James. A global weighted version of Bézout's theorem. *The Arnoldfest (Toronto, ON, 1997)*, 24:115–129, 1999.

[109] G. Jeronimo, J. Heintz, J. Sabia, and P. Solernó. Intersection theory and deformation algorithms: the multi-homogeneous case (draft).

[110] G. Jeronimo, G. Matera, P. Solernó, and A. Waissbein. Deformation techniques for sparse systems. *Foundations of Computational Mathematics*, 9(1):1–50, 2009.

[111] G. Jeronimo and D. Perrucci. A probabilistic symbolic algorithm to find the minimum of a polynomial function on a basic closed semialgebraic set. *Discrete & Computational Geometry*, 52(2):260–277, 2014.

[112] K. Kalorkoti. Counting and Gröbner bases. *Journal of Symbolic Computation*, 31(3):307–313, 2001.

[113] E. Kaltofen. Greatest common divisors of polynomials given by straight-line programs. *Journal of the ACM (JACM)*, 35(1):231–264, 1988.

[114] E. Kaltofen. Factorization of polynomials given by straight-line programs. *Advances in Computing Research*, 5:375–412, 1989.

[115] D. Kapur and Y. N. Lakshman. *Elimination methods: An introduction*. State University of New York at Albany, Department of Computer Science, 1991.

[116] D. Kapur and T. Saxena. Comparison of various multivariate resultant formulations. In *Proceedings of the 1995 international symposium on Symbolic and algebraic computation*, pages 187–194, 1995.

[117] A.G. Khovanskii. Newton polytopes and toric varieties. *Functional Anal. Appl*, 11:289–298, 1977.

[118] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Annual International Cryptology Conference*, pages 19–30. Springer, 1999.

[119] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die Reine und Angewandte Mathematik*, 92:1–122, 1882.

[120] W. Krull. Idealtheorie in ringen ohne endlichkeitsbedingung. *Mathematische Annalen*, 101(1):729–744, 1929.

[121] A. G. Kushnirenko. Newton polytopes and the Bézout theorem. *Functional analysis and its applications*, 10(3):233–235, 1976.

[122] F. Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th international symposium on symbolic and algebraic computation*, pages 296–303, 2014.

[123] G. Lecerf. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *ISSAC'00*, pages 209–216. ACM, 2000.

[124] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4):564–596, 2003.

[125] G. Lecerf and É. Schost. Fast multivariate power series multiplication in characteristic zero. *SADIO Electronic Journal on Informatics and Operations Research*, 5(1):1–10, September 2003.

[126] T.-Y. Li. Numerical solution of multivariate polynomial systems by homotopy continuation methods. *Acta numerica*, 6:399–436, 1997.

[127] T.-Y. Li and X. Li. Finding mixed cells in the mixed volume computation. *Foundations of Computational Mathematics*, 1(2):161–181, 2001.

[128] T.-Y. Li and X. Wang. The BKK root count in $\mathbb{C}^n$. *Mathematics of Computation*, pages 1477–1484, 1996.

[129] T.-Y. Li and X. S. Wang. Solving real polynomial systems with real homotopies. *Mathematics of Computation*, 60(202):669–680, 1993.

[130] F. S. Macaulay. Some formulae in elimination. *Proceedings of the London Mathematical Society*, 1(1):3–27, 1902.

[131] F. S. Macaulay. *The Algebraic Theory of Modular Systems*. Cambridge University Press, 1916.

[132] F.S. Macaulay. Algebraic theory of modular systems, volume 19 of. *Cambridge Tracts in Mathematics*, 1916.

[133] I. G. Macdonald. *Symmetric functions and Hall polynomials*. Oxford University Press, 1998.

[134] A. Maciuk, J.-H. Renault, R. Margraff, P. Trébuchet, M. Zèches-Hanrot, and J.-M. Nuzillard. Anion-exchange displacement centrifugal partition chromatography. *Analytical Chemistry*, 76(21):6179–6186, 2004.

[135] H. Matsumura. *Commutative Ring Theory*. Cambridge studies in advanced mathematics. Cambridge University Press, 1986.

[136] E. Miller and B. Sturmfels. *Combinatorial Commutative Algebra*. Springer Verlag, New York, 2005.

[137] D. Moody, R. Perlner, and D. Smith-Tone. An asymptotically optimal structural attack on the ABC multivariate encryption scheme. In *International Workshop on Post-Quantum Cryptography*, pages 180–196. Springer, 2014.

[138] D. Moody, R. Perlner, and D. Smith-Tone. Improved attacks for characteristic-2 parameters of the cubic ABC simple matrix encryption scheme. In *International Workshop on Post-Quantum Cryptography*, pages 255–271. Springer, 2017.

[139] A. Morgan. *Solving polynomial systems using continuation for engineering and scientific problems*, volume 57. SIAM, 2009.

[140] Alexander Morgan. *Solving polynomial systems using continuation for engineering and scientific problems*. SIAM, 2009.

[141] S. Morrison. The differential ideal $[P] : M^{\infty}$. *Journal of Symbolic Computation*, 28(4-5):631–656, 1999.

[142] B. Mourrain. Isolated points, duality and residues. *Journal of Pure and Applied Algebra*, 117/118:469–493, 1997. Algorithms for algebra (Eindhoven, 1996).

[143] J. Nie, J. Demmel, and B. Sturmfels. Minimizing polynomials via sum of squares over the gradient ideal. *Mathematical programming*, 106(3):587–606, 2006.

[144] J. Nie and K. Ranestad. Algebraic degree of polynomial optimization. *SIAM Journal on Optimization*, 20(1):485–502, April 2009.

[145] S. Petitjean. Algebraic geometry and computer vision: Polynomial systems, real and complex roots. *Journal of Mathematical Imaging and Vision*, 10(3):191–220, 1999.

[146] A. Poteaux and É. Schost. On the complexity of computing with zero-dimensional triangular sets. *Journal of Symbolic Computation*, 50:110–138, 2013.

[147] M. Raghavan and B. Roth. Solving polynomial systems for the kinematic analysis and synthesis of mechanisms and robot manipulators. *Journal of Mechanical Design*, 117(B):71–79, 06 1995.

[148] 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.

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

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

[151] J. M. Rojas. A convex geometric approach to counting the roots of a polynomial system. *Theoretical Computer Science*, 133(1):105–140, 1994.

[152] J. M. Rojas. Toric intersection theory for affine root counting. *Journal of Pure and Applied algebra*, 136(1):67–100, 1999.

[153] J. M. Rojas and X. Wang. Counting affine roots of polynomial systems via pointed Newton polytopes. *Journal of Complexity*, 12(2):116–133, 1996.

[154] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[155] F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a re al algebraic set defined by a single equation. *Journal of Complexity*, 16:716–750, 2000.

[156] 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 *ISSAC'03*, pages 224–231. ACM, 2003.

[157] M. Safey El Din and É. Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete and Computational Geometry*, 45(1):181–220, 2011.

[158] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM (JACM)*, 63(6):1–37, 2017.

[159] 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.

[160] M. Safey El Din and P.-J. Spaenlehauer. Critical point computations on smooth varieties: Degree and complexity bounds. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 183–190, New York, NY, USA, 2016. ACM.

[161] B. Saugata, P. Richard, and R. Marie-Francoise. Computing roadmaps of semi-algebraic sets on a variety. *Journal of the American Mathematical Society*, 13(1):55–82, 2000.

[162] É. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):349–393, 2003.

[163] J. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM (JACM)*, 27(4):701–717, 1980.

[164] A. J. Sommese and J. Verschelde. Numerical homotopies to compute generic points on positive dimensional algebraic sets. *Journal of Complexity*, 16(3):572–602, 2000.

[165] A. J. Sommese, J. Verschelde, and C. W. Wampler. Numerical decomposition of the solution sets of polynomial systems into irreducible components. *SIAM Journal on Numerical Analysis*, 38(6):2022–2046, 2001.

[166] F. Sottile, R. Vakil, and J. Verschelde. Solving Schubert problems with Littlewood-Richardson homotopies. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 179–186. ACM, 2010.

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

[168] A. J. Stothers. *On the complexity of matrix multiplication*. PhD thesis, The University of Edinburgh, 2010.

[169] B. Sturmfels. *Sparse elimination theory*, volume 91. Mathematical Sciences Institute, Cornell University, 1991.

[170] B. Sturmfels. *Algorithms in Invariant Theory*. Springer-Verlag, Berlin, Heidelberg, 1993.

[171] A. Takeda, M. Kojima, and K. Fujisawa. Enumeration of all solutions of a combinatorial linear inequality system arising from the polyhedral homotopy continuation method. *Journal of the Operations Research Society of Japan*, 45(1):64–82, 2002.

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

[173] J. Vates and D. Smith-Tone. Key recovery attack for all parameters of HFE. In *International Workshop on Post-Quantum Cryptography*, pages 272–288. Springer, 2017.

[174] J. Verschelde, K. Gatermann, and R. Cools. Mixed-volume computation by dynamic lifting applied to polynomial system solving. *Discrete & Computational Geometry*, 16(1):69–112, 1996.

[175] J. Verschelde, P. Verlinden, and R. Cools. Homotopies exploiting newton polytopes for solving sparse polynomial systems. *SIAM Journal on Numerical Analysis*, 31(3):915–930, 1994.

[176] V. V. Williams. Multiplying matrices faster than Coppersmith-Winograd. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 887–898, 2012.

[177] S.S.-T. Yau and L. Zhang. An upper estimate on integral points in real simplices with an application in singularity theory. *Mathematical Research Letters*, 6:911–921, 2006.

[178] O. Zariski and P. Samuel. *Commutative Algebra*. Van Nostrand, 1958.