Counting Solutions of Algebraic Systems via Triangular Decomposition

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften
der RWTH Aachen University zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Computermathematiker

Thomas Martin Bächler

aus Offenbach am Main

Berichter: Universitätsprofessor Dr. Wilhelm Plesken
Universitätsprofessorin Dr. Eva Zerz

Tag der mündlichen Prüfung: 04.07.2014

Contents

Chapter 1

Introduction

Abstract. The goal of this thesis is to analyze the solution sets of systems of polynomial equations and inequations over algebraically closed fields algorithmically. In order to give a measure for the size of such a set, we define a polynomial called the counting polynomial, which we use as a generalization of the cardinality of a finite set. The computation of the counting polynomial requires a decomposition of the solution set into pairwise disjoint subsets defined by a special kind of triangular polynomial systems called simple systems. These simple systems have interesting properties themselves, which we study as well. Most importantly, due to their triangular structure, they can be solved iteratively, giving a clear description of their solution set. We will use simple systems and counting polynomials to study algebraic varieties and constructible sets. Finally, we will use the counting polynomial to count the number of solutions of certain polynomial systems over finite fields.

Triangular Decomposition. Triangular systems are commonly used to solve systems of equations iteratively. A system of linear equations can easily be transformed into a triangular system using the well-known GAUSSian elimination algorithm. To eliminate a variable from an equation, this algorithm adds a multiple of another equation such that the coefficient of that variable cancels. Applying such a method to a non-linear system leads to two problems. First, if the degree of an equation with respect to a specific variable is larger than one, we cannot use it to cancel this variable from arbitrary equations. Second, the coefficients may again be polynomials and thus cannot be easily cancelled since they are not invertible in the polynomial ring.

In the case of two univariate polynomials, elimination is performed using the EUCLIDean algorithm that computes the greatest common divisor of two polynomials. For the multivariate case, resultants and subresultants can be used to refine the EUCLIDean algorithm in order to get conditions for the degree of the greatest common divisor. Since these conditions are polynomials in the remaining variables, the result depends on the values substituted for these variables. Thus, not every polynomial system can be transformed into a triangular one. In order to describe the solution set of a polynomial system via triangular systems, we need to decompose it into smaller subsets.

In the 1930s, Joseph Miller Thomas described a method for performing a decomposition into simple systems (cf. [Tho37, Tho62]). This method distinguishes the different cases for the outcome of the EUCLIDean algorithm precisely by introducing inequations. This has the side-effect that the original set is decomposed into pairwise disjoint subsets. His method is very elementary and requires no advanced knowledge of the theory of rings and ideals. Thomas' original motivation was the treatment of non-linear differential equations. The differential THOMAS decomposition is based on the algebraic one, as discussed in detail in Markus Lange-Hegermann's thesis (cf. [LH14]).

Other triangular decomposition methods have been proposed, most notably the characteristic set method by Ritt and Wu (cf. [Rit50, Wu00]) and decompositions into regular chains. Regular chains were defined by Michael Kalkbrenner (cf. [Kal93]) and later refined by Daniel Lazard

as normalized triangular sets (cf. [Laz91]). Regular chains have become rather popular since they have favorable properties and the algorithms that compute regular chain decompositions are more efficient than other triangular decomposition algorithms. Such algorithms have been implemented in the RegularChains package, which is distributed with recent versions of MAPLE (cf. [MM99, LMMX05]). A comprehensive overview of methods and theory regarding regular chains can be found in [Hub03a, Hub03b].

Neither characteristic sets nor regular chains are suitable for defining the counting polynomial. They do not allow the same strict treatment of inequations as simple systems, and the decompositions into these sets usually do not yield disjoint solution sets. Therefore, the THOMAS decomposition remains the only known general method for computing the counting polynomial. Algorithms for such a decomposition based on Thomas' original description have been implemented by Dongming Wang (cf. [Wan98, Wan01, LW99, Wan04, Wan03]) and as part of my diploma thesis (cf. [Bäc08]).

In this thesis, I devised and implemented a modernized algorithm to perform an algebraic THOMAS decomposition. This algorithm was partially inspired by the methods used in the regular chain decomposition algorithms. It is more efficient than an implementation based on the method Thomas suggests. I also devised a modified algorithm which is the first to allow computing a THOMAS decomposition in positive characteristic. The implementation is available in the AlgebraicThomas package for MAPLE (cf. [BLH14]). At the same time, Markus Lange-Hegermann devised an algorithm for performing a differential THOMAS decomposition and implemented it in the DifferentialThomas package. The differential algorithm builds upon the algebraic one and thus Markus Lange-Hegermann also had a strong influence on the development of the latter. Both these algorithms have been published in [BGLHR12], which was joint work with Vladimir Gerdt, Daniel Robertz and Markus Lange-Hegermann. Relevant parts of this publication are repeated in section 3.2.

Counting Polynomial. The counting polynomial has been defined by Wilhelm Plesken in an attempt to represent some of the information contained in a THOMAS decomposition concisely (cf. [Ple09a]). If a set is finite, its counting polynomial equals its cardinality. For an infinite set, the counting polynomial encodes some information about the fibration structure of the set as imposed by the choice and the order of the indeterminates. It helps deciding equality of sets and contains information about the structure of the solution set, such as its dimension. In some cases, it can be used to count the number of solutions of a polynomial system over a finite field, which Plesken demonstrated in [Ple09b].

Overview. This thesis is organized as follows. In chapter 2, we approach the counting polynomial axiomatically. We give conditions for a class of sets on which the counting polynomial is well-defined and unique. We then define the counting polynomial and prove its most important properties. As a first example of a class of sets that admits a counting polynomial, we consider solution sets of linear systems, i.e. finite unions of intersections of hyperplanes and complements of hyperplanes. This class allows us to give the first simple examples. To conclude this chapter, we define the counting tree, which is a refined version of the counting polynomial that encodes more information about the structure of a set.

Chapter 3 deals with polynomial systems and the THOMAS decomposition. In section 3.1, we first define simple systems and show how they can be used to compute the counting polynomial. We start section 3.2 by summarizing Thomas' original method of performing a decomposition into simple systems and pointing out its weaknesses. To improve on this method, we give a reduction method that helps avoiding unnecessary computations. We introduce subresultants and use them in several algorithms that split polynomial systems into subsystems. We then combine these methods into the main algorithm and prove its correctness and termination.

Section 3.3 deals with special problems that only arise in positive characteristic. In particular, we consider the problem of making a polynomial square-free. We need to extend our base ring by adding roots of indeterminates, since the polynomial ring is not sufficient for this purpose.

The result is the first algorithm capable of computing a Thomas decomposition of an arbitrary polynomial system over a field of positive characteristic, although its implementation is currently restricted to finite fields. We continue with a brief discussion regarding the computation of intersections, complements and unions of solution sets of polynomial systems in section 3.4. The following section 3.5 deals with the comprehensive Thomas decomposition. This decomposition allows treating systems that depend on parameters. It also provides the means to compute the counting tree of a polynomial system. We conclude the chapter with a short discussion of the computation of projections in section 3.6 and a demonstration of the implementation provided by the AlgebraicThomas package in section 3.7.

In chapter 4, we analyze the behaviour of counting polynomials and counting trees under transformations of the underlying polynomial systems. This chapter also contains an analysis of the counting polynomial of the set of $k \times n$-matrices of rank k.

Chapter 5 gives a connection between simple system and embeddings of affine or projective varieties into affine or projective space, respectively. For this purpose, an ideal is assigned to a simple system that describes the Zariski closure of its solution set. We then demonstrate how to compute a Thomas decomposition and the counting polynomial of an embedding of a toric variety without the use of our decomposition algorithm.

In section 5.6, we make a connection between constructible sets and polynomial systems. In particular, we give a method of writing these sets as finite unions of quasi-affine sets, which can themselves be expressed in terms of pairs of ideals.

We conclude this chapter with section 5.7, where we apply the Thomas decomposition to rational maps. We demonstrate how to test whether a given rational map is well-defined and compute its image, as well as test injectivity and surjectivity and give interesting examples.

The final chapter 6 deals with faithful counting polynomials. If a faithful counting polynomial exists, it can be used to determine the number of solutions of a polynomial system over a finite field by merely substituting the cardinality of that field into the polynomial. Again, we give interesting examples to demonstrate the computation of a faithful counting polynomial.

Acknowledgements. I would like to thank everyone who accompanied or influenced me in my life.

First of all, special thanks go to Prof. Wilhelm Plesken for his supervision and ongoing support. I thank my friend and colleague Markus Lange-Hegermann for the countless fruitful discussions, the productive work on our joint projects and for putting up with me even on my bad days. I thank Daniel Robertz and Mohamed Barakat for all the help they have given me over the past decade. I thank my dear colleagues and former colleagues at Lehrstuhl B für Mathematik, particularly Jan Jongen, Sebastian Gutsche, Sebastian Posur, Martin Leuner, Björn Niehenke and Matthias Wisotzky for being open and helpful even when they had other things to do. I thank Wolfgang Krass for always taking a few minutes to brighten everyone's day.

Last but not least, I thank my wife Annette for being there for me unconditionally and believing in me even in times when I doubted myself and my son Robin for always giving me a reason to smile, even on the worst days. I love you both.

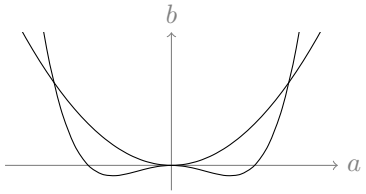
Chapter 2

The Counting Polynomial

In this chapter, we introduce the concepts of enumerable sets, counting polynomials and counting trees and show their most important properties. We define well-behaved classes of enumerable sets that allow defining the counting polynomial. As a first simple example of a well-behaved class of enumerable sets, we consider unions and intersections of hyperplanes and their complements. Starting in the next chapter, we will treat the solution sets of polynomial systems over an algebraically closed field and provide tools to compute the counting polynomial and counting tree.

We provide a first simple example that shows the idea of the counting polynomial.

Example 2.1. Consider the subset of $\mathbb{R}^2 = \{(a, b) | a, b \in \mathbb{R}\}$ given in the following picture:



Consider the projection onto the first component. The image of this projection is $\mathbb{R}$, thus we say that the number of points of the image of the projection is ∞.

We see that there are two different types of fibers - three fibers have only one element, and all other fibers have two elements. Thus, we count the number of points in the whole set as $(\infty - 3) \cdot 2 + 3 \cdot 1$, which we call the **counting polynomial** of the set. ◁

Notation 2.2. Let K be an infinite set, let K^n be its n-th cartesian power and define the projection $\alpha_i : K^n \to K : (a_1, \ldots, a_n) \mapsto a_i$. Furthermore, define $\alpha = (\alpha_1, \ldots, \alpha_n)$ and

$$\pi_n := \pi_n^\alpha := (\alpha_1, \ldots, \alpha_{n-1}) : K^n \to K^{n-1} : (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_{n-1}) \ .$$

We omit the superscript α if it is clear from the context. ◁

2.1 Enumerable Sets

The concept of enumerable sets is designed to allow counting in the following sense. We consider a subset of K enumerable if it is either finite or cofinite so that we can consider the cardinality of either the set itself or of its complement. Enumerability of a subset of K^n is determined by considering the image and all the fibers of π_n, where the latter may again be considered subsets of K.

Definition 2.3. We call $V \subseteq K^n$ (K, n)**-enumerable** if either

1. $n = 1$ and $|V| < \infty$ or $|K \setminus V| < \infty$

or

2. $n > 1$ and
   (a) $\pi_n(V)$ is $(K, n-1)$-enumerable.
   (b) there is $k \geq 0$ such that $V = \biguplus_{i=1}^{k} V_i$ and for each $1 \leq i \leq k$, $\pi_n(V_i)$ is $(K, n-1)$-enumerable and for all $v_1, v_2 \in \pi_n(V_i)$ either
   $$\left|(\pi_n)^{-1}_{|V_i}(\{v_1\})\right| = \left|(\pi_n)^{-1}_{|V_i}(\{v_2\})\right| < \infty$$
   or
   $$\left|K \setminus \alpha_n\left((\pi_n)^{-1}_{|V_i}(\{v_1\})\right)\right| = \left|K \setminus \alpha_n\left((\pi_n)^{-1}_{|V_i}(\{v_2\})\right)\right| < \infty$$
   holds, in particular, $\alpha_n\left((\pi_n)^{-1}_{|V_i}(\{v\})\right)$ is $(K,1)$-enumerable for all $v \in \pi_n(V_i)$.

We call V **elementary** (K,n)**-enumerable** if either $n = 1$ and V is $(K,1)$-enumerable or if $\pi_n(V)$ is elementary $(K, n-1)$-enumerable and one can choose $k = 1$ in 2b. ◁

Clearly, the empty set and K^n are elementary (K,n)-enumerable. Also note that the sets V_i given in 2b are again (K,n)-enumerable.

We show some basic examples that can easily be verified using only the above definition.

Example 2.4.
1. If $V_1, \ldots, V_n \subseteq K^1$ are $(K,1)$-enumerable, then $V_1 \times \cdots \times V_n$ is elementary (K,n)-enumerable.
2. Let $V \subseteq K^{n-1}$ be elementary $(K, n-1)$-enumerable and $X_1, X_2 \subseteq K^1$ be $(K,1)$-enumerable with either $|X_1| = |X_2| < \infty$ or $|K \setminus X_1| = |K \setminus X_2| < \infty$. If $V = W_1 \uplus W_2$ with (not necessarily enumerable) sets W_1, W_2, then $(W_1 \times X_1) \uplus (W_2 \times X_2)$ is elementary (K,n)-enumerable. In general, this is not the case for $(X_1 \times W_1) \uplus (X_2 \times W_2)$. ◁

In the following, we denote the set of (K,n)-enumerable sets by $\mathcal{C}^n = \mathcal{C}^n_K$.

Lemma 2.5. *If V is (K,n)-enumerable, then V is the union of finitely many pairwise disjoint elementary (K,n)-enumerable sets.*

Proof. Let V be (K,n)-enumerable. If $n = 1$ then it is elementary $(K,1)$-enumerable by definition. Consider $n > 1$ and assume that the statement holds for all subsets of K^i with $i < n$. Let $V = \biguplus_{i=1}^{k} V_i$ be the decomposition from (2.3)2b), in particular, all $\pi_n(V_i)$ are $(K, n-1)$-enumerable. By induction, each $\pi_n(V_i)$ is the disjoint union of finitely many elementary $(K, n-1)$-enumerable sets, i.e. $\pi_n(V_i) = \biguplus_{j=1}^{l_i} W_{i,j}$. Set $X_{i,j} := V_i \cap (W_{i,j} \times K)$ for all $i = 1, \ldots, k$ and $j = 1, \ldots, l_i$. By definition,
$$V = \biguplus_{i=1}^{k} V_i = \biguplus_{i=1}^{k} \biguplus_{j=1}^{l_i} X_{i,j}$$
holds. For each $X_{i,j}$, $\pi_n(X_{i,j}) = W_{i,j}$ is elementary $(K, n-1)$-enumerable and due to $W_{i,j} \subseteq \pi_n(V_i)$ and due to the choice of the V_i, property (2.3)2b)holds with only one set in the decomposition. Therefore, all $X_{i,j}$ are elementary (K,n)-enumerable. □

A first and simple example of enumerable sets are finite sets.

Proposition 2.6. *Every finite set $V \subseteq K^n$ is (K,n)-enumerable.*

Proof. Any finite set $V \subseteq K$ is $(K,1)$-enumerable by definition. For $n > 1$, let $V = \{v_1, \ldots, v_{|V|}\}$ and define $V_i := \{v_i\}$, $i = 1, \ldots, |V|$. Since $\pi_n(V)$ is a finite subset of K^{n-1}, it is $(K, n-1)$-enumerable by induction. For each $v \in \pi_n(V)$, $\alpha_n\left((\pi_n)^{-1}_{|V}(\{v\})\right) \subseteq K$ is finite and thus $(K,1)$-enumerable. Finally, $V = \biguplus_{i=1}^{|V|} V_i$, each $\pi_n(V_i)$ is finite and thus $(K, n-1)$-enumerable, and since $|\pi_n(V_i)| = 1$, property (2.3)2b)holds trivially. □

In general, (K,n)-enumerability depends on the order of the α_i, as the following example shows.

Remark 2.7. Consider the set

$$V := \left\{(x,1) \in \mathbb{C}^2 \middle| x \in \mathbb{N}\right\} \cup \left\{(x,-1) \in \mathbb{C}^2 \middle| x \notin \mathbb{N}\right\} \subseteq \mathbb{C}^2$$

Clearly, $\pi_2(V) = \mathbb{C}$ is $(\mathbb{C},1)$-enumerable. For all $x \in \mathbb{C}$,

$$\alpha_2\left(\left(\pi_2\right)_{|V}^{-1}\left(\{x\}\right)\right) \in \{\{1\},\{-1\}\}$$

is finite and thus $(\mathbb{C},2)$-enumerable. Furthermore, for all $x \in \mathbb{C}$, $\left|\alpha_2\left(\left(\pi_2\right)_{|V}^{-1}\left(\{x\}\right)\right)\right| = 1$, i.e. the cardinality is independent of x.

Now apply the bijection $T : K^2 \to K^2 : (x,y) \mapsto (y,x)$ and define $W := T(V)$. This leads to $\pi_2(W) = \{-1,1\}$ and we have $a_2\left(\left(\pi_2\right)_{|W}^{-1}\left(\{1\}\right)\right) = \mathbb{N}$ and $a_2\left(\left(\pi_2\right)_{|W}^{-1}\left(\{-1\}\right)\right) = \mathbb{C} \setminus \mathbb{N}$. Neither of these sets is $(\mathbb{C},1)$-enumerable and thus W is not $(\mathbb{C},2)$-enumerable. ◁

2.2 The Counting Polynomial

We now define the central object of this chapter, the counting polynomial, which has first been introduced in [Ple09a]. Its basic idea is best explained by considering enumerable subsets of K. Since a $(K,1)$-enumerable set of V is either finite or cofinite, it either has $|V|$ elements or its complement has $|K \setminus V|$ elements, respectively. In the latter case, we say that V has $\infty - |K \setminus V|$ elements.

Definition 2.8. Define the map

$$c_1 : \mathcal{C}_K^1 \to \mathbb{Z}[u] : V \mapsto \begin{cases} |V| & |V| < \infty \\ u - |K \setminus V| & \text{otherwise} \end{cases}.$$

We call $c_1(V)$ the **counting polynomial** of $V \in \mathcal{C}_K^1$. ◁

To extend this notion to subsets of K^n for $n > 1$, we need to restrict ourselves to classes of enumerable sets that have more properties.

Notation 2.9. Let $0 \leq l \leq n$ and define the map $\pi_{n,l} : K^n \to K^l$ recursively by $\pi_{n,l}(a) = \pi_{l+1}\left(\pi_{n,l+1}(v)\right)$ for all $v \in K^n$ and $\pi_{n,n} = \mathrm{Id}_{K^n}$, i.e. $\pi_{n,l}\left((a_1,\ldots,a_n)\right) = (a_1,\ldots,a_l)$.

In particular, note that $\pi_{n,n-1} = \pi_n$. ◁

Definition 2.10. Let $\mathcal{X} = (\mathcal{X}^n)_{n=0}^{\infty}$ with $\mathcal{X}^n \subseteq \mathcal{C}_K^n$ such that for every $n > 0$ and $V, W \in \mathcal{X}^n$, the following holds:

1. If $V = \biguplus_{i=1}^k V_i$ as in (2.3)2b), then V_i can be chosen such that $V_i \in \mathcal{X}^n$.
2. $\pi_n(V) \in \mathcal{X}^{n-1}$.
3. $K^n \setminus V \in \mathcal{X}^n$.
4. $V \cup W \in \mathcal{X}^n$.
5. If $U \in \mathcal{X}^{n-1}$ with $U \subseteq \pi_n(V)$, then $U \times K \in \mathcal{X}^n$ (fiber axiom).
6. If $m < n$ and $(a_1,\ldots,a_m) \in \pi_{n,m}(V)$, then

$$\{(a_{m+1},\ldots,a_n) | (a_1,\ldots,a_m,a_{m+1},\ldots,a_n) \in V\} \in \mathcal{X}^{n-m}$$

(evaluation axiom).

Then we call $\mathcal{X}$ a **strongly well-behaved class of enumerable sets** over K.

Replace 6. by the following condition.

6'. There is a strongly well-behaved class of enumerable sets $\mathcal{Y}$ with $\mathcal{X}^i \subseteq \mathcal{Y}^i$, $i \geq 0$ such that if $m < n$ and $(a_1, \ldots, a_m) \in \pi_{n,m}(V)$, then $\{(a_{m+1}, \ldots, a_n) | (a_1, \ldots, a_m, a_{m+1}, \ldots, a_n) \in V\} \in \mathcal{Y}^{n-m}$ (weak evaluation axiom).

Then we call $\mathcal{X}$ a **well-behaved class of enumerable sets** over K. ◁

As a result of 1. and 2., we get that the decomposition produced in Lemma (2.5) can be chosen such that all elementary enumerable sets are in $\mathcal{X}^n$. Conditions 3. and 4. combined imply that for each $V, W \in \mathcal{X}^n$, $V \cap W \in \mathcal{X}^n$. Furthermore, if $W \subseteq V$, then $V \setminus W \in \mathcal{X}^n$.

Conditions 5 and 6' make sure our class is large enough for later purposes.

Corollary 2.11. *Let $\mathcal{X}$ be a well-behaved class of enumerable sets. Then for $X \subseteq K^n$ it holds that $X \in \mathcal{X}^n$ if and only X is the disjoint union of finitely many elementary (K, n)-enumerable sets in $\mathcal{X}$.*

Proof. If $X \in \mathcal{X}$, then according to Lemma (2.5), $X = \biguplus_{i=1}^{k} X_i$ where X_i is elementary (K, n)-enumerable. According to Definition (2.10)1. and the proof of Lemma (2.5), we can choose $X_i \in \mathcal{X}$.

Conversely, if $X = \biguplus_{i=1}^{k} X_i$ with $X_i \in \mathcal{X}$, then $X \in \mathcal{X}$ according to Definition (2.10)4. □

From now on, let $\mathcal{X}$ be a well-behaved class of enumerable sets over K.

Definition 2.12 (Counting Polynomial)**.** Let $n > 1$ and consider a map $c_n : \mathcal{X}^n \to \mathbb{Z}[u]$ with the following properties:

1. If $V, W \in \mathcal{X}^n$ are disjoint, then $c_n(V \uplus W) = c_n(V) + c_n(W)$
2. Let $V \in \mathcal{X}^n$, $U \in \mathcal{X}^{n-1}$ such that $\pi_n(V) = U$ and
$$c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V}(\{v_1\})\right)\right) = c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V}(\{v_2\})\right)\right)$$
for all $v_1, v_2 \in U$. Then
$$c_n(V) = c_{n-1}(U) \cdot c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V}(\{v\})\right)\right)$$
for any $v \in U$.

We call $c_n(V)$ the **counting polynomial** of $V \in \mathcal{X}^n$. If n is clear from the context, we also write c instead of c_n. If the projections α are not clear from the context, we write c^α or c^α_n. ◁

Remark 2.13. Definition (2.8) defines a map $c_1 : \mathcal{C}^1 \to \mathbb{Z}[u]$. Let $V = V_1 \uplus V_2 \in \mathcal{C}^1$. If V_1 and V_2 are finite, then $c(V) = |V| = |V_1| + |V_2| = c(V_1) + c(V_2)$. If either of them is infinite, without loss of generality V_1, then $c(V) = u - |K \setminus V| = u - |K \setminus (V_1 \uplus V_2)| = u - |(K \setminus V_1) \setminus V_2| = u - (|K \setminus V_1| - |V_2|) = c(V_1) + c(V_2)$. Therefore, c_1 fulfills condition (2.12)1.

The same holds for its restriction $(c_1)_{|\mathcal{X}^1} : \mathcal{X}^1 \to \mathbb{Z}[u]$. ◁

The variable u is a placeholder for the cardinality of the set K, thus we sometimes write ∞ instead of u. We consider some basic properties of the counting polynomial:

Lemma 2.14. *Assume that for $n \geq 0$, the map c_n exists. Then the following holds.*

1. $c_n(K^n) = u^n$.
2. *If $V, W, \in \mathcal{X}^n$, then $c(V \cup W) + c(V \cap W) = c(V) + c(W)$.*
3. *If $|V| < \infty$ then $c(V) = |V|$.*

4. If $V, W \in \mathcal{X}^n$ with $W \subseteq V$, then $c(V \setminus W) = c(V) - c(W)$.

Proof. 1. If $n = 1$, then $c_1(K^1) = c_1(K) = u$ due to Definition (2.8). If $n > 1$, it holds that $K^n = K^{n-1} \times K$. Due to Definition (2.12)2., $c_n(K^n) = c_{n-1}(\pi_n(K^n)) \cdot c_1(K) = c_{n-1}(K^{n-1}) \cdot u$.

2. From Definition (2.12)1) we get

$$\begin{aligned} c(V) + c(W) &= c((V \setminus (V \cap W)) \uplus (V \cap W)) + c(W) \\ &= c(V \setminus (V \cap W)) + c(V \cap W) + c(W) \\ &= c(V \setminus (V \cap W) \uplus W) + c(V \cap W) \\ &= c(V \cup W) + c(V \cap W) \ . \end{aligned}$$

3. Let $n = 1$, then $c_1(\{v\}) = 1$ due to Definition (2.8). For $n > 1$, $c_n(\{v\}) = c_{n-1}(\pi_n(\{v\})) \cdot 1$ and thus $c_n(\{v\}) = 1$.

   Let $V = \{v_1, \ldots, v_{|V|}\}$. Then $V = \biguplus_{i=1}^{|V|} \{v_i\}$ and thus $c(V) = \sum_{i=1}^{|V|} c(\{v_i\}) = |V|$.

4. $c(V) = c((V \setminus W) \uplus W) = c(V \setminus W) + c(W)$. □

To prove that the counting polynomial is well-defined, we first need to prove that we can make every family of sets in $\mathcal{X}^n$ disjoint.

Lemma 2.15. *Let $U_i \in \mathcal{X}^n$, $i = 1, \ldots, k$. Then there are $W_i \in \mathcal{X}^n$, $i = 1, \ldots, l$ such that*

1. $\bigcup_{i=1}^{k} U_i = \biguplus_{i=1}^{l} W_i$.
2. *For every $1 \leq i \leq k$ and $1 \leq j \leq l$ either $W_j \subseteq U_i$ or $W_j \cap U_i = \emptyset$.*

Proof. For $m \in \mathbb{N}$, define an m-defect of $(U_i)_{i=1,\ldots,k}$ as a subset $I \subseteq \underline{k}$ with $|I| = m$ such that $\bigcap_{i \in I} U_i \neq \emptyset$. A defect I is maximal if there is no defect I' with $I \subsetneq I'$. Consider the largest m such that there is an m-defect I. If $m = 1$ then the sets U_i are already pairwise disjoint.

Otherwise, without loss of generality, assume that $k-1, k \in I$ and define $X_i := U_i$, $i = 1, \ldots, k-2$, $X_{k-1} := U_{k-1} \setminus U_k$, $X_k := U_k \setminus U_{k-1}$ and $X_{k+1} := V_{k-1} \cap V_k$. Then $\bigcup_{i=1}^{k} V_i = \bigcup_{i=1}^{k+1} X_k = \bigcup_{i=1}^{k-2} X_k \cup (X_{k-1} \uplus X_k \uplus X_{k+1})$.

We construct *all* defects of $(X_i)_i$ by analyzing the defects of $(V_i)_i$. Thus, let $m' \in \mathbb{N}$ and let I be any m'-defect of $(V_i)_i$. We distinguish the following cases:

1. $k-1, k \notin I$: Then I is an m'-defect of $(X_i)_i$.
2. I is maximal with $k-1 \in I$ and $k \notin I$: Then there is no defect I' of $(V_i)_i$ with $I \cup \{k\} \subseteq I'$ and thus I is an m'-defect of $(X_i)_i$.
3. I is not maximal with $k-1 \in I$ and $k \notin I$: Since I is not maximal, $m' < m$. At least one of I and $(I \setminus \{k-1\}) \cup \{k+1\}$ is an m'-defect of $(X_i)_i$. This potentially increases the number of m'-defects of $(X_i)_i$ compared to the number of m'-defects of $(V_i)_i$.
4. I is maximal with $k \in I$ and $k-1 \notin I$: Analogous to case 2.
5. I is not maximal with $k \in I$ and $k-1 \notin I$: Analogous to case 3.
6. Both $k-1 \in I$ and $k \in I$: Then I yields up to three $m'-1$-defects of the form $I \setminus \{k-1\}$, $I \setminus \{k\}$, or $(I \setminus \{k-1, k\}) \cup \{k+1\}$ of $(X_i)_i$. This increases the number of $m'-1$-defects of $(X_i)_i$ compared to the number of $m'-1$-defects of $(V_i)_i$, but strictly decreases the number of m'-defects.

In particular, the number of m-defects of $(X_i)_i$ is smaller than the number of m-defects of $(V_i)_i$, and $(X_i)_i$ has no m'-defects for $m' > m$. Iterating this process thus yields, after finitely many steps, a family $(W_i)_{i=1}^{l}$ without m-defects for any $m > 1$. By construction, $W_i \in \mathcal{X}^n$ for all i. The construction also ensures the second property. □

The previous lemma only requires that $\mathcal{X}^n$ is closed under intersections, unions and complements and does not use the remaining axioms of Definition (2.10).

Theorem 2.16. *For $n \geq 0$, Definition (2.8) and Definition (2.12) define a unique map $c_n : \mathcal{X}^n \to \mathbb{Z}[u]$.*

Proof. For $n = 1$, this is obvious from Definition (2.8) and Remark (2.13). We use induction over n, thus assume that $n > 1$ and that Definition (2.8) and Definition (2.12) define a unique map $c_{n-1} : \mathcal{X}^{n-1} \to \mathbb{Z}[u]$. First assume that the map c_n exists and show that it is unique.

Let V such that for all $v, w \in \pi_n(V)$, $c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V}(\{v\})\right)\right) = c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V}(\{w\})\right)\right)$ $(\star)$. Then, Definition (2.12)2. states

$$c_n(V) = c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V}(\{v\})\right)\right) \cdot c_{n-1}\left(\pi_n(V)\right) \tag{2.1}$$

for an arbitrary $v \in \pi_n(V)$.

If V is not of this form, then for any decomposition $V = \biguplus_{i=1}^k V_i$ into sets $V_i \in \mathcal{X}^n$ that fulfill property $(\star)$, then according to (2.12)1.,

$$c_n(V) = \sum_{i=1}^k c_n(V_i) \ . \tag{2.2}$$

If we assume that choosing a different decomposition yields the same result, this implies that c_n is unique.

Now show that the map c_n exists. Since $\mathcal{X}^n \subseteq \mathcal{C}^n_K$, condition (2.3)2b)implies that a decomposition $V = \biguplus_{i=1}^k V_i$ into sets V_i with property $(\star)$ exists. Thus, the map defined by (2.1) and (2.2) exists if we again assume that choosing a different decomposition yields the same result.

It remains to prove that the result of (2.2) does not depend on the decomposition $V = \biguplus_{i=1}^k V_i$.

First, let $W_i, i = 1, \ldots, l$ be a family such that $\biguplus_{i=1}^l W_i = \bigcup_{i=1}^k \pi_n(V_i)$ as given in Lemma (2.15). Furthermore, let $v_i \in V_i$ and $Y_i := \left(\alpha_n\left((\pi_n)^{-1}_{|V_i}(\{v_i\})\right)\right)$, then $c_n(V_i) = c_{n-1}(\pi_n(V_i)) \cdot c_1(Y_i)$.

$$\begin{aligned}
\sum_{i=1}^k c_n(V_i) &= \sum_{i=1}^k c_{n-1}(\pi_n(V_i)) \cdot c_1(Y_i) \\
&= \sum_{i=1}^k c_{n-1}\left(\biguplus_{j=1}^l W_j \cap \pi_n(V_i)\right) \cdot c_1(Y_i) \\
&= \sum_{i=1}^k \sum_{j=1}^l c_{n-1}\left(W_j \cap \pi_n(V_i)\right) \cdot c_1(Y_i) \\
&= \sum_{j=1}^l c_{n-1}\left(W_j\right) \cdot \sum_{\substack{i=1,\ldots,k \\ W_j \subseteq \pi_n(V_i)}} c_1(Y_i)
\end{aligned}$$

This means that with $X_j := (W_j \times K) \cap V \in \mathcal{X}^n$, $(X_j)_{j=1}^l$ is another decomposition into sets with property $(\star)$ that produces the same counting polynomial. In particular, for all $v \in W_j$

$$(\pi_n)^{-1}_{|X_j}(\{v\}) = \biguplus_{i=1}^k (\pi_n)^{-1}_{|V_i}(\{v\}) = (\pi_n)^{-1}_{|V}(\{v\}) \ . \tag{2.3}$$

We can therefore without loss of generality assume a decomposition X_j such that the sets $\pi_n(X_j)$ are disjoint and property (2.3) holds.

Let $V \in \mathcal{X}^n$ and let $V = \biguplus_{i=1}^{k_1} V_i = \biguplus_{i=1}^{k_2} W_i$ be two such decompositions with $V_i, W_i \in \mathcal{X}^n$. If $X_{i,j} = V_i \cap W_j$, then $V_i = \biguplus_{j=1}^{k_2} X_{i,j}$ and $W_j = \biguplus_{i=1}^{k_1} X_{i,j}$. By (2.12)1. it most hold that

$$\sum_{i=1}^{k} c_n(V_i) = \sum_{i=1}^{k}\sum_{j=1}^{l} c_n(X_{i,j}) = \sum_{j=1}^{l}\sum_{i=1}^{k} c_n(X_{i,j}) = \sum_{j=1}^{l} c_n(W_j) \ .$$

Property (2.3) implies that for each $v \in \pi_n(V_i \cap W_j)$,

$$(\pi_n)^{-1}_{|V_i}(\{v\}) = (\pi_n)^{-1}_{|W_j}(\{v\}) = (\pi_n)^{-1}_{|V_i \cap W_j}(\{v\}) \ .$$

Thus, there is a set $Y_{i,j} \in \mathcal{X}^1$ such that $c_n(V_i \cap W_j) = c_{n-1}(\pi_n(V_i \cap W_j)) \cdot c_1(Y_{i,j})$. This proves that c_n is independent of the decomposition. □

We now prove further important properties of the counting polynomial.

Lemma 2.17. *Let $U, V \in \mathcal{X}^n$.*

1. *If $c(V) \neq 0$, then the leading coefficient of $c(V)$ is positive.*
2. *$c(V) = 0$ if and only if $V = \emptyset$.*
3. *If $U \subseteq V$ and $c(U) = c(V)$ then $U = V$.*
4. *If $c(V) \in \mathbb{Z}$, then $|V| < \infty$.*

Proof. 1.,2. $V = \emptyset$ implies $c(V) = 0$ due to Lemma (2.14)3. We prove part 1. and $c(V) = 0 \implies V = \emptyset$ simultaneously via induction over n.

If $V \in \mathcal{C}^1_K$ is infinite, then $K^1 \setminus V$ is finite and $u = c_1(K) = c_1(V) + c_1\left(K^1 \setminus V\right) = c_1(V) + \left|K^1 \setminus V\right|$ and thus $c_1(V) = u - \left|K^1 \setminus V\right| \neq 0$, with leading coefficient 1. If V is finite, then (2.14)3. implies $c_1(V) = |V| \geq 0$. If $c_1(V) = 0$, then $|V| = 0$ and thus $V = \emptyset$.

For the induction step, consider $V \in \mathcal{X}^{n+1}$. If $c_n(\pi_{n+1}(V)) = 0$, then by induction $\pi_{n+1}(V)$ is empty, and thus V is. Otherwise, choose a decomposition $V = \biguplus_{i=1}^{k} V_i$ that fulfills the properties of (2.3)2b)such that $c_{n+1}(V) = \sum_{i=1}^{k} c_{n+1}(V_i)$ and such that for each i, $c_{n+1}(V_i) = c_1(W_i)\, c_n(\pi_{n+1}(V_i))$ holds for some $W_i \in \mathcal{X}^1$. We can assume that $c_n(\pi_{n+1}(V_i)) \neq 0$ with a positive leading coefficient for each i. As $c_1(W_i)$ has a positive leading coefficient if it is non-zero, we conclude that in this case, $c_{n+1}(V_i)$ has a positive leading coefficient for all i, and thus the same holds for $c_{n+1}(V)$. This proves the first statement. We also conclude that $c_{n+1}(V) = 0$ if and only if $c_1(W_i) = 0$ for all i. This implies $W_i = \emptyset$ for all i and thus $V = \emptyset$.

3. Since $V \setminus U \in \mathcal{X}^n$, $c_n(V) = c_n(V \setminus U) + c_n(U)$ and therefore $c_n(V \setminus U) = 0$. This implies $V \setminus U = \emptyset$.

4. Assume that V is infinite and choose $W \subseteq V$ with $|W| = c(V)$. Then $c(W) = c(V)$ and by 3., $W = V$. This contradicts the assumption that V is an infinite set. □

We now need a method to determine whether a given class of sets is a well-behaved class of enumerable sets. We will do this by showing that each set in a class can be decomposed into elementary enumerable sets.

Proposition 2.18. *Let $\mathcal{X} = (\mathcal{X}^n)_{n=0}^{\infty}$ with $\mathcal{X}^n \subseteq \mathrm{Pot}(K^n)$ such that*

1. *for every $n > 0$ and $V, W \in \mathcal{X}^n$, properties (2.10)2.-5 and 6' hold.*
2. *for each $X \in \mathcal{X}^n$, there are $X_i \in \mathcal{X}^n$ which are elementary (K, n)-enumerable with $X = \biguplus_{i=1}^{k} X_i$.*

Then $\mathcal{X}$ is a well-behaved class of enumerable sets.

Proof. We show by induction that $\mathcal{X}^n \subseteq \mathcal{C}^n$. For each n, it must hold that the disjoint union of finitely many elementary (K,n)-enumerable sets in $\mathcal{X}^n$ is (K,n)-enumerable. Instead, we show the slightly stronger statement that the disjoint union of any two (K,n)-enumerable sets in $\mathcal{X}^n$ is (K,n)-enumerable.

For $n = 1$, let $V, W \in \mathcal{X}^1$. If both V and W are finite, then $V \uplus W$ is finite and thus $(K,1)$-enumerable. Otherwise, without loss of generality, V is infinite with a finite complement. Since they are disjoint, W is finite and $V \uplus W$ is again infinite with a finite complement.

Now assume that for $n' < n$, it holds that $\mathcal{X}^{n'} \subseteq \mathcal{C}^{n'}$ and let $V, W \in \mathcal{X}^n \cap \mathcal{C}^n$ be disjoint. Then $\pi_n(V \cup W) = \pi_n(V) \cup \pi_n(W) \in \mathcal{X}^{n-1} \subseteq \mathcal{C}^{n-1}$ is $(K, n-1)$-enumerable by induction.

Due to 2, there are decompositions $V = \biguplus_{i=1}^{k_1} V_i$ and $W = \biguplus_{i=1}^{k_2} W_i$ where $V_i, W_i \in \mathcal{X}^n \cap \mathcal{C}^n$ are elementary (K,n)-enumerable. Define $X_i^V = \pi_n(V_i) \setminus (\pi_n(V_i) \cap \pi_n(W))$, $X_i^W = \pi_n(W_i) \setminus (\pi_n(W_i) \cap \pi_n(V))$ and $X_{i,j}^{V,W} = \pi_n(V_i) \cap \pi_n(W_j)$. Further define $Y_i^V = V_i \cap \left(X_i^V \times K\right)$, $Y_i^W = W_i \cap \left(X_i^W \times K\right)$ and $Y_{i,j}^{V,W} = \left(V_i \cap (X_{i,j}^{V,W} \times K)\right) \cup \left(W_j \cap (X_{i,j}^{V,W} \times K)\right)$. We get

$$\begin{aligned} V \uplus W &= \biguplus_{i=1}^{k_1} V_i \cup \biguplus_{i=1}^{k_2} W_i \\ &= \biguplus_{i=1}^{k_1} \left(Y_i^V \uplus \biguplus_{j=1}^{k_2} Y_{i,j}^{V,W} \right) \cup \biguplus_{j=1}^{k_2} \left(Y_j^W \uplus \biguplus_{i=1}^{k_1} Y_{i,j}^{V,W} \right) \\ &= \biguplus_{i=1}^{k_1} Y_i^V \uplus \biguplus_{j=1}^{k_2} Y_j^W \uplus \biguplus_{i=1}^{k_1} \biguplus_{j=1}^{k_2} Y_{i,j}^{V,W} \ . \end{aligned}$$

Since $\pi_n(V), \pi_n(W), \pi_n(V_i), \pi_n(W_i) \in \mathcal{X}^{n-1}$, it holds that $\pi_n\left(Y_i^V\right) = X_i^V$, $\pi_n\left(Y_i^W\right) = X_i^W$ and $\pi_n\left(Y_{i,j}^{V,W}\right) = X_{i,j}^{V,W}$ are elements of $\mathcal{X}^{n-1} \subseteq \mathcal{C}^{n-1}$.

For all $v, w \in X_i^V$, we get

$$\begin{aligned} c_1\left(\alpha_n\left((\pi_n)^{-1}_{|Y_i^V}(\{v\})\right)\right) &= c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V_i}(\{v\})\right)\right) \\ &= c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V_i}(\{w\})\right)\right) \\ &= c_1\left(\alpha_n\left((\pi_n)^{-1}_{|Y_i^V}(\{w\})\right)\right) \ . \end{aligned}$$

An analogous argument holds for $v, w \in X_i^W$.

For $v, w \in X_{i,j}^{V,W}$, we have

$$\begin{aligned} c_1\left(\alpha_n\left((\pi_n)^{-1}_{|X_{i,j}^{V,W}}(\{v\})\right)\right) &= c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V_i}(\{v\})\right) \uplus \alpha_n\left((\pi_n)^{-1}_{|W_i}(\{v\})\right)\right) \\ &= c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V_i}(\{v\})\right)\right) + c_1\left(\alpha_n\left((\pi_n)^{-1}_{|W_i}(\{v\})\right)\right) \\ &= c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V_i}(\{w\})\right)\right) + c_1\left(\alpha_n\left((\pi_n)^{-1}_{|W_i}(\{w\})\right)\right) \\ &= c_1\left(\alpha_n\left((\pi_n)^{-1}_{|V_i}(\{w\})\right) \uplus \alpha_n\left((\pi_n)^{-1}_{|W_i}(\{w\})\right)\right) \\ &= c_1\left(\alpha_n\left((\pi_n)^{-1}_{|X_{i,j}^{V,W}}(\{w\})\right)\right) \ . \end{aligned}$$

In summary, the $Y_{i,j}^{V,W}$ give a decomposition of $V \uplus W$ that fulfills (2.3)2b), which proves that $V \uplus W$ is (K,n)-enumerable. □

2.3 Linear Systems

In this section, we give a first, simple example for a well-behaved class of enumerable sets.

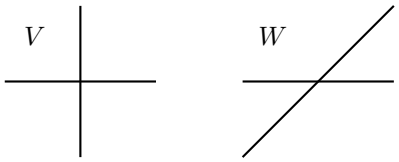
Definition 2.19. Let K be an infinite field. For any linear polynomial $p \in K[x_1, \ldots, x_n]$, the set $H(p) = \{\mathbf{a} \in K^n | p(\mathbf{a}) = 0\}$ is called a **hyperplane** in K^n.

Let $\mathcal{H}^n = \mathcal{H}^n_K$ be the closure of the set of all hyperplanes and complements of hyperplanes in K^n under finite intersections and finite unions. ◁

This is more general than hyperplane arrangements as discussed in [OT92]. In particular, a hyperplane arrangement only represents a set of hyperplanes and all their intersections, but does not consider the intersection of a hyperplane with the complement of another hyperplane. We will consider the special case of hyperplane arrangements in Example (2.23).

Before we show that this is a strongly well-behaved class of enumerable sets over K, we provide a simple example of two $(\mathbb{Q}, 2)$-enumerable sets in $\mathcal{H}^2$ and compute their counting polynomials.

Example 2.20. Let $V := \{(a, 0) | a \in \mathbb{Q}\} \cup \{(0, a) | a \in \mathbb{Q}\} \subseteq \mathbb{Q}^2$ and $W := \{(a, 0) | a \in \mathbb{Q}\} \cup \{(a, a) | a \in \mathbb{Q}\} \subseteq \mathbb{Q}^2$.



First consider V. To show $(\mathbb{Q}, 2)$-enumerability, rewrite $V = V_1 \uplus V_2$ with

$$V_1 := \{(a, 0) | a \in \mathbb{Q} \setminus \{0\}\} \qquad V_2 := \{(0, a) | a \in \mathbb{Q}\} \ .$$

Since $\pi_2(V_1) = \mathbb{Q} \setminus \{0\} \subseteq \mathbb{Q}^1$ is $(\mathbb{Q}, 1)$-enumerable and $\alpha_2((\pi_2)^{-1}_{|V}(\{a\})) = \{0\}$ for all $a \in \mathbb{Q} \setminus \{0\}$. We see that V_1 is elementary $(\mathbb{Q}, 2)$-enumerable with $c(V_1) = (u - 1) \cdot 1$. Looking at V_2, we get $\pi_2(V_2) = \{0\}$ and $\alpha_2((\pi_2)^{-1}_{|V}(\{0\})) = \mathbb{Q}$, again showing elementary $(\mathbb{Q}, 2)$-enumerability with $c(V_2) = 1 \cdot u$. In summary, we get $c(V) = c(V_1) + c(V_2) = 2u - 1$.

In a similar manner, we rewrite $W = W_1 \uplus W_2$ with $W_1 := W \setminus \{(0, 0)\}$ and $W_2 := \{(0, 0)\}$. For all $a \in \pi_2(W_1) = \mathbb{Q} \setminus \{0\}$, we get $\alpha_2((\pi_2)^{-1}_{|W}(\{a\})) = \{0, a\}$ and thus $c(W_1) = (u-1) \cdot 2$. Thus, $c(W) = c(W_1) + c(W_2) = c(W_1) + |W_2| = 2u - 1$. ◁

We notice that the counting polynomial of two lines that intersect in a single point is always $2u - 1$. We will generalize this result below.

Theorem 2.21. *The class $\mathcal{H}$ as defined in Definition (2.19) is a strongly well-behaved class of enumerable sets.*

Proof. Let $n \in N$. By De-Morgan's rules, each set in $\mathcal{H}^n$ can be written as

$$\bigcup_i \left(\bigcap_j H(p_{i,j}) \cap \bigcap_j K^n \setminus H(q_{i,j}) \right) \tag{2.4}$$

for given linear polynomials $p_{i,j}$ and $q_{i,j}$. The complement of such a set is again of this form, in particular

$$\begin{aligned} K^n \setminus \bigcup_{i=1}^{k} \left(\bigcap_{j=1}^{l_i} H(p_{i,j}) \cap \bigcap_{j=1}^{m_i} K^n \setminus H(q_{i,j}) \right) &= \bigcap_{i=1}^{k} \left(K^n \setminus \left(\bigcap_{j=1}^{l_i} H(p_{i,j}) \cap \bigcap_{j=1}^{m_i} K^n \setminus H(q_{i,j}) \right) \right) \\ &= \bigcap_{i=1}^{k} \left(\bigcup_{j=1}^{l_i} (K^n \setminus H(p_{i,j})) \cup \bigcup_{j=1}^{m_i} H(q_{i,j}) \right) \end{aligned}$$

$$= \bigcup_{j_1=1}^{l_1+m_1} \cdots \bigcup_{j_k=1}^{l_k+m_k} \bigcap_{i=1}^{k} \begin{cases} K^n \setminus H(p_{i,j_i}) & j_i \leq l_i \\ H(q_{i,j_i-l_i}) & j_i > l_i \end{cases} ,$$

and thus $\mathcal{H}^n$ is closed under unions, complements and intersections. Now consider

$$\pi_n \left(\bigcup_i \left(\bigcap_j H\left(p_{i,j}\right) \cap \bigcap_j K^n \setminus H\left(q_{i,j}\right) \right) \right) = \bigcup_i \left(\pi_n \left(\bigcap_j H\left(p_{i,j}\right) \cap \bigcap_j K^n \setminus H\left(q_{i,j}\right) \right) \right) .$$

In order to show that this is an element of $\mathcal{H}^{n-1}$, it is sufficient to show that the set

$$\pi_n \left(\bigcap_{j=1}^{l} H\left(p_j\right) \cap \bigcap_{j=1}^{m} K^n \setminus H\left(q_j\right) \right)$$

is in $\mathcal{H}^{n-1}$.

Due to the Gaussian algorithm, we may without loss of generality assume that if for any $1 \leq i \leq l$, $l_i = \max \left\{ l' \in \underline{n} \middle| \deg_{x_{l'}}(p_i) \neq 0 \right\}$, then for any $j \neq i$, $\deg_{x_{l_i}}(p_j) = 0$ and for any j, $\deg_{x_{l_i}}(q_j) = 0$. In this situation, we can simply omit all p_i and q_i with $\deg_{x_n}(p_i) \neq 0$ and $\deg_{x_n}(q_i) \neq 0$, respectively, and get

$$\pi_n \left(\bigcap_{j=1}^{l} H\left(p_j\right) \cap \bigcap_{j=1}^{m} K^n \setminus H\left(q_j\right) \right) = \bigcap_{\substack{j=1,\ldots,l \\ \deg_{x_n}(p_j)=0}} H\left(p_j\right) \cap \bigcap_{\substack{j=1,\ldots,l \\ \deg_{x_n}(q_j)=0}} K^n \setminus H\left(q_j\right) .$$

To show (2.10)5., note that for every $U \in \mathcal{H}^{n-1}$, $U \times K \in \mathcal{H}^n$, since the latter set is given by the same linear polynomials that define U.

Condition (2.10)6. holds since for any $p \in K[x_1, \ldots, x_n]$ that defines a hyperplane and any $(a_1, \ldots, a_m) \in K^m$, $p(a_1, \ldots, a_m, x_{m+1}, \ldots, x_n) \in K[x_{m+1}, \ldots, x_n]$ again defines a hyperplane.

According to Proposition (2.18), we need to show that each set can be decomposed into a disjoint union of elementary enumerable sets. First note that according to Lemma (2.15), we can rewrite the representation (2.4) such that the union is disjoint. In particular, if $H_{i,j} = \begin{cases} H\left(p_{i,j}\right) & j \leq l_j \\ K^n \setminus H\left(q_{i,j}\right) & j > l_j \end{cases}$, then

$$\left(\bigcap_{j=1}^{l_1+m_1} H_{1,j} \right) \cup \left(\bigcap_{j=1}^{l_2+m_2} H_{2,j} \right) = \left(\bigcap_{j=1}^{l_1+m_1} H_{1,j} \right) \uplus \left(\left(\bigcap_{j=1}^{l_2+m_2} H_{2,j} \right) \setminus \left(\bigcap_{j=1}^{l_1+m_1} H_{1,j} \right) \right)$$

and

$$\left(\left(\bigcap_{j=1}^{l_2+m_2} H_{2,j} \right) \setminus \left(\bigcap_{j=1}^{l_1+m_1} H_{1,j} \right) \right) = \biguplus_{i=1}^{l_1+m_1} \left(\bigcap_{j=1}^{l_2+m_2} H_{2,j} \cap \bigcap_{j=1}^{i-1} H_{1,j} \cap \left(K^n \setminus H_{1,i}\right) \right) .$$

It remains to show that each set $M = \bigcap_{j=1}^{l} H\left(p_j\right) \cap \bigcap_{j=1}^{m} K^n \setminus H\left(q_j\right)$ is elementary (K,n)-enumerable. Assume without loss of generality that (as above), the p_i are in reduced row echelon form and that the q_j are reduced modulo the p_i, i.e. if for any $1 \leq i \leq l$, $l_i = \max \left\{ l' \in \underline{n} \middle| \deg_{x_{l'}}(p_i) \neq 0 \right\}$, then for any $j \neq i$, $\deg_{x_{l_i}}(p_j) = 0$ and for any j, $\deg_{x_{l_i}}(q_j) = 0$. Also assume that none of the p_j is zero and none of the q_j is a non-zero constant and that for all $a \in K^*$ and all $i \neq j$, $p_i \neq a \cdot p_j$ and $q_i \neq a \cdot q_j$.

If any p_j is a nonzero constant or any $q_j = 0$, then the set is empty. For the other cases, we show elementary (K,n)-enumerability by induction. For $n = 1$, we either have $l = 1$ and $m = 0$,

in which case the set only has one element, or we have $l = 0$ and $m >= 0$, which implies that the complement has $m < \infty$ elements.

For $n > 1$, we know by induction that $\pi_n(M)$ is elementary $(K, n-1)$-enumerable. We again have two cases: In the first case, there is a unique i such that $\deg_{x_n}(p_i) = 1$. In this case, for every $v \in \pi_n(M)$, we get $|(\pi_n)^{-1}_{|M}(\{v\})| = 1$. In the second case, there is no such i. Then, let $d = \left|\left\{j \middle| \deg_{x_n}(q_j) = 1\right\}\right|$. For every $v \in \pi_n(M)$, we now get $\left|K \setminus \alpha_n\left((\pi_n)^{-1}_{|M}(\{v\})\right)\right| = d$.

In summary, we have shown that the class $\mathcal{H}$ is a strongly well-behaved class of enumerable sets over K. □

The last theorem also makes it obvious how to compute the counting polynomials of linear systems with the Gaussian algorithm. We reconsider the previous example.

Example 2.22. Let V, W be as in Example (2.20). Then

$$\begin{aligned} V &= H(x_2) \cup H(x_1) \\ &= H(x_2) \uplus \left(H(x_1) \cap \left(\mathbb{Q}^2 \setminus H(x_2)\right)\right) \end{aligned}$$

and

$$\begin{aligned} W &= H(x_2) \cup H(x_1 - x_2) \\ &= H(x_2) \uplus \left(H(x_1 - x_2) \cap \left(\mathbb{Q}^2 \setminus H(x_2)\right)\right) \\ &= H(x_2) \uplus \left(H(x_1 - x_2) \cap \left(\mathbb{Q}^2 \setminus H(x_1)\right)\right) \ . \end{aligned}$$

According to this, the counting polynomials are $c(V) = c(W) = u \cdot 1 + 1 \cdot (u-1) = 2u - 1$. ◁

We conclude this section by determining the counting polynomials of a large class of linear systems.

Example 2.23. Let K be an infinite field, $n > 1$, and $p_1, \ldots, p_m \in K[x_1, \ldots, x_n]$ pairwise distinct. Assume that there are no $j_1 < \ldots < j_{\min\{m,n\}}$ such that there is a non-trivial linear combination $\sum_{i=1}^{\min\{m,n\}} a_i p_{j_i} \in K$. Further assume that there are no $j_1 < \ldots < j_{\min\{m,n+1\}}$ such that there is a non-trivial linear combination $\sum_{i=1}^{\min\{m,n+1\}} a_i p_{j_i} = 0$. In particular, no two hyperplanes are parallel and any two hyperplanes intersect.

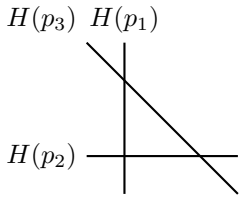
Let $V = \bigcap_{j=1}^{m} H(p_m)$. Then, according to the proof of Theorem (2.21),

$$c(V) = \begin{cases} u^{n-m} & m \leq n \\ 0 & m > n \end{cases} \ .$$

As a consequence of this and of Lemma (2.14)2., we can determine the counting polynomial of the complement of the union our m hyperplanes:

$$c\left(K^n \setminus \bigcup_{i=0}^{m} H(p_i)\right) = \sum_{i=0}^{\min\{m,n\}} (-1)^i \binom{m}{i} u^{n-i}$$

As a first example, consider $n = 2$, $p_1 = x_1$, $p_2 = x_2$ and $p_3 = x_1 + x_2 - 1$ and $V_1 = K^2 \setminus (H(p_1) \cup H(p_2) \cup H(p_3))$. We get $c(V_1) = u^2 - 3u + 3$, which is also evident from the following picture, where the lines indicate the complement of V_1:



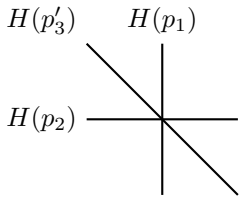
We now set $p_3' = x_1 + x_2$ and $V_2 = K^2 \setminus (H(p_1) \cup H(p_2) \cup H(p_3'))$. However, $p_1 + p_2 = p_3$ and thus we cannot apply the previous result. Again using Lemma (2.14)2., we write the counting polynomial as follows.

$$\begin{aligned} c(V_2) = c(K^2) & \\ & - c(H(p_1)) - c(H(p_2)) - c(H(p_3')) \\ & + c(H(p_1) \cap H(p_2)) + c(H(p_1) \cap H(p_3')) + c(H(p_2) \cap H(p_3')) \\ & - c(H(p_1) \cap H(p_2) \cap H(p_3')) \end{aligned}$$

Everything except the last summand can be determined using the above method. Therefore $c(V_2) = u^2 - 3u + 3 - c(H(p_1) \cap H(p_2) \cap H(p_3'))$. We use the proof of Theorem (2.21) and the GAUSSian algorithm to rewrite

$$\begin{aligned} H(p_1) \cap H(p_2) \cap H(p_3') &= H(x_1) \cap H(x_2) \cap H(x_1 + x_2) \\ &= H(x_1) \cap H(x_2) \cap H(0) \\ &= H(x_1) \cap H(x_2) \end{aligned}$$

and get $c(H(x_1) \cap H(x_2) \cap H(x_1 + x_2)) = 1$, implying $c(V_2) = u^2 - 3u + 2$. Again, we demonstrate this result in a picture:



This counting polynomial is the characteristic polynomial of the hyperplane arrangement defined by the p_i, cf. [OT92, Def. 2.52]. ◁

2.4 The Counting Tree

We will now introduce the counting tree. It is a refined version of the counting polynomial that takes into account the fibration structure exposed by the projections π_i.

For any set $V \subseteq K^n$, we can construct an element of V by iteratively taking fibers of the projections. In particular, if $(a_1, \ldots, a_l)$ is the tuple of the first l components of an element in V, i.e. $(a_1, \ldots, a_l) \in \pi_{n,l}(V)$, then the fiber of the projection is $F_{l,V}((a_1, \ldots, a_l)) = \{a_{l+1} | (a_1, \ldots, a_l, a_{l+1}) \in \pi_{n,l+1}(V)\}$.

If the set V is elementary enumerable, we also know that the fiber is either finite or cofinite, and $\tau_l(V) := c_1(F_{l,V}(a_1, \ldots, a_l))$ is independent of the element $(a_1, \ldots, a_l)$. Thus, the tuple $\mathrm{ct}(V) := (\tau_1(V), \ldots, \tau_n(V))$ is a property of the set V, which we call the counting type of V. It shows us exactly how many possibilities we have for choosing each component of an element when all previous components are fixed.

The counting polynomial is the product $c_n(V) = \tau_1(V) \cdots \tau_n(V)$, but this fibration information is lost with the multiplication. For example, if $\mathrm{ct}(V) = (2, 3)$ and $\mathrm{ct}(W) = (3, 2)$, then $c_2(V) = c_2(W)$, but their fibration structure is different.

Providing the same information for a not necessarily elementary enumerable set V is more complicated since $\mathrm{ct}(V)$ is not defined. We first consider the case $n = 2$, so let V be $(K, 2)$-enumerable. For $a \in \pi_2(V)$, the fiber over a is

$$\phi_a(V) := \{b \in K | (a, b) \in V\} = \alpha_2 \left((\pi_2)_{|V}^{-1}(\{a\}) \right) ,$$

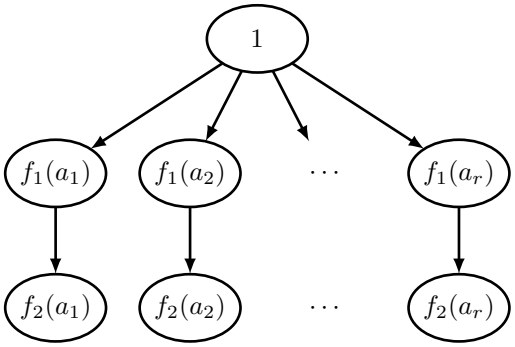
which we also call the evaluation at a. Define

$$F(a) := \{b \in K | c_1(\phi_a(V)) = c_1(\phi_b(V))\} ,$$

which is the set of all $b \in K$ whose fiber has the same size as the fiber of a. Then the set $\biguplus_{b \in F(a)} (\{b\} \times \phi_b(V))$ is elementary $(K, 2)$-enumerable with counting type

$$(f_1(a), f_2(a)) := (c_1(F(a)), c_1(\phi_a(V))) \ .$$

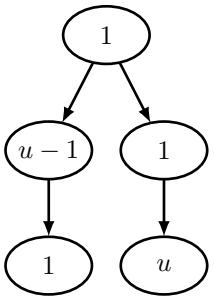
By construction, $\{F(b) | b \in \pi_2(V)\}$ is a partition of $\pi_2(V)$. We will later see that this partition is finite and thus equal to $\{F(a_1), \ldots, F(a_r)\}$ for certain $a_1, \ldots, a_r \in K$ with $F(a_i) \cap F(a_j) = \emptyset$ for $i \neq j$. This construction encodes the fibration structure of V into the tuples $(f_1(a_i), f_2(a_i)), i = 1, \ldots, r$, which we visualize in a tree structure as follows.



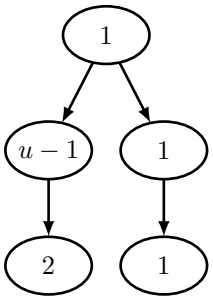
We call this visualization the counting tree of V.

Example 2.24. Reconsider Example (2.20). While we had $c(V) = c(W) = 2u - 1$, the fibration structure of V and W was different. For all $a \in \mathbb{Q} \setminus \{0\}$, the fiber $(\pi_2)^{-1}_{|V}(\{a\})$ had one element, while the fiber $(\pi_2)^{-1}_{|W}(\{a\})$ had two elements. Furthermore, the fiber $(\pi_2)^{-1}_{|V}(\{0\})$ was infinite with counting polynomial u and the fiber $(\pi_2)^{-1}_{|W}(\{0\})$ had one element.

Following the considerations above, the counting trees of V and W must be as follows.



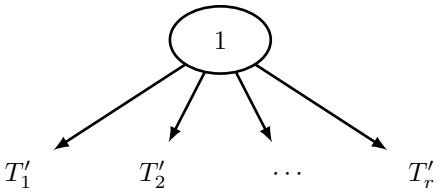
(a) Counting tree of V



(b) Counting tree of W

◁

Now consider $n = 3$ and let V be $(K, 3)$-enumerable. For every $a \in \pi_{3,1}(V) \subseteq K$, the evaluation at a is defined by $\phi_a(V) := \{(b_1, b_2) \in K^2 | (a, b_1, b_2) \in V\}$ and is clearly $(K, 2)$-enumerable. Therefore, due to the discussion above, we can construct the counting tree of $\phi_a(V)$. As before, partition the set into classes $F(a) := \{b \in K | \phi_b(V)$ and $\phi_a(V)$ have the same counting tree$\}$. We will later show that this partition is again finite and thus given by $F(a_1), \ldots, F(a_r)$ for $a_1, \ldots, a_r \in K$. Denote the counting tree of $\phi_{a_i}(V)$ by T_i and let T_i' be the same tree, but with the 1 in the root replaced by $c_1(F(a_i))$. Then we visualize the fibration structure with the following counting tree.



For $n = 3$, we will give an example of a counting tree in Example (2.38). It is obvious how the above description of the counting tree can be generalized to $n > 3$.

In order to formally define and construct such a counting tree, a specific decomposition into enumerable sets is required.

Definition 2.25. Let $V \neq \emptyset$ be (K, n)-enumerable and $V = \biguplus_{i=1}^{k} V_i$ where each V_i is non-empty and elementary (K, n)-enumerable. We call $(V_i)_{i=1,\dots,k}$ a **hereditarily disjoint decomposition** of V if for each l with $0 \leq l \leq n$, $\{\pi_{n,l}(V_i) | 1 \leq i \leq k\}$ is a finite set of pairwise disjoint non-empty (K, l)-enumerable sets. ◁

From now on, let $\mathcal{X}$ be a well-behaved class of enumerable sets. Before proceeding to the definition of counting trees, we show that a hereditarily disjoint decomposition exists.

Lemma 2.26. *Let $S \in \mathcal{X}^n$ be elementary (K, n)-enumerable and $T \in \mathcal{X}^l$ be elementary (K, l)-enumerable with $l < n$ such that $T \subseteq \pi_{n,l}(S)$. Then $S \cap (T \times K^{n-l}) \in \mathcal{X}^n$ is elementary (K, n)-enumerable.*

Proof. $S \cap (T \times K^{n-l}) \in \mathcal{X}^n$ according to Definition (2.10)5.

Consider $v, w \in \pi_{l'}\left(\pi_{n,l'}\left(S \cap \left(T \times K^{n-l}\right)\right)\right)$. If $l' \leq l$, then

$$\begin{aligned}(\pi_{l'})^{-1}_{|\pi_{n,l'}(S\cap(T\times K^{n-l}))}(\{v\}) &= (\pi_{l'})^{-1}_{|\pi_{n,l'}(T)}(\{v\}) \\ &= (\pi_{l'})^{-1}_{|\pi_{n,l'}(T)}(\{w\}) = (\pi_{l'})^{-1}_{|\pi_{n,l'}(S\cap(T\times K^{n-l}))}(\{w\}) \ .\end{aligned}$$

Otherwise

$$\begin{aligned}(\pi_{l'})^{-1}_{|\pi_{n,l'}(S\cap(T\times K^{n-l}))}(\{v\}) &= (\pi_{l'})^{-1}_{|\pi_{n,l'}(S)}(\{v\}) \\ &= (\pi_{l'})^{-1}_{|\pi_{n,l'}(S)}(\{w\}) = (\pi_{l'})^{-1}_{|\pi_{n,l'}(S\cap(T\times K^{n-l}))}(\{w\}) \ .\end{aligned}$$

□

Theorem 2.27. *For every $V \in \mathcal{X}^n \setminus \{\emptyset\}$, a hereditarily disjoint decomposition $(V_i)_{i=1,\dots,k}$ of V exists.*

Proof. We introduce an order on univariate polynomials with positive leading coefficients: For $a, b \in \mathbb{Z}[x]$, we say that $a \prec b$ if $b - a$ has a positive leading coefficient.

According to Lemma (2.5) and Definition (2.10), there exists a decomposition $V = \biguplus_{i=1}^{k} V_i$ where each $V_i \in \mathcal{X}^n$ is elementary (K, n)-enumerable. Find the largest l such that the elements of $X := \{\pi_{n,l}(V_i) | 1 \leq i \leq k\}$ are not pairwise disjoint. According to Lemma (2.15), there is a set $X' \subseteq \mathcal{X}^n$ such that the elements of X' are disjoint and their union is the same as the union of the elements of X. Construct the set $\bar{X}$ by replacing each set in X' with a disjoint decomposition into elementary (K, n)-enumerable sets in $\mathcal{X}^n$. By construction, for each $1 \leq j \leq k$ and each $S \in \bar{X}$, either $\pi_{n,l}(V_j) \cap S = \emptyset$ or $S \subseteq \pi_{n,l}(V_j)$. Define

$$W = \left\{V_j \cap \left(S \times K^{n-l}\right) \middle| 1 \leq j \leq n, S \in \bar{X}\right\} \setminus \{\emptyset\} = \{W_1, \dots, W_{k'}\} \ .$$

Clearly, $V = \biguplus_{i=1}^{k'} W_i$ and by Lemma (2.26), each element of W is elementary (K, n)-enumerable.

The set $\{\pi_{n,l}(S) | S \in W\}$ now contains pairwise disjoint sets by construction. It remains to be shown that $\{\pi_{n,l'}(S) | S \in W\}$ remains a set of pairwise disjoint sets for $l' > l$. The method described above constructs a disjoint decomposition $Q_1, \dots, Q_r$ of $\pi_{n,l}(V)$. Let $\{\pi_{n,l'}(V_i) | 1 \leq i \leq$

$k\} = \{P_1, \ldots, P_m\}$ such that $\pi_{n,l'}(V) = \biguplus_{i=1}^{m} P_i$. Furthermore, for each P_i there is at least one $t(i)$ such that $\pi_{n,l'}(V_{t(i)}) = P_i$ (in particular, for $l' = n$, $t(i) = i$). Then the following holds:

$$\begin{aligned}
\pi_{n,l'}(V) &= \biguplus_{i=1}^{m} P_i = \biguplus_{i=1}^{m} \pi_{n,l'}\left(V_{t(i)}\right) \\
&= \biguplus_{i=1}^{m} \pi_{n,l'}\left(V_{t(i)} \cap \left(\pi_{n,l}(V) \times K^{n-l}\right)\right) \\
&= \biguplus_{i=1}^{m} \pi_{n,l'}\left(V_{t(i)} \cap \left(\biguplus_{j=1}^{r} Q_j \times K^{n-l}\right)\right) \\
&= \biguplus_{i=1}^{m} \biguplus_{j=1}^{r} \pi_{n,l'}\left(V_{t(i)} \cap \left(Q_j \times K^{n-l}\right)\right) \\
&= \biguplus_{i=1}^{m} \biguplus_{j=1}^{r} \pi_{n,l'}\left(V_{t(i)} \cap \left(Q_j \times K^{n-l}\right)\right) \\
&= \biguplus_{i=1}^{m} \biguplus_{j=1}^{r} P_i \cap \left(Q_j \times K^{l'-l}\right)
\end{aligned}$$

Therefore, by iterating the process, we eventually arrive at a hereditarily disjoint decomposition. □

A hereditarily disjoint decomposition of an enumerable set is the right decomposition to be able to define the counting tree.

For this definition, we need some basic terminology from graph theory. A **graph** $(\mathcal{V}, \mathcal{E})$ is defined by its finite set of vertices $\mathcal{V}$ and its set of edges $\mathcal{E}$. In an **undirected graph** $\mathcal{E} \subseteq \mathcal{V}^2/\sim$, where $\sim$ is the equivalence relation generated by $\{(a,b) \sim (b,a) | a, b \in \mathcal{V}\}$. In a **directed graph** $\mathcal{E} \subseteq \mathcal{V}^2$. In both cases, we assume that the graph has no loops, i.e. $(v,v) \notin \mathcal{E}$ for all $v \in \mathcal{V}$. Each directed graph defines a corresponding undirected graph by replacing each edge with its equivalence class w.r.t. $\sim$. An isomorphism of two (directed or undirected) graphs $(\mathcal{V}, \mathcal{E})$ and $(\mathcal{V}', \mathcal{E}')$ is a bijection $\varphi : \mathcal{V} \xrightarrow{\sim} \mathcal{V}'$ that induces a bijection $(\varphi, \varphi) : \mathcal{E} \xrightarrow{\sim} \mathcal{E}'$.

A **path** is an r-tuple $(p_0, \ldots, p_r) \in \mathcal{V}^r$ for some $r > 0$ such that $(p_{i-1}, p_i) \in \mathcal{E}$ for $i = 1, \ldots, r$. In the undirected case, we also require that $(p_{i-2}, p_{i-1}) \neq (p_{i-1}, p_i)$ for $i = 2, \ldots, r$. If $v \neq w$, the **distance** from v to w, is the length of the shortest path from v to w, or ∞ if no path from v to w exists. We further define the distance from v to itself as 0. A graph is **connected** if for each $v \neq w \in \mathcal{V}$, there is a **path** from v to w. A **cycle** is a path from a vertex $v \in \mathcal{V}$ to itself.

A graph that is connected and has no cycles is a **tree**. A **directed tree** is a directed graph with no cycles whose underlying undirected graph is a tree. A **rooted tree** is a directed tree with a distinguished root $\mathcal{R}$, such that there is no vertex $v \in \mathcal{V}$ with $(v, \mathcal{R}) \in \mathcal{E}$ and for every vertex $v \in \mathcal{V}$ there is a (unique) path from $\mathcal{R}$ to v. The distance from the root to v is called the **order** of v.

Definition 2.28. Let $(\mathcal{V}, \mathcal{E})$ be a rooted tree. Furthermore, let L be any set and $\lambda : \mathcal{V} \to L$. We call $(\mathcal{V}, \mathcal{E}, \lambda)$ a **labeled tree**, L the set of labels and λ the label map.

An isomorphism of two labelled trees $(\mathcal{V}, \mathcal{E}, \lambda)$ and $(\mathcal{V}', \mathcal{E}', \lambda')$ is an isomorphism φ of graphs such that $\lambda'(\varphi(v)) = \lambda(v)$ for all $v \in \mathcal{V}$. ◁

Definition 2.29. Let $V \in \mathcal{X}^n \setminus \{\emptyset\}$ and $(V_i)_{i=1,\ldots,k}$ a hereditarily disjoint decomposition of V. Consider the directed graph with vertices

$$\mathcal{V} = \{\pi_{n,l}(V_i) | l = 0, \ldots, n, i = 1, \ldots, k\}$$

and edges

$$\mathcal{E} = \left\{(W_1, W_2) \in \mathcal{V}^2 \middle| \exists 1 \leq l \leq n : W_1 \in \mathcal{X}_K^{l-1}, W_2 \in \mathcal{X}_K^l, W_1 = \pi_l(W_2)\right\} .$$

We call the graph $(\mathcal{V}, \mathcal{E})$ a **fibration tree** of V.

Consider the map $\hat{c} : \mathcal{V} \to \mathbb{Z}[u]$ that maps a vertex W to $c_1\left(\alpha_j\left(\pi_{j|W}^{-1}(\{w\})\right)\right)$ for any $w \in \pi_j(W)$ if $W \in \mathcal{X}^j$, $j > 0$. If $W \in \mathcal{X}^0$, then $W = \pi_{n,0}(V_i) = K^0$ and we define $\hat{c}(W) = 1$. We call the labelled tree $(\mathcal{V}, \mathcal{E}, \hat{c})$ (and any labelled tree isomorphic to it) a **pre-counting tree** of V. ◁

Following an edge in the tree means taking the pre-image of a projection, and the labels are the counting polynomials of the fibers. We get an analogon of the counting polynomial that tells us more about its origin.

Note that the set of vertices includes $\pi_{n,0}(V_i) = K^0$. This is the formal 0-tuple, i.e. $K^0 = \{()\}$. Thus, $\pi_{n,0}(V_i)$ is independent of i.

In a pre-counting tree, we are only interested in the labels, not the vertices themselves, which is why we allow any isomorphic tree as pre-counting tree. In fact, we draw the tree in a way that keeps the structure defined by the edges and label it, but do not keep the actual objects in $\mathcal{V}$.

We need to make sure that Definition (2.29) actually yields a well-defined rooted tree.

Proposition 2.30. *Let $V \in \mathcal{X}^n \setminus \{\emptyset\}$ and $(V_i)_{i=1,\dots,k}$ a hereditarily disjoint decomposition of V.*

1. *The fibration tree defined by $(V_i)_i$ is a rooted tree with root $\pi_{n,0}(V_i) = K^0$.*
2. *The pre-counting tree defined by $(V_i)_i$ is a labelled tree.*

Proof. 1. As every edge connects a set in $\mathcal{X}^{i-1}$ with a set in $\mathcal{X}^i$, the graph cannot have cycles (both as directed and as undirected graph). For every $i = 1, \dots, k$, there is a unique path $\pi_{n,0}(V_i) \mapsto \pi_{n,1}(V_i) \mapsto \dots \mapsto \pi_{n,n}(V_i) = V_i$ from the root to V_i. This implies that the underlying undirected tree is connected and thus we have a well-defined rooted tree.

2. Follows directly from the previous statement. □

It is apparent that each leaf of a pre-counting tree of V has order n, since a path from the root to the leaf in a fibration tree is always given by $(\pi_{n,0}(X), \dots, \pi_{n,n}(X))$ for some $X \subseteq V$. We can thus draw a counting tree by arranging the vertices in rows according to their order, then draw edges pointing from top to bottom.

We want to use a pre-counting tree to obtain the counting tree of a (K, n)-enumerable set.

Definition 2.31. Let $T = (\mathcal{V}, \mathcal{E}, \lambda)$ be a labelled tree with set of labels L and $v \in \mathcal{V}$ a vertex. Define

$$\mathcal{V}' = \left\{w \in \mathcal{V} \middle| \exists r > 0, (p_0, \dots, p_r) \in \mathcal{V}^{r+1} \text{ such that } p_0 = v, p_r = w, (p_{i-1}, p_i) \in \mathcal{E}, i = 1, \dots, r\right\}$$

and $\mathcal{E}' = \{(a, b) \in \mathcal{E} | a, b \in \mathcal{V}'\}$. Further define

$$\lambda' : \mathcal{V}' \to L \uplus \{O\} : w \mapsto \begin{cases} O & w = v \\ \lambda(w) & \text{otherwise} \end{cases} .$$

Then we call $(\mathcal{V}', \mathcal{E}', \lambda')$ the **subtree** of v in T. ◁

Definition 2.32. Let $T = (\mathcal{V}, \mathcal{E}, \lambda)$ be a labelled tree with set of labels L and $\mathcal{W} \subseteq \mathcal{V}$. Define $\mathcal{E}_{|\mathcal{W}} = \{(c, d) \in \mathcal{E} | c, d \in \mathcal{W}\}$. Then we call $T_{|\mathcal{W}} = \left(\mathcal{W}, \mathcal{E}_{|\mathcal{W}}, \lambda_{|W}\right)$ the **restriction** of T to $\mathcal{W}$. ◁

Note that the restriction of a tree is again a tree if the difference between $\mathcal{V}$ and $\mathcal{W}$ corresponds to a union of subtrees.

Definition 2.33. Define the relation $\widehat{\prec}$ on pre-counting trees as follows: For $T_1 = (\mathcal{V}_1, \mathcal{E}_1, \hat{c}_1)$ and $T_2 = (\mathcal{V}_2, \mathcal{E}_2, \hat{c}_2)$, $T_1 \widehat{\prec} T_2$ if there are vertices $l_1 \in \mathcal{V}_1$ and $l_{2,1}, l_{2,2} \in \mathcal{V}_2$, such that

1. the subtrees of l_1, $l_{2,1}$ and $l_{2,2}$ are isomorphic as labelled trees,
2. $\hat{c}_1(l_1) = \hat{c}_2(l_{2,1}) + \hat{c}_2(l_{2,2})$,
3. $(T_1)_{|\mathcal{V}_1 \setminus \mathcal{W}_{l_1}} \cong (T_2)_{|\mathcal{V}_2 \setminus (\mathcal{W}_{l_{2,1}} \cup \mathcal{W}_{l_{2,2}})}$ where $\mathcal{W}_m$ is the set of vertices of the subtree of m for $m \in \{l_1, l_{2,1}, l_{2,2}\}$.

Let $\prec$ be the transitive hull of $\widehat{\prec}$.

Let furthermore $\sim$ be the reflexive, symmetric and transitive hull of $\prec$. Then we say that T_1 and T_2 are equivalent if $T_1 \sim T_2$. ◁

If $l_1, l_{2,1}, l_{2,2}$ are given as in the previous definition, we say that T_1 has been constructed from T_2 by merging $l_{2,1}$ and $l_{2,2}$ into l_1.

Proposition 2.34. *Every equivalence class of pre-counting trees has a unique $\prec$-smallest element.*

Proof. If $T_1 \prec T_2$, then the number of vertices of T_1 is smaller than then number of vertices of T_2. Therefore, there are no cycles.

Now consider $T_1 \widehat{\prec} T$ and $T_2 \widehat{\prec} T$ with $T_1 \neq T_2$. We now prove that there exists a pre-counting tree S with $S \prec T_1$ and $S \prec T_2$.

Let $t_1, t_2, t_{1,1}, t_{1,2}, t_{2,1}, t_{2,2}$ be vertices of T such that T_i is constructed from T by merging $t_{i,1}$ and $t_{i,2}$ into t_i for $i = 1, 2$. We distinguish three cases:

1. $t_{1,1}$, $t_{1,2}$, $t_{2,1}$ and $t_{2,2}$ are pairwise different vertices and none is contained in the subtree of another. Then, obtain S by merging $t_{2,1}$ and $t_{2,2}$ in T_1. Obviously, this is the same as merging $t_{1,1}$ and $t_{1,2}$ in T_2.
2. Two of the vertices are identical, without loss of generality $t_{1,1} = t_{2,1}$. Then S can be obtained from T_1 by merging t_1 with $t_{2,2}$, or from T_2 by merging t_2 with $t_{1,2}$.
3. One is contained in a subtree of the other. Without loss of generality, let $t_{2,1}$ and $t_{2,2}$ be contained in a subtree of $t_{1,1}$. The subtrees of $t_{1,1}$ and $t_{1,2}$ are isomorphic as labelled trees, thus define $t'_{2,1}$ and $t'_{2,2}$ as the images of $t_{2,1}$ resp. $t_{2,2}$ under an isomorphism. Furthermore, the subtrees of $t_{1,1}$ and t_1 are isomorphic, and we denote by $\overline{t_{2,1}}, \overline{t_{2,2}}$ the images of $t_{2,1}, t_{2,2}$. Construct S from T_1 by merging $\overline{t_{2,1}}$ and $\overline{t_{2,2}}$.

   Now, obtain a pre-counting tree from T_2 by merging $t'_{2,1}$ and $t'_{2,2}$. Since and the subtrees of $t_{1,1}$ and $t_{1,2}$ are now isomorphic again, we can merge them as well to get the same S.

It follows that for any two equivalent pre-counting trees T'_1 and T'_2, there is a pre-counting tree S' with $S' \prec T'_1$ and $S \prec T'_2$. Since the number of vertices gets smaller in a decreasing chain of pre-counting trees, but is always a positive integer, this implies that each equivalence class of pre-counting trees has a unique minimum. □

Theorem 2.35. *Any two pre-counting trees of $V \in \mathcal{X}^n \setminus \{\emptyset\}$ are equivalent.*

Proof. For $n = 1$, any pre-counting tree is of the form

$$\left(\{0, \dots, k\}, \{(0, i) | i = 1, \dots, k\}, \hat{c}\right),$$

where $\hat{c}(0) = 1$ and $\sum_{i=1}^{k} \hat{c}(i) = c(V)$. Therefore, it is equivalent to $\left(\{0, 1\}, \{(0, 1)\}, \hat{c}'\right)$ with $\hat{c}'(0) = 1$ and $\hat{c}'(1) = c(V)$.

Now assume that any two pre-counting trees of any $V \in \mathcal{X}^{n-1}$ are equivalent and prove the same for $V \in \mathcal{X}^n$. Let $V \in \mathcal{X}^n$ and for each $a \in \pi_{n,1}(V) \subseteq K$ define

$$V_a = \left\{(a_2, \dots, a_n) \in K^{n-1} \middle| (a, a_2, \dots, a_n) \in V\right\} \in \mathcal{Y}^{n-1}$$

for some strongly well-behaved class of enumerable sets $\mathcal{Y}$. For any $a \in \pi_{n,1}(V)$, per induction, any two pre-counting trees of V_a are equivalent. Now take two pre-counting trees $T = (\mathcal{V}, \mathcal{E}, \hat{c})$ and $T' = (\mathcal{V}', \mathcal{E}', \hat{c}')$ of V with the property that $(\mathcal{V}, \mathcal{E})$ and $(\mathcal{V}', \mathcal{E}')$ are fibration trees of V and let $O \in \mathcal{V}$ and $O' \in \mathcal{V}'$ be their respective roots.

Choose a fixed $v \in \mathcal{V}$ with $(O, v) \in \mathcal{V}$. The subtree of v in T is a pre-counting tree of V_a for some $a \in \pi_{n,1}(V)$ and thus equivalent to the counting tree of V_a. Let $M_a \subseteq \pi_{n,1}(V)$ be the set of all b such that V_b admits the same counting tree as V_a. It is non-empty since $a \in M_a$ and $M_a \in \mathcal{X}^1$ since it is a finite union of sets from $\mathcal{X}^1$:

$$M_a = \biguplus_{s \in S} s = \biguplus_{s \in S'} s \text{ for some } S \subseteq \mathcal{V}, S' \subseteq \mathcal{V}' \ .$$

In particular, S is the subset of $\mathcal{V}$ such that the subtree of w is equivalent to the subtree of v for all $w \in S$ and S' is the corresponding subset of $\mathcal{V}'$. Therefore, T is equivalent to a pre-counting tree where all the vertices in S are merged into a vertex $\overline{v}$, and T' is equivalent to a pre-counting tree where all the vertices in S' are merged into a vertex $\overline{v}'$. If $\overline{c}, \overline{c}'$ are the label functions of those trees, respectively, then $\overline{c}(\overline{v}) = c(M_a) = \overline{c}(\overline{v}')$.

Iterating this process will yield two isomorphic counting trees, showing that T and T' are in fact equivalent. □

Definition 2.36. Let $V \in \mathcal{X}^n \setminus \{\emptyset\}$. The $\prec$-minimal pre-counting tree of V is called the **counting tree** of V. ◁

The counting tree has an obvious connection to the counting polynomial.

Remark 2.37. Let $T = (\mathcal{V}, \mathcal{E}, \hat{c})$ be the counting tree of a set V with root $O \in \mathcal{V}$. Denote by $L = \{v \in \mathcal{V} | \nexists v' \in \mathcal{V} : (v, v') \in \mathcal{E}\}$ the set of leaves of T. For each leaf $l \in L$, there is a unique path $(O = v_0, v_1, \ldots, v_n = l)$ from the root to the leaf, such that $(v_{i-1}, v_i) \in \mathcal{E}$ for $i = 1, \ldots, n$. If we denote by $p(l) = \{v_0, \ldots, v_n\}$ the set of vertices in that path, we can recover the counting polynomial from the counting tree as follows:

$$c(V) = \sum_{l \in L} \prod_{v \in p(l)} \hat{c}(v)$$ ◁

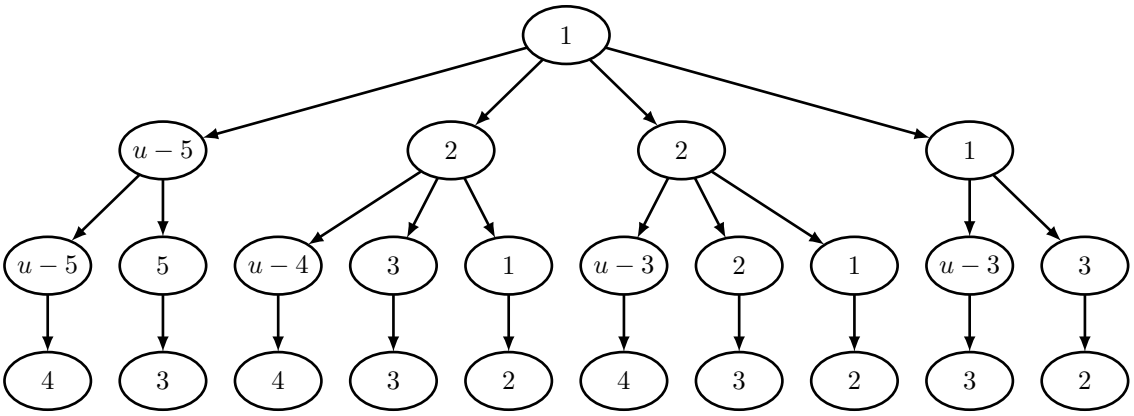
Proof. By definition of the counting tree, $V = \biguplus_{l \in L} l$ and all $l \in L$ are elementary (K, n)-enumerable. Thus, the counting polynomial is

$$\begin{aligned} c_n(V) &= \sum_{l \in L} c_n(l) \\ &= \sum_{l \in L} c_{n-1}\left(\pi_n(l)\right) \cdot c_1\left(\alpha_n\left(\left(\pi_n\right)^{-1}_{|\pi_n(l)}\left(\{v_l\}\right)\right)\right) \\ &= \sum_{l \in L} c_{n-1}\left(\pi_n(l)\right) \cdot \hat{c}(l) \end{aligned}$$

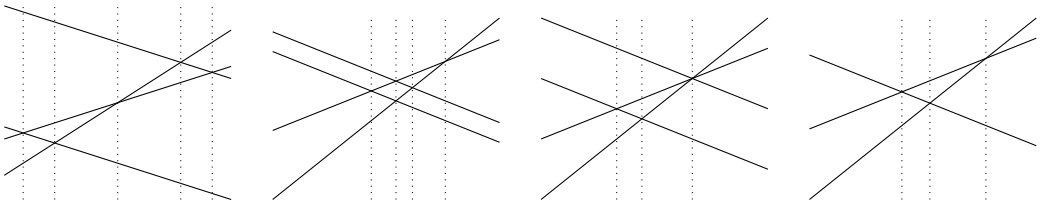
where $v_l \in \pi_n(l)$ is an arbitrary element. Since for $l \in \mathcal{X}^1$, $c_1(l) = \hat{c}(l)$, the statement holds by induction. □

We conclude our discussion of counting trees with the counting tree of the union of four hyperplanes in $\mathbb{Q}^3$.

Example 2.38. Let $p_1, p_2, p_3, p_4 \in \mathbb{Q}[x_1, x_2, x_3]$ with $p_1 := 10x_1 + x_2 + x_3 + 10$, $p_2 := x_1 + x_2 + x_3 - 1$, $p_3 := -x_2 + x_3 + 2$ and $p_4 := -3x_1 - 2x_2 + x_3 + 1$ and consider $V := \biguplus_{i=1}^4 H(p_i) \in \mathcal{H}^3_{\mathbb{Q}}$. The counting tree of V is as follows.



The four branches of the tree correspond to the sets $W_1 := \mathbb{Q} \setminus \left\{-\frac{11}{9}, -\frac{14}{11}, -\frac{27}{23}, -\frac{3}{2}, -1\right\}$, $W_2 := \left\{-\frac{14}{11}, -\frac{27}{23}\right\}$, $W_3 := \left\{-\frac{3}{2}, -1\right\}$ and $W_4 := \left\{-\frac{11}{9}\right\}$, respectively. We draw pictures of the sets $\phi_a(V) := \{(b_2, b_3) | (a, b_2, b_3) \in V\}$.



(a) $a \in W_1$ (b) $a \in W_2$ (c) $a \in W_3$ (d) $a \in W_4$

The counting trees of the evaluations $\phi_a(V)$ are apparent from those pictures. ◁

2.5 Further properties of the counting polynomial

Now that we have the counting tree, we can prove a proposition that generalizes (2.3)2b).

Proposition 2.39. *Let $\mathcal{X}$ be a well-behaved class of enumerable sets. Let $m, n \in \mathbb{N}$ with $V \in \mathcal{X}^{m+n}$, $U \in \mathcal{X}^m$ such that $\pi_{m+n,m}(V) = U$ and*

$$c_{m+n}\left(\left(\pi_{m+n,m}\right)_{|V}^{-1}(\{v_1\})\right) = c_{m+n}\left(\left(\pi_{m+n,m}\right)_{|V}^{-1}(\{v_2\})\right)$$

for all $v_1, v_2 \in U$. Then

$$\begin{aligned} c_{m+n}(V) &= c_m(U)\, c_n\left((\alpha_{m+1}, \ldots, \alpha_{m+n})\left(\left(\pi_{m+n,m}\right)_{|V}^{-1}(\{v\})\right)\right) \\ &= c_m(U)\, c_{m+n}\left(\left(\pi_{m+n,m}\right)_{|V}^{-1}(\{v\})\right) \end{aligned}$$

for all $v \in U$.

Proof. First note that if $|\pi_{m+n,m}(V)| = 1$, then clearly $c_{m+n}(V) = c_n\left((\alpha_{m+1}, \ldots, \alpha_{m+n})(V)\right)$. Since $\pi_{m+n,m}\left(\left(\pi_{m+n,m}\right)_{|V}^{-1}(\{v\})\right) = \{v\}$, the last equality holds.

Now, assume that V is elementary (K, n)-enumerable. Then $c(V) = \prod_{i=1}^{m+n} \hat{c}\left(\pi_{m+n,i}(V)\right)$ with $\hat{c}$ as in Definition (2.29). Let $v \in U = \pi_{m+n,m}(V)$. The definition of elementary enumerable sets immediately implies that $c_{m+n}\left(\left(\pi_{m+n,m}\right)_{|V}^{-1}(\{v\})\right) = \prod_{i=m+1}^{m+n} \hat{c}\left(\pi_{m+n,i}(V)\right)$ for any $v \in V$. Since $c_m(U) = \prod_{i=1}^{m} \hat{c}\left(\pi_{m+n,i}(V)\right)$, the statement clearly holds for all elementary (K, n)-enumerable sets.

Now let $U = \biguplus_{i=1}^{k} U_i$ be a decomposition of U into elementary (K, m)-enumerable sets and $V = \biguplus_{i=1}^{k} \biguplus_{j=1}^{l_i} V_{i,j}$ a decomposition of V into elementary $(K, m+n)$-enumerable sets such that $\pi_{m+n,m}(V_{i,j}) = U_i$ for all $i = 1, \ldots, k, j = 1, \ldots, l_i$. Such a decomposition exists since, for example, any hereditarily disjoint decomposition fulfills this property. We get the counting polynomial as follows:

$$\begin{aligned} c_{m+n}(V) &= \sum_{i=1}^{k} \sum_{j=1}^{l_i} c_{m+n}(V_{i,j}) \\ &= \sum_{i=1}^{k} \sum_{j=1}^{l_i} c_m(U_i) c_{m+n}\left((\pi_{m+n,m})^{-1}_{|V_{i,j}} (\{v_{i,j}\}) \right) \\ &= \sum_{i=1}^{k} c_m(U_i) \sum_{j=1}^{l_i} c_{m+n}\left((\pi_{m+n,m})^{-1}_{|V_{i,j}} (\{u_i\}) \right) \end{aligned}$$

where $u_i \in U_i$ is arbitrary. Denote $V_i = \biguplus_{j=1}^{l_i} V_{i,j}$. Since

$$\left((\pi_{m+n,m})^{-1}_{|V_i} (\{u_i\}) \right) = \biguplus_{j=1}^{l_i} \left((\pi_{m+n,m})^{-1}_{|V_{i,j}} (\{u_i\}) \right)$$

holds, we also get

$$c_{m+n}(V) = \sum_{i=1}^{k} c_m(U_i) c_{m+n}\left((\pi_{m+n,m})^{-1}_{|V_i} (\{u_i\}) \right)$$

As there are no $v \in V \setminus V_i$ with $\pi_{m+n,m}(v) = u_i$, we further conclude

$$c_{m+n}(V) = \sum_{i=1}^{k} c_m(U_i) c_{m+n}\left((\pi_{m+n,m})^{-1}_{|V} (\{u_i\}) \right)$$

Since $c_{m+n}\left((\pi_{m+n,m})^{-1}_{|V} (\{w_1\}) \right) = c_{m+n}\left((\pi_{m+n,m})^{-1}_{|V} (\{w_2\}) \right)$ for all $w_1, w_2 \in U$ by assumption, we get

$$\begin{aligned} c_{m+n}(V) &= c_{m+n}\left((\pi_{m+n,m})^{-1}_{|V} (\{w\}) \right) \sum_{i=1}^{k} c_m(U_i) \\ &= c_{m+n}\left((\pi_{m+n,m})^{-1}_{|V} (\{w\}) \right) c_m(U) \end{aligned}$$

for any $w \in U$. □

In general, if κ is a bijection of K^n and $V, \kappa(V) \in \mathcal{X}^n$, the counting polynomials of V and $\kappa(V)$ may be different. One exception is when components are independent of each other.

Definition 2.40. The component α_n is called **independent** of α_{n-1} with respect to $V \in \mathcal{X}^n$ if for all $v \in \pi_{n-1}(\pi_n((V))$ and for all $w_1, w_2 \in (\pi_{n-1})^{-1}_{|\pi_n(V)} (\{v\})$, the following holds:

$$\alpha_n\left((\pi_n)^{-1}_{|V} (\{w_1\}) \right) = \alpha_n\left((\pi_n)^{-1}_{|V} (\{w_2\}) \right)$$ ◁

Remark 2.41. Let $V \in \mathcal{X}^n$ and consider the bijection

$$\kappa : K^n \to K^n : (a_1, \ldots, a_{n-2}, a_{n-1}, a_n) \mapsto (a_1, \ldots, a_{n-2}, a_n, a_{n-1}) \ .$$

If α_n is independent of α_{n-1} with respect to V, then $c_n(V) = c_n(\kappa(V))$. ◁

Proof. Define $(\beta_1, \ldots, \beta_n) := (\alpha_1, \ldots, \alpha_{n-2}, \alpha_n, \alpha_{n-1})$. If α_n is independent of α_{n-1}, then for v, w_1, w_2 as in definition (2.40), the following holds:

$$\alpha_n\left((\pi_n^\alpha)_{|V}^{-1}(\{w_1\})\right) = \alpha_n\left((\pi_n^\alpha)_{|V}^{-1}(\{w_2\})\right) = \beta_{n-1}\left(\left(\pi_{n-1}^\beta\right)_{|V}^{-1}(\{v\})\right)$$

Clearly, β_n is now independent of β_{n-1} and the statement follows. □

Remark 2.42. Let $\mathcal{X}$ be a well-behaved class of enumerable sets and $V \in \mathcal{X}^n$, $W \in \mathcal{X}^m$, as well as $V \times W \in \mathcal{X}^{n+m}$. Then $c_{n+m}(V \times W) = c_n(V)c_m(W)$. ◁

Proof. For all $v \in \pi_{m+n,n}(V \times W) = V$,

$$(\alpha_{n+1}, \ldots, \alpha_{n+m})\left((\pi_{m+n,n})_{|V}^{-1}(\{v\})\right) = W$$

and from Proposition (2.39), it follows that $c_{n+m}(f(V \times W)) = c_n(V)c_m(W)$. □

Chapter 3

Polynomial Systems

In this chapter, we analyze how polynomial systems give rise to enumerable sets. In particular, we will consider systems of polynomial equations and inequations over a fixed field. The concept of simple systems will help us to prove enumerability of their solution sets over an algebraically closed field and to compute their counting polynomials.

We will see that polynomial systems give rise to another well-behaved class of enumerable sets. We will give an algorithm that generalizes the use of the GAUSSian algorithm in Theorem (2.21) to general polynomial systems.

Let K be any field and denote by $\overline{K}$ any algebraically closed field extension of K. For example, for $K = \mathbb{Q}$, we can choose $\overline{K} = \overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, or $\overline{K} = \mathbb{C}$.

Remark 3.1. Let $V \subseteq \overline{K}^1$. If V is the $\overline{K}$-solution set of a polynomial equation or inequation in $K[x]$, then $V \in \mathcal{C}^1_{\overline{K}}$. If $V \in \mathcal{C}^1_{\overline{K}}$, then there is a finitely generated field extension $K \subseteq L \subseteq \overline{K}$ such that V is the solution set of a polynomial equation or inequation in $L[x]$. ◁

Proof.

"$\Longrightarrow$" A non-zero univariate polynomial has finitely many roots. Considered as an equation, it yields a finite solution set. Considered as an inequation, it yields all points in $\overline{K}^1$ with finitely many exceptions. The zero polynomial yields all of $\overline{K}^1$ if considered an equation, and the empty set if considered an inequation. The same holds for constant polynomials, with the roles of equations and inequations switched.

"$\Longleftarrow$" If $V = \emptyset$ or $V = \overline{K}^1$, then we can use a constant polynomial as an inequation or the zero polynomial as an equation, respectively. If V is a finite set, use the monic generator of the vanishing ideal of V in $\overline{K}[x]$ as an equation - clearly this generator is contained in a finitely generated extension of K. If V is infinite, consider the complement and use the monic generator of the vanishing ideal as an inequation. □

Example 3.2.

1. Let $p = x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$. Then the set $\{a \in \overline{\mathbb{Q}} | p(a) \neq 0\}$ is $V := \overline{\mathbb{Q}} \setminus \{i, -i\}$, where we consider $\overline{\mathbb{Q}}$ either as the algebraic closure of $\mathbb{Q}$ or as $\mathbb{C}$. The counting polynomial is given by
$$c(V) = c_1(V) = u - 2 \in \mathbb{Z}[u] .$$

2. Let $V := \{1, \sqrt{2}, -\sqrt{2}, \sqrt{3}\} \subseteq \mathbb{C}$. Then $V = \{a \in \overline{\mathbb{Q}} | q(a) \neq 0\}$ where $q = x^4 - \left(1 + \sqrt{3}\right) x^3 + \left(\sqrt{3} - 2\right) x^2 + 2\left(1 + \sqrt{3}\right) x - 2\sqrt{3} \in \mathbb{Q}\left[\sqrt{3}\right]$. ◁

Although all $(\overline{K}, 1)$-enumerable sets are given by univariate polynomials, the same is in general not true in higher dimensions. We will now consider sets that are defined as the solution sets of systems of multivariate polynomials.

Definition 3.3. Let K be a field and consider $p \in K[x_1, \ldots, x_n]$. We call $p_=$ the **equation** and $p_\neq$ the **inequation** defined by p. For $p_1, \ldots, p_r, q_1, \ldots, q_s \in K[x_1, \ldots, x_n]$, we call the set

$$S := \left\{(p_1)_=, \ldots, (p_r)_=, (q_1)_\neq, \ldots, (q_s)_\neq\right\}$$

a **polynomial system** over $K[x_1, \ldots, x_n]$. The **solution** operator $\mathcal{L}$ is defined as follows:

$$\mathcal{L}(S) := \left\{\mathbf{a} \in \overline{K}^n \middle| p_i(\mathbf{a}) = 0, 1 \leq i \leq r, q_j(\mathbf{a}) \neq 0, 1 \leq j \leq s\right\} \subseteq \overline{K}^n \qquad \triangleleft$$

The results in the one-dimensional case indicate that there is a relation between enumerable sets and polynomial systems. In the following, we will determine the exact relation between the two in the multivariate case.

3.1 Simple Systems

Simple systems form an analogon to elementary enumerable sets in the case of multivariate polynomial systems. In fact, their solution sets are elementary enumerable and we will show how to represent the solution set of each polynomial system as a disjoint union of such sets.

However, not all enumerable sets can be expressed using polynomials, as the following example shows:

Example 3.4. Consider the set $V = \left\{(x, 1) \in \mathbb{C}^2 \middle| x \in \mathbb{N}\right\} \cup \left\{(x, -1) \in \mathbb{C}^2 \middle| x \notin \mathbb{N}\right\}$ from Remark (2.7). As discussed earlier, this set is $(\mathbb{C}, 2)$-enumerable, but there is no polynomial system in $\mathbb{C}[x, y]$ that describes this set: If there were such a system, then by substituting $y = 1$ into all polynomials we would get a polynomial system in $\mathbb{C}[x]$ with solution set $\mathbb{N}$. Without loss of generality, we can assume that such a system would consist only of equations or only of inequations. As $\mathbb{C}[x]$ is a principal ideal domain, in both cases we can further assume that we only have a single equation or inequation, respectively. However, as both $\mathbb{N}$ and $\mathbb{C} \setminus \mathbb{N}$ are infinite, there is no polynomial that has either as its set of solutions. $\triangleleft$

Definition 3.5. Consider the polynomial ring $K[x_1, \ldots, x_n]$ and a polynomial $p \in K[x_1, \ldots, x_n]$.

1. A total order $<$ on $\{1, x_1, \ldots, x_n\}$ with $1 < x_i$ for all i is called a **ranking**. Unless stated otherwise, we always consider the ranking defined by $x_i < x_j$ if $i < j$.
2. The **leader** or **main variable** of p is the $<$-largest variable x_i such that $p \in K[x_1, \ldots, x_i] \setminus K[x_1, \ldots, x_{i-1}]$. We denote it by $\mathrm{ld}(p) = x_i$. For $p \in K$, we define $\mathrm{ld}(p) = 1$.
3. If $\mathrm{ld}(p) > 1$, the **main degree** of p, denoted by $\mathrm{mdeg}(p)$, is its degree in $\mathrm{ld}(p)$.
4. If $\mathrm{ld}(p) > 1$, the **initial** of p, denoted by $\mathrm{init}(p)$, is the coefficient of $\mathrm{ld}(p)^{\mathrm{mdeg}(p)}$ in p.

For an equation $p_=$ or an inequation $p_\neq$, define ld, mdeg and init as the respective properties of the underlying polynomial. For a set S of polynomials or equations and inequations, define $\mathrm{ld}(S)$ as the set of the leaders of all its elements. $\triangleleft$

Notation 3.6. For $\mathbf{a} \in K^n$, define the evaluation homomorphism

$$\phi_\mathbf{a} : K[x_1, \ldots, x_n] \to \overline{K} : x_i \mapsto \mathbf{a}_i \ .$$

For $\mathbf{a} \in \overline{K}^j$, $k - 1 \leq j \leq n$, define the partial evaluation homomorphism:

$$\phi_{<x_k, \mathbf{a}} : K[x_1, \ldots, x_n] \to \overline{K}[x_k, \ldots, x_n] : x_i \mapsto \begin{cases} \mathbf{a}_i, & i < k \\ x_i, & \text{otherwise} \end{cases}$$

Note that if $\mathrm{ld}(p) = x_k$, then $\phi_{<x_k, \mathbf{a}}(p) \in \overline{K}[x_k]$ is a univariate polynomial. $\triangleleft$

Notation 3.7. For a polynomial system S, denote by S_x the set of all terms with leader x. Denote by $S_{<x}$ the set of all terms with leader smaller than x, which we again consider a polynomial system. Finally, denote by $S^=$ and $S^\neq$ the set of all equations and inequations in S, respectively. ◁

Definition 3.8. A polynomial system S over $K[x_1, \ldots, x_n]$ is called **simple** if it fulfills the following properties:

1. S is **triangular**, i.e. $|S_{x_i}| \leq 1$ for all $1 \leq i \leq n$ and $S \cap \{c_=, c_\neq | c \in K\} = \emptyset$.
2. S has **non-vanishing initials**, i.e. $\phi_{\mathbf{a}}(\operatorname{init}(p)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x_i})$ and all $p \in S_{x_i}$, $1 < i \leq n$.
3. S is **square-free**, i.e. $\phi_{<x_i,\mathbf{a}}(p)$ is a square-free univariate polynomial in $\overline{K}[x_i]$ for all $\mathbf{a} \in \mathcal{L}(S_{<x_i})$ and all $p \in S_{x_i}$ for $1 \leq i \leq n$. ◁

For ease of notation, if a system S is triangular, we denote by S_x both the set and its unique element, if the set is non-empty.

Example 3.9. Consider the system $S_1 := \{p_=\} = \left\{(xy^2 + (x-1))_=\right\}$ over $K[x, y]$ with $x < y$. It is clearly triangular, but not simple.

The initial of p is x, but $0 \in \mathcal{L}\left((S_1)_{<y}\right) = \overline{K}$ is a root of x, thus S_1 does not have non-vanishing initials.

The system $S_2 := \{p_=, x_\neq\}$ has non-vanishing initials, but it is not square-free. The solution $1 \in \mathcal{L}\left((S_2)_{<y}\right) = \overline{K} \setminus \{0\}$ yields $\phi_{<y,(1)}(p) = y^2$ which is not square-free.

The final system $S_3 := \{p_=, (x(x-1))_\neq\}$ is simple. ◁

Remark 3.10. Every simple system has a solution. In particular, if $\mathbf{b} \in \mathcal{L}(S_{<x})$ and S_x is not empty, then $\phi_{<x,\mathbf{b}}(S_x)$ is a univariate polynomial with exactly $\operatorname{mdeg}(S_x)$ *distinct* roots. When S_x is an equation, each solution $\mathbf{b} \in \mathcal{L}(S_{<x})$ extends to a solution $(\mathbf{b}, a) \in \mathcal{L}(S_{\leq x})$ with $\operatorname{mdeg}(S_x)$ possible choices $a \in \overline{K}$. Otherwise, all but finitely many $a \in \overline{K}$ yield a solution $(\mathbf{b}, a) \in \mathcal{L}(S_{\leq x})$, because an inequation S_x excludes $\operatorname{mdeg}(S_x)$ different a, and $S_x = \emptyset$ imposes no restriction on a.

Conversely, if $(a_1, \ldots, a_n) \in \mathcal{L}(S)$ where S is a system over $K[x_1, \ldots, x_n]$ with $x_1 < \ldots < x_n$, then $(a_1, \ldots, a_i) \in \mathcal{L}(S_{\leq x_i})$. ◁

Corollary 3.11. *Let S be a simple system over $K[x_1, \ldots, x_n]$. Then $S_{<x_n}$ is a simple system and $\pi_n(\mathcal{L}(S)) = \mathcal{L}(S_{<x_n})$.*

Corollary 3.12. *Let S be a simple system over $K[x_1, \ldots, x_n]$. If $\mathbf{a} \in \mathcal{L}(S_{<x_i})$ then $\phi_{<x_i,\mathbf{a}}(S_{\geq x_i})$ is a simple system over $\overline{K}[x_i, \ldots, x_n]$ for all $1 \leq i \leq n$.*

Definition 3.13. A **family of polynomial systems** over the polynomial ring $K[x_1, \ldots, x_n]$ is a tuple $S = (S_1, \ldots, S_k)$ of polynomial systems for some $k \in \mathbb{N}$. The solution set of S is

$$\mathcal{L}(S) = \bigcup_{i=1}^{k} S_i$$

and the family is called **disjoint** if the union is disjoint, i.e. for any $i \neq j$, $\mathcal{L}(S_i) \cap \mathcal{L}(S_j) = \emptyset$. For two families $S = (S_1, \ldots, S_k)$ and $T = (T_1, \ldots, T_l)$, the family $(S, T) := (S_1, \ldots, S_k, T_1, \ldots, T_k)$ is called the **concatenation** of S and T.

A family of polynomial systems S is called **decomposition** of a system s if $\mathcal{L}(s) = \mathcal{L}(S)$. The decomposition is called disjoint if the family S is disjoint. A disjoint decomposition of a polynomial system into simple systems is called Thomas **decomposition**. ◁

We now aim to show that the solution set of each polynomial system over $K[x_1, \ldots, x_n]$ is $\left(\overline{K}, n\right)$-enumerable.

Definition 3.14. For every $n \geq 0$, define

$$\mathcal{P}^n := \mathcal{P}^n_K := \left\{ \bigcup_{i=1}^{k} \mathcal{L}(S_i) \middle| S_i \text{ is a polynomial system over } K[x_1, \ldots, x_n], i = 1, \ldots, k \right\} . \quad (3.1)$$

◁

Eventually, we want to show that $\mathcal{P} = \mathcal{P}_K$ is a well-behaved class of enumerable sets over $\overline{K}$, cf. Definition (2.10). According to Proposition (2.18), we need to show that conditions (2.10)2.-5 and 6'. hold. In addition, we need to show that we can disjointly decompose every set in $\mathcal{P}^n$ into elementary $\left(\overline{K}, n\right)$-enumerable sets in $\mathcal{P}^n$, i.e. that every set can be represented by a family of simple systems.

Lemma 3.15. *If every polynomial system can be disjointly decomposed into finitely many simple systems, then $\mathcal{P} = \mathcal{P}_K$ is a well-behaved class of enumerable sets over $\overline{K}$.*

Proof. First note that (2.10)4. holds by definition of $\mathcal{P}^n$. Since for $S_1, S_2 \in \mathcal{P}^n$, $\mathcal{L}(S_1) \cap \mathcal{L}(S_2) = \mathcal{L}(S_1 \cup S_2)$, it holds that $\mathcal{P}^n$ also closed under intersection. To prove (2.10)3., first note that $\overline{K}^n \setminus \bigcup_{i=1}^{k} \mathcal{L}(S_i) = \bigcap \overline{K}^n \setminus \mathcal{L}(S_i)$, thus it suffices to show that for a single polynomial system S, the complement of $\mathcal{L}(S)$ is in $\mathcal{P}^n$. The following holds:

$$\begin{aligned}
\overline{K}^n \setminus \mathcal{L}(S) &= \overline{K}^n \setminus \left(\bigcap_{j=1}^{l} \mathcal{L}(\{(p_i)_=\}) \cap \bigcap_{j=1}^{m} \mathcal{L}(\left\{(q_i)_{\neq}\right\}) \right) \\
&= \bigcup_{i=1}^{l} \overline{K}^n \setminus \mathcal{L}(\{(p_i)_=\}) \cup \bigcup_{i=1}^{m} \overline{K}^n \setminus \mathcal{L}(\left\{(q_i)_{\neq}\right\}) \\
&= \bigcup_{i=1}^{l} \mathcal{L}(\left\{(p_i)_{\neq}\right\}) \cup \bigcup_{i=1}^{m} \mathcal{L}(\{(q_i)_=\}) ,
\end{aligned}$$

This is a union of finitely many polynomial systems, implying (2.10)3.

For (2.10)5., note that a polynomial system T over $K[x_1, \ldots, x_m]$ can also be interpreted as a polynomial system T' over $K[x_1, \ldots, x_n]$, such that $\mathcal{L}(T) \times K^{n-m} = \mathcal{L}(T')$. As $\mathcal{P}^n$ is closed under intersection, property (2.10)5. follows.

For any polynomial system S over $K[x_1, \ldots, x_n]$ and any $(a_1, \ldots, a_m) \in \overline{K}^m$, $S_{|x_1=a_1,\ldots,x_m=x_m}$ is a polynomial system over $\overline{K}[x_{m+1}, \ldots, x_n]$. If K is algebraically closed, that implies condition (2.10)6. Otherwise, it implies (2.10)6'. if $\mathcal{P}_{\overline{K}}$ is a strongly well-behaved class of enumerable sets over $\overline{K}$.

Using the same arguments as in Theorem (2.21), we can without loss of generality assume that the union in (3.1) is disjoint.

Now assume that for every polynomial system over $K[x_1, \ldots, x_n]$, there is a disjoint decomposition into simple systems over $K[x_1, \ldots, x_n]$, i.e. $\mathcal{L}(S) = \biguplus_{i=1}^{k} \mathcal{L}(S_i)$ where every $\mathcal{L}(S_i)$ is elementary (K, n)-enumerable. Under this assumption, we can write every set in $\mathcal{P}^n_K$ as a disjoint union of solution sets of simple systems over $K[x_1, \ldots, x_n]$. Since $\pi_n(\mathcal{L}(S)) = \pi_n(\biguplus_{i=1}^{k} \mathcal{L}(S_i)) = \bigcup_{i=1}^{k} \pi_n(\mathcal{L}(S_i)) = \bigcup_{i=1}^{k} \mathcal{L}((S_i)_{<x_n})$, it follows that $\pi_n(\mathcal{L}(S)) \in \mathcal{P}^{n-1}_K$ and thus (2.10)2. holds.

In summary, this means that $\mathcal{P}^n_K$ is a strongly well-behaved class of enumerable sets over K if K is algebraically closed. As a consequence, for a not necessarily algebraically closed field K, $\mathcal{P}^n_K$ is a well-behaved class of enumerable sets over $\overline{K}$. □

All that remains to be shown is that for every polynomial system over $K[x_1, \ldots, x_n]$, there is a disjoint decomposition into simple polynomial systems over $K[x_1, \ldots, x_n]$. The following sections will concern themselves with this topic.

Before we consider the decomposition algorithm, we reconsider counting polynomials. If $\mathcal{P}_K$ is a well-behaved class of enumerable sets, there is a well-defined map $c_n : \mathcal{P}^n_K \to \mathbb{Z}[u]$ that gives the counting polynomial. We demonstrate how simple systems can be used to determine that counting polynomial. To simplify notation, for a polynomial system S, we define $c(S) := c(\mathcal{L}(S))$.

Theorem 3.16. *For every simple system S over $K[x_1, \ldots, x_n]$, $\mathcal{L}(S)$ is elementary $\left(\overline{K}, n\right)$-enumerable with counting polynomial*

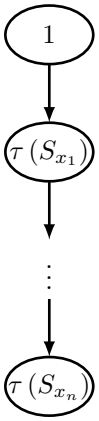
$$c(S) = \prod_{i=1}^{n} \tau\left(S_{x_i}\right) \in \mathbb{Z}[u]$$

where

$$\tau\left(S_{x_i}\right) = \begin{cases} \operatorname{mdeg}\left(S_{x_i}\right), & \text{if } S_{x_i} \text{ is an equation} \\ u - \operatorname{mdeg}\left(S_{x_i}\right), & \text{if } S_{x_i} \text{ is an inequation} \\ u, & \text{if } S_{x_i} \text{ is empty} \end{cases}$$

Proof. Consider i such that $S_{x_i} \neq \emptyset$. Then, since S is simple, $\phi_{<x_i,\mathbf{a}}(S_{x_i}) \in \overline{K}[x_i]$ is a polynomial of degree $d := \operatorname{mdeg}(S_{x_i})$ for all $\mathbf{a} \in \mathcal{L}(S_{<x_i})$. Since $\overline{K}$ is algebraically closed, $\phi_{<x_i,\mathbf{a}}(S_{x_i})$ has exactly d distinct roots. Therefore, $\mathcal{L}(S)$ is elementary $\left(\overline{K}, n\right)$-enumerable. Due to Definitions (2.8) and (2.12)1., the statement follows. □

Another way to see this is by looking at the counting tree.



3.2 Algebraic Thomas Decomposition

This section presents our main algorithm for decomposing polynomial systems and its subalgorithms. The termination and correctness of this algorithm will be proven, which proves the existence of a disjoint decomposition of a polynomial system into simple systems. Most of this section is joint work that has been published in [BGLHR12].

Note that some subalgorithms do not apply if the characteristic of K is non-zero. For that case, we will add the missing pieces in section 3.3.

For shorter notation, we fix $n \in \mathbb{N}$ and define $R := K[x_1, \ldots, x_n]$ where K is an arbitrary field. For a fixed variable y, we denote by $R_{<y}$ and $R_{\leq y}$ the polynomials in R with leader smaller than y and smaller or equal than y, respectively.

3.2.1 J.M. Thomas' original decomposition method

The American mathematician Joseph Miller Thomas was the first to describe a method to decompose a polynomial system into simple systems in 1937, cf. [Tho37]. While his approach certainly yields a correct decomposition after finitely many steps, his description is imprecise and the method is often infeasible. However, his method is rather simple to explain and gives a good idea of what steps are needed.

One of his first observations states that for any polynomial system S over R and any $p \in R$, $\mathcal{L}(S) = \mathcal{L}(S \cup \{p_{\neq}\}) \uplus \mathcal{L}(S \cup \{p_{=}\})$, allowing to use arbitrary polynomials to construct disjoint decompositions of S. Let $1 \leq k \leq n$. For every equation $p_{=} \in S_{x_k}$, it holds that

$$\mathcal{L}(S) = \mathcal{L}(S \cup \{\text{init}(p)_{\neq}\}) \uplus \mathcal{L}\left((S \setminus \{p_{=}\}) \cup \left\{\text{init}(p)_{=}, \left(p - \text{init}(p)\, x_k^{\text{mdeg}(p)}\right)_{=}\right\}\right)$$

and analogously

$$\mathcal{L}(S) = \mathcal{L}(S \cup \{\text{init}(p)_{\neq}\}) \uplus \mathcal{L}\left((S \setminus \{p_{\neq}\}) \cup \left\{\text{init}(p)_{=}, \left(p - \text{init}(p)\, x_k^{\text{mdeg}(p)}\right)_{\neq}\right\}\right)$$

for any inequation $p_{\neq} \in S_{x_k}$. For both cases, this defines a decomposition into two systems. Setting the right-hand side system in this decomposition aside for the moment and iterating this process for the left-hand side system, we obtain a new system T that contains every initial of an element of T_{x_k} as an inequation.

For every equation $p_{=} \in T_{x_k}$ or inequation $p_{\neq} \in T_{x_k}$, let $D_0(p)$ be its discriminant and $D_i(p)$ be the leading coefficient of its i-th subdiscriminant with respect to x_k for $i > 0$ (cf. section 3.2.6). Determine a number d such that $D_0(p), D_1(p), \ldots, D_{d-1}(p)$ are either 0 or "obviously implied as equations" by $T_{<x_k}$ and $D_d = D_d(p) \neq 0$. It is possible to find polynomials F, f_1, f_2 such that $\phi_{<x_k,\mathbf{a}}(D_d^2 p) = \phi_{<x_k,\mathbf{a}}(F f_1)$, $\phi_{<x_k,\mathbf{a}}(D_d^2 p') = \phi_{<x_k,\mathbf{a}}(F f_2)$ and $\phi_{<x_k,\mathbf{a}}(D_0(f_1)) \neq 0$ for any $\mathbf{a} \in \mathcal{L}(S_{<x_k} \cup \{(D_d)_{\neq}\})$. We will discuss how to determine such polynomials in section 3.2.6. We get a decomposition of T such that

$$\mathcal{L}(T) = \mathcal{L}((T \setminus \{p_{=}\}) \cup \{(f_1)_{=}, (D_d)_{\neq}\}) \uplus \mathcal{L}(T \cup \{(D_d)_{=}\})$$

in the equation case and

$$\mathcal{L}(T) = \mathcal{L}((T \setminus \{p_{\neq}\}) \cup \{(f_1)_{\neq}, (D_d)_{\neq}\}) \uplus \mathcal{L}(T \cup \{(D_d)_{=}\})$$

in the inequation case. Again, iterating the process with the left-hand side of the decomposition yields a system U such that $\phi_{<x_k,\mathbf{a}}(D_0(p)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(U_{<x_k})$ and all $p \in U_{x_k}$.

If there is no equation in U_{x_k}, multiply all inequations in U_{x_k} and remove common factors using the method demonstrated in the previous paragraph. Otherwise, choose an equation $p_{=} \in U_{x_k}$ and a polynomial $q \neq p$ with either $q_{=} \in U_{x_k}$ or $q_{\neq} \in U_{x_k}$. Let $R_0(p,q)$ be the resultant and $R_i(p,q)$ the leading coefficient of the i-th subresultant with respect to x_k for $i > 0$ (cf. section 3.2.6). Find d such that $R_0(p,q), R_1(p,q), R_{d-1}(p,q)$ are either 0 or "obviously implied as equations" by $U_{<x_k}$ and $R_d = R_d(p,q) \neq 0$. Similarly as before, there are polynomials f_1, g_1, φ such that $\phi_{<x_k,\mathbf{a}}(R_d^2 p) = \phi_{<x_k,\mathbf{a}}(\varphi f_1)$, $\phi_{<x_k,\mathbf{a}}(R_d^2 q) = \phi_{<x_k,\mathbf{a}}(\varphi g_1)$ and $\phi_{<x_k,\mathbf{a}}(f_1), \phi_{<x_k,\mathbf{a}}(g_1), \phi_{<x_k,\mathbf{a}}(\varphi)$ are coprime for all $\mathbf{a} \in \mathcal{L}(U_{<x_k} \cup \{(R_d)_{\neq}\})$. Now consider the decomposition

$$\mathcal{L}(U) = \mathcal{L}(T \cup \{(R_d)_{\neq}\}) \uplus \mathcal{L}(T \cup \{(R_d)_{=}\}) \ .$$

Thomas distinguishes two cases:

In the case $d = 0$, for any solution $\mathbf{a} \in \mathcal{L}(T \cup \{(R_d)_{\neq}\})$, $\gcd(\phi_{<x_k,\mathbf{a}}(p), \phi_{<x_k,\mathbf{a}}(q)) = 1$ and $\frac{\phi_{<x_k,\mathbf{a}}(p)}{\gcd(\phi_{<x_k,\mathbf{a}}(p), \phi_{<x_k,\mathbf{a}}(q))} = \phi_{<x_k,\mathbf{a}}(p)$. Therefore, if $q_{=}$ is an equation, $p_{=}$ and $q_{=}$ can be replaced by $1_{=}$, resulting in an inconsistency. If $q_{\neq}$ is an inequation, it can be omitted from the system.

If $d > 0$, then $\gcd(\phi_{<x_k,\mathbf{a}}(p), \phi_{<x_k,\mathbf{a}}(q)) = \phi_{<x_k,\mathbf{a}}(\varphi)$ and $\frac{\phi_{<x_k,\mathbf{a}}(p)}{\gcd(\phi_{<x_k,\mathbf{a}}(p), \phi_{<x_k,\mathbf{a}}(q))} = \phi_{<x_k,\mathbf{a}}(f_1)$. If $q_{=}$ is an equation, $p_{=}$ and $q_{=}$ can be replaced by $\varphi_{=}$. If $q_{\neq}$ is an inequation, $p_{=}$ and $q_{\neq}$ can be replaced by $(f_1)_{=}$.

As before, iterating this process with the left-hand side of the decomposition yields a system V with $|V_{x_k}| \leq 1$. If we start with $k = n$ and complete this whole process, then continue with $k = n - 1$ and so on, until $k = 1$, we finally get a simple system V, as well as a number of "unfinished" systems. If we subject each of the unfinished systems to the same treatment, after finitely many steps, we obtain a decomposition into simple systems.

This description, first published in [Tho37, pg. 59-61], is imprecise in many aspects, most importantly the following: The method may add add $c_=$ or $c_\neq$ to a system for $c \in K$. If $0_=$ or $c_\neq, c \neq 0$ are added, they can be immediately omitted, since they have no consequence on the solution set. However, when $c_=, c \neq 0$ or $0_\neq$ are added, the entire system becomes inconsistent.

In particular, when considering two equations $p_=, q_=$ of the same leader with $R(p,q) \neq 0$, the instructions explicitly state to add $R_0(p,q)_\neq$, which implies that $1_=$ must be added, too. This yields an inconsistent and thus non-simple system, contradicting the statement that following the left-hand side of the decomposition always yields a simple system.

Despite being theoretically possible, this method is computationally infeasible for most examples, since it has no way of detecting inconsistencies in a system as they occur. In several places, Thomas instructs to check whether a polynomial is "obviously implied as an equation" by the system, yet he offers no method to perform this test. In fact, at this stage, the polynomial systems are so chaotic and unstructured that such a test seems impossible, unless the equation in question is already contained in the system. This leaves no other choice than to assume that the equation is not implied by the system and risk performing lengthy computations and further decompositions on an inconsistent system.

Dongming Wang presented and implemented an algorithm based on Thomas' method (cf. [Wan98]), but improved it significantly. His implementation uses MAPLE, but only works with MAPLE 7 and 8, but not any newer versions.

We devised a new algorithm that addresses the shortcomings of Thomas' method and implemented it in MAPLE. We introduce a reduction method (cf. section 3.2.3), that allows simplifying polynomials modulo a (not necessarily simple) system that occurs in the course of the computation. Instead of ensuring simplicity of the system for the higher variables first, we start with the lowest variable, thus allowing to use reduction to simplify polynomials. In particular, this approach makes it possible to test whether an equation is already implied by the system, preventing the creation of inconsistent branches in most cases.

Our approach combines ideas used in other triangular decomposition algorithms (cf. for example [MM99]) with the strict requirements for the THOMAS decomposition.

3.2.2 Preliminaries

The decomposition algorithm represents each system as a pair consisting of a candidate simple system and a queue of unprocessed equations and inequations. In each step, the algorithm chooses a suitable polynomial from the queue, pseudo-reduces it and afterwards combines it with the polynomial from the candidate simple system having the same leader. In this process, the algorithm may split the system, i.e., add a new polynomial into the queue as an inequation and at the same time create a new subsystem with the same polynomial added to the queue as an equation. This way, we ensure that no solutions are lost and the solution sets are disjoint. The algorithm considers a system inconsistent and discards it when an equation of the form $c_=$ with $c \in K \setminus \{0\}$ or the inequation $0_\neq$ is produced.

We consider a system S as a pair of sets (S_T, S_Q), where S_T represents the candidate simple system and S_Q is the queue. We require S_T to be triangular and thus $(S_T)_x$ denotes the unique equation or inequation of leader x in S_T. We say that $(S_T)_x$ is empty if no such equation or inequation exists. Moreover, S_T must fulfill a weaker form of the other two simplicity conditions, in particular, in conditions (3.8)(2) and (3), the tuple $\mathbf{a}$ can be a solution of $(S_T)_{<x} \cup (S_Q)_{<x}$ instead of just $(S_T)_{<x}$. Obviously, $S_Q = \emptyset$ implies simplicity of S.

We denote the set of these systems by $\mathcal{S}$. For $S \in \mathcal{S}$, we define $S_{<x} = (S_T)_{<x} \cup (S_Q)_{<x}$ and analogously S_x, $S_{\leq x}$, $S^=$, $S^\neq$ and so on. The solutions of S are given by $\mathcal{L}(S) = \mathcal{L}(S_T \cup S_Q)$.

3.2.3 Reduction

This section introduces our reduction algorithm. It utilizes the triangular structure of a system and thus can only respect the candidate simple system S_T of a system S.

From now on, let prem be a **pseudo remainder algorithm**[1] in R and pquo the corresponding **pseudo quotient algorithm**. To be precise, if $p, q \in R$ with $\mathrm{ld}(p) = \mathrm{ld}(q) = x$, then

$$m \cdot p = \mathsf{pquo}(p, q, x) \cdot q + \mathsf{prem}(p, q, x) \tag{3.2}$$

holds, where $\deg_x(q) > \deg_x(\mathsf{prem}(p, q, x))$, $\mathrm{ld}(m) < x$ and $m \mid \mathrm{init}(q)^k$ for some $k \in \mathbb{Z}_{\geq 0}$. Note that for any $\mathbf{a} \in \overline{K}^n$, $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ and $\phi_{\mathbf{a}}(\mathrm{init}(q)) \neq 0$ imply $\phi_{\mathbf{a}}(\mathrm{lcoeff}(\mathsf{pquo}(p, q, x), x)) \neq 0$ and $\phi_{\mathbf{a}}(m) \neq 0$.

The following algorithm employs prem to define a function that **reduces** a polynomial modulo S_T:

Algorithm 3.17 (Reduce)**.**
Input: A system S, a polynomial $p \in R$.
Output: A polynomial $q \in R$ that fulfills the properties of Proposition (3.18), Remark (3.19), Corollary (3.20) and Remark (3.21).
Algorithm:

1: $x \leftarrow \mathrm{ld}(p)$; $q \leftarrow p$
2: ***while*** $x > 1$, $(S_T)_x$ *is an equation and* $\mathrm{mdeg}(q) \geq \mathrm{mdeg}((S_T)_x)$ ***do***
3: $\quad q \leftarrow \mathsf{prem}(q, (S_T)_x, x)$
4: $\quad x \leftarrow \mathrm{ld}(q)$
5: ***end while***
6: ***if*** $x > 1$ *and* $\mathsf{Reduce}(S, \mathrm{init}(q)) = 0$ ***then***
7: $\quad$ ***return*** $\mathsf{Reduce}(S, q - \mathrm{init}(q) x^{\mathrm{mdeg}(q)})$
8: ***else***
9: $\quad$ ***return*** q
10: ***end if***

The most important property of Reduce is that it does not change the common solutions of the polynomial and the system. This is a consequence of the special treatment that the initial gets in the Reduce algorithm, lines 6–7.

Proposition 3.18. *If $q = \mathsf{Reduce}(S, p)$ then $\phi_{\mathbf{a}}(p) = 0$ if and only if $\phi_{\mathbf{a}}(q) = 0$ for every $\mathbf{a} \in \mathcal{L}(S)$.*

Proof. There exist $m \in R \setminus \{0\}$ with $\mathrm{ld}(m) < \mathrm{ld}(p)$ and $\phi_{\mathbf{a}}(m) \neq 0$ for all $\mathbf{a} \in \mathcal{L}\left(S_{\leq \mathrm{ld}(p)}\right)$ such that

$$\mathsf{Reduce}(S, p) = mp - \sum_{y \leq \mathrm{ld}(p)} c_y \cdot (S_T)_y$$

with $c_y \in R$ and $\mathrm{ld}(c_y) \leq \mathrm{ld}(p)$ if $(S_T)_y$ is an equation and $c_y = 0$ otherwise. This implies

$$\phi_{\mathbf{a}}(\mathsf{Reduce}(S, p)) = \underbrace{\phi_{\mathbf{a}}(m)}_{\neq 0} \phi_{\mathbf{a}}(p) - \sum_{y \leq x} \phi_{\mathbf{a}}(c_y) \underbrace{\phi_{\mathbf{a}}((S_T)_y)}_{=0}$$

and therefore $\phi_{\mathbf{a}}(p) = 0$ if and only if $\phi_{\mathbf{a}}(\mathsf{Reduce}(S, p)) = 0$. □

Note that this algorithm only uses the equation part of the triangular system in S, i.e. $S_T^{=}$.

We say that a polynomial p **reduces to** q **modulo** S_T if $\mathsf{Reduce}(S, p) = q$. A polynomial is **reduced modulo** S_T if it reduces to itself.

Later, we will use the following facts about the Reduce algorithm.

Remark 3.19. Let $q = \mathsf{Reduce}(S, p) \neq 0$.

1. If $\mathrm{ld}(q) > 1$ and $S_{\mathrm{ld}(q)}$ is an equation, then $\mathrm{mdeg}(q) < \mathrm{mdeg}(S_{\mathrm{ld}(q)})$.
2. If $\mathrm{ld}(q) > 1$, then $\mathsf{Reduce}(S, \mathrm{init}(q)) \neq 0$.

[1] In our context prem does not necessarily have to be the classical pseudo remainder, but any sparse pseudo remainder with property (3.2) will suffice.

3. $\mathrm{ld}(q) \leq \mathrm{ld}(p)$ and if $\mathrm{ld}(q) = \mathrm{ld}(p) > 1$, then $\mathrm{mdeg}(q) \leq \mathrm{mdeg}(p)$. ◁

The result of the Reduce algorithm does not need to be a canonical normal form, however, the algorithm recognizes polynomials that vanish on all solutions.

Corollary 3.20. *Let $p \in R$ with $\mathrm{ld}(p) = x$. $\mathsf{Reduce}(S, p) = 0$ implies $\phi_{\mathbf{a}}(p) = 0 \ \forall\ \mathbf{a} \in \mathcal{L}(S_{\leq x})$.*

Proof. For all $\mathbf{a} \in \mathcal{L}(S_{\leq x})$, it holds that $\phi_{\mathbf{a}}(p) = 0$ if and only if $\phi_{\mathbf{a}}(\mathsf{Reduce}(S, p)) = 0$. The statement follows from $\phi_{\mathbf{a}}(\mathsf{Reduce}(S, p)) = \phi_{\mathbf{a}}(0) = 0$. □

The converse of this corollary does not hold in general. Thus, we provide two weaker statements in the following remark.

Remark 3.21. Let p and x as in Corollary (3.20).

1. If $(S_Q)_{\leq x} = \emptyset$, i.e., $S_{\leq x} = (S_T)_{\leq x}$ is simple, then $\mathsf{Reduce}(S, p) \neq 0$ implies that there exists $\mathbf{a} \in \mathcal{L}(S_{\leq x})$ such that $\phi_{\mathbf{a}}(p) \neq 0$.
2. If $(S_Q)^{=}_{<x} = \emptyset$ and $\mathsf{Reduce}(S, p) \neq 0$ hold, then either $\mathcal{L}(S_{<x}) = \emptyset$ or there exists $\mathbf{a} \in \mathcal{L}(S_{<x} \cup \{(S_T)_x\})$ such that $\phi_{\mathbf{a}}(p) \neq 0$. ◁

Proof. We only prove the second part, as the first part easily follows.

Let $(S_Q)^{=}_{<x} = \emptyset$, $\mathsf{Reduce}(S, p) \neq 0$ and $|\mathcal{L}(S_{<x})| > 0$. As $\mathrm{ld}((S_T)_x) = x$ and $\mathrm{mdeg}((S_T)_x) > 0$, for each $\mathbf{a} \in \mathcal{L}(S_{<x})$, the univariate polynomial $\phi_{<x,\mathbf{a}}((S_T)_x) \in \overline{K}[x]$ has positive degree. Thus $|\mathcal{L}(S_{<x} \cup \{(S_T)_x\})| > 0$.

Let $\phi_{\mathbf{a}}(p) = 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x} \cup \{(S_T)_x\})$ (*). Then $(S_T)_x$ is an equation and $\deg_x(p) \geq \deg_x((S_T)_x)$ and therefore $p \neq \mathsf{Reduce}(S, p)$. In fact, (*) further implies $\mathrm{ld}(\mathsf{Reduce}(S, p)) < x$, as otherwise $\deg_x(\mathsf{Reduce}(S, p)) \geq \deg_x((S_T)_x)$ would hold. By repeating the previous arguments, we can inductively conclude $\mathrm{ld}(\mathsf{Reduce}(S, p)) = 1$. As $\phi_{\mathbf{a}}(p) = 0$, we conclude $\mathsf{Reduce}(S, p) = 0$, a contradiction. □

The first part of this remark in conjunction with Corollary (3.20) implies [Wan98, Thm. 4].

Each reduction can be followed by a coefficient reduction. The most prominent example is the full coefficient reduction.

Algorithm 3.22 (FullCoeffReduce)**.**
Input: A system S, a polynomial $p \in R$ that is reduced modulo S_T.
Output: A polynomial q such that

1. *q is reduced modulo S_T.*
2. *$\phi_{\mathbf{a}}(p) = 0$ if and only if $\phi_{\mathbf{a}}(q) = 0$ for each $\mathbf{a} \in \mathcal{L}(S)$.*
3. *$\deg_y(q) < \mathrm{mdeg}\left((S_T)_y\right)$ for all y such that $(S_T)_y$ is an equation.*

Algorithm:

```
q ← p
y ← max(z | z < ld(p) and (S_T)_z is an equation)
while y > 1 do
    q ← prem(q, (S_T)_y, y)
    y ← max(z | z < y and (S_T)_z is an equation)
end while
```

Proof of Correctness. Let $x = \mathrm{ld}(p)$, $y < x$ such that $(S_T)_y$ is an equation and

$$\mathsf{prem}\left(\mathrm{coeff}\left(q, x^i\right), (S_T)_y, y\right) = m_i \cdot \mathrm{coeff}\left(q, x^i\right) - c_i \cdot (S_T)_y$$

where $\mathrm{ld}(m_i) < y$ and $\mathrm{ld}(c_i) \leq y$, $i = 1, \ldots, \mathrm{mdeg}(p)$. Then, with $m = \mathrm{lcm}\left(m_i | i = 0, \ldots, \mathrm{mdeg}(p)\right)$,

$$\mathsf{prem}(q, (S_T)_y, y) = m \cdot q - \sum_{i=0}^{\mathrm{mdeg}(p)} \frac{m}{m_i} c_i \cdot (S_T)_y \cdot x^i$$

This shows that $\phi_{\mathbf{a}}(\mathsf{prem}(q, (S_T)_y, y)) = \phi_{\mathbf{a}}(q)$ for all $\mathbf{a} \in \mathcal{L}(S)$.

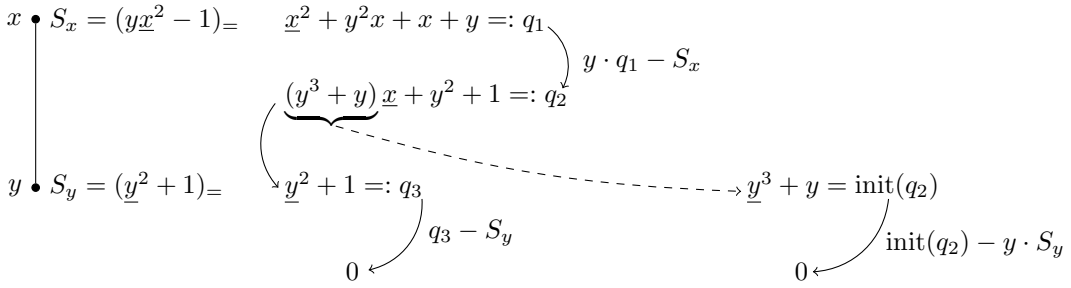
As S_T is triangular, this also shows that a prem reduction with a polynomial with leader y only changes variables smaller or equal y in the coefficients of p with respect to x. Therefore, the main degree remains constant during the computation and $\mathsf{prem}(q, (S_T)_y, y)$ remains reduced modulo S_T if q was reduced modulo S_T.

Finally, by construction $\deg_y(\mathsf{prem}(q, (S_T)_y, y)) < \mathrm{mdeg}((S_T)_y)$. □

We call a polynomial **fully coefficient-reduced modulo** S_T if $p = \mathsf{FullCoeffReduce}(S, p)$.

The Reduce algorithm differs slightly from the classical $\mathsf{prem}(p, S_T^=)$ as defined in [ALMM99]. While $\mathsf{prem}(p, S_T^=)$ fully reduces p modulo all variables, $\mathsf{Reduce}(S, p)$ only reduces modulo the leader and ensures that the initial of the reduced form does not vanish. Performing $\mathsf{Reduce}(S, p)$ in combination with full coefficient reduction is the same as computing $\mathsf{prem}(p, S_T^=)$. It is therefore possible to replace $\mathsf{Reduce}(S, p)$ with $\mathsf{prem}(p, S_T^=)$ in the following algorithms. Our approach adds some flexibility, as we can choose to omit a full coefficient reduction in an implementation. In particular, if a polynomial does not reduce to zero, we can determine that without performing a full prem reduction. We apply this multiple times in our implementation, most prominently in Algorithm (3.40). However, if a polynomial reduces to zero, Reduce has no advantage over prem.

Example 3.23. Reduce $q_1 := x^2 + y^2x + x + y$ modulo the simple system on the left.



In the first reduction step, q_1 is pseudo-reduced modulo S_x. The result q_2 still has leader x, but a main degree smaller than S_x. We determine that the initial of q_2 reduces to 0 and remove the highest power of x from q_2. The resulting polynomial q_3 now pseudo-reduces to 0 modulo S_y, i.e. $\mathsf{Reduce}(\{S_x, S_y\}, q_1) = 0$. ◁

3.2.4 Canonical Form of a Simple System

This section shortly demonstrates how to use reduction to define and compute a canonical form of a simple system. While the procedures presented here are not needed for the decomposition algorithm, we will need the general ideas in later chapters. We start by defining a canonical form of a polynomial modulo a simple system.

Algorithm 3.24 ($\mathsf{Canonicalize}$)**.**
Input: A system S and a polynomial $p \in R$ with $x = \mathrm{ld}(p)$, such that $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$ and $(S_Q)_{<x} = \emptyset$, i.e. $S_{<x} = (S_T)_{<x}$ is simple
Output: A polynomial q such that

1. *$\phi_{\mathbf{a}}(p) = 0$ if and only if $\phi_{\mathbf{a}}(q) = 0$ for every $\mathbf{a} \in \mathcal{L}(S)$.*
2. *q is reduced and fully coefficient-reduced modulo S_T.*
3. *if $S_y = (S_T)_y$ is an equation, then $\deg_y(\mathrm{init}(q)) = 0$ for all $y < \mathrm{ld}(q)$.*

Algorithm: Let $R_{U,\leq y} := K\,[z | z \leq y$ or $(S_T)_z^= = \emptyset]$ and analogously $R_{U,<y}$.

1: $q \leftarrow \mathsf{Reduce}(S, p)$
2: $y \leftarrow \max\,(z | z < x$ *and* $(S_T)_z$ *is an equation)*
3: ***while*** $y > 1$ ***do***
4: $\quad q \leftarrow \mathsf{prem}\,(q, (S_T)_y, y)$

5: ***if*** $\deg_y(\mathrm{init}(q)) > 0$ ***then***
6: *Compute* $a, b \in R_{U,\leq y} \setminus \{0\}$ *such that* $a \cdot \mathrm{init}(q) + b \cdot (S_T)_y \in R_{U,<y}$
7: $q \leftarrow \mathsf{prem}\,(a \cdot q, (S_T)_y, y)$
8: ***end if***
9: $y \leftarrow \max\,(z | z < y$ *and* $(S_T)_z$ *is an equation*$)$
10: ***end while***

Proof of Correctness. Consider line 6. Assume that $(S_T)_y$ is an equation and $\mathrm{init}(q) \in R_{U,\leq y}$ with $\phi_{\mathbf{a}}(\mathrm{init}(q)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$. Then a refined version of the extended Euclidean algorithm in gives us $a, b \in R_{U,\leq y}$ such that

$$a \cdot \mathrm{init}(q) + b \cdot (S_T)_y = r := \mathrm{res}(\mathrm{init}(q), (S_T)_y, y) \in R_{U,<y}\ .$$

Since $\phi_{\mathbf{a}}((S_T)_y) = 0$ and $\phi_{\mathbf{a}}(\mathrm{init}(q)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$, it holds that $\phi_{<y,\mathbf{a}}((S_T)_y)$ and $\phi_{<y,\mathbf{a}}(\mathrm{init}(q))$ have no common divisor in $\overline{K}[y]$ and therefore $\phi_{\mathbf{a}}(r) \neq 0$. This implies

$$0 \neq \phi_{\mathbf{a}}(r) = \phi_{\mathbf{a}}(a \cdot \mathrm{init}(q) + b \cdot (S_T)_y) = \phi_{\mathbf{a}}(a) \cdot \phi_{\mathbf{a}}(\mathrm{init}(q))$$

and thus $\phi_{\mathbf{a}}(a) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$. By definition of prem, there is an m with $\phi_{\mathbf{a}}(m) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$ such that

$$\mathsf{prem}(a \cdot \mathrm{init}(q), (S_T)_y, y) = m \cdot (a \cdot \mathrm{init}(q) + b \cdot (S_T)_y) \in R_{U,<y}\ .$$

Define $\tilde{q} := \mathsf{prem}\,(a \cdot q, (S_T)_y, y)$. With the same argument as in the proof of Algorithm (3.22),

$$\deg_y\left(\mathrm{init}\left(\tilde{q}\right)\right) = 0\ .$$

This implies further that $\mathrm{init}(\tilde{q}) \in R_{U,<y}$ and that $\phi_{\mathbf{a}}(\mathrm{init}(\tilde{q})) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$. By induction and by the the same arguments as in the proof of Algorithm (3.22), this shows correctness. □

We say that a polynomial p is **canonicalized** modulo S if $\mathsf{Canonicalize}(S, p) = p$.

Remark 3.25. Let S be a simple system and $p, q \in R$ reduced modulo S such that $\mathrm{ld}(p) = \mathrm{ld}(q) =: x$ and for all $\mathbf{a} \in \mathcal{L}(S_{<x})$ the following conditions hold:

1. $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ and $\phi_{\mathbf{a}}(\mathrm{init}(q)) \neq 0$.
2. $\phi_{<x,\mathbf{a}}(p)$ and $\phi_{<x,\mathbf{a}}(q)$ are square-free,
3. For all $a \in \overline{K}$, $\phi_{<x,\mathbf{a}}(p)_{|x=a} = 0$ if and only if $\phi_{<x,\mathbf{a}}(q)_{|x=a} = 0$.

Define $U := \{\ y < x \mid (S_T)_y$ is an inequation or empty $\}$. Then there exist $c, d \in K[U] \setminus \{0\}$ such that $c \cdot \mathsf{Canonicalize}(S, p) = d \cdot \mathsf{Canonicalize}(S, q)$ for all $\mathbf{a} \in \mathcal{L}(S)$. ◁

Proof. Due to condition 1, we have $\deg_x(\phi_{<x,\mathbf{a}}(p)) = \mathrm{mdeg}(p)$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$ and the same statement holds for q. From 2 and 3, we immediately get that $\mathrm{mdeg}(p) = \mathrm{mdeg}(q) =: d$.

Let $\tilde{p} := \mathsf{Canonicalize}(S, p)$ and $\tilde{q} := \mathsf{Canonicalize}(S, q)$ and $c := \frac{\mathrm{lcm}(\mathrm{init}(\tilde{p}), \mathrm{init}(\tilde{q}))}{\mathrm{init}(\tilde{p})}$ and $d := \frac{\mathrm{lcm}(\mathrm{init}(\tilde{p}), \mathrm{init}(\tilde{q}))}{\mathrm{init}(\tilde{q})}$. Then $c, d \in K[U]$, since $\mathrm{init}(\tilde{p}), \mathrm{init}(\tilde{q}) \in K[U]$ by assumption. By definition of c and d, $c \cdot \tilde{p} = \mathsf{Canonicalize}(c \cdot \tilde{p})$ and $d \cdot \tilde{q} = \mathsf{Canonicalize}(d \cdot \tilde{q})$ and it holds that $\phi_{\mathbf{a}}(c) \neq 0 \neq \phi_{\mathbf{a}}(d)$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$. There is a polynomial $r \in R$ such that

$$c \cdot \tilde{p} = d \cdot \tilde{q} + r\ .$$

Since $\mathrm{init}(c \cdot \tilde{p}) = \mathrm{init}(d \cdot \tilde{q})$, we see that $\deg_x(r) < d$. For all $\mathbf{a} \in \mathcal{L}(S_{<x})$, we have

$$\phi_{<x,\mathbf{a}}(c) \cdot \phi_{<x,\mathbf{a}}(\tilde{p}) = \phi_{<x,\mathbf{a}}(d) \cdot \phi_{<x,\mathbf{a}}(\tilde{q}) + \phi_{<x,\mathbf{a}}(r)$$

and by assumption, there are exactly d distinct values $a \in \overline{K}$ such that $(\phi_{<x,\mathbf{a}}(c) \cdot \phi_{<x,\mathbf{a}}(\tilde{p}))_{|x=a} = 0$ and $(\phi_{<x,\mathbf{a}}(d) \cdot \phi_{<x,\mathbf{a}}(\tilde{q}))_{|x=a} = 0$. This implies $\phi_{<x,\mathbf{a}}(r)_{|x=a} = 0$ holds for d distinct values a. Since r has a degree smaller than d, it follows that $\phi_{<x,\mathbf{a}}(r) = 0$. Therefore, if $r = \sum_{i=0}^{d-1} c_i x^i$, then $\mathsf{Reduce}(S_{<x}, c_i) = 0$ for $i = 0, \ldots, d-1$. For each i, we therefore get $c_i = \sum_{y<x} b_y S_y$. Since $\deg_y(c \cdot \tilde{q}) < \mathrm{mdeg}(S_y)$, we get that $b_y \neq 0$ implies $\deg_y(c \cdot \tilde{p}) \geq \mathrm{mdeg}(S_y)$ which contradicts $c \cdot \tilde{p} = \mathsf{Canonicalize}(c \cdot \tilde{p})$. In summary, this implies $r = 0$. □

We want to define a simple system that is uniquely given by its solution set. If each polynomial p in a simple system S is canonicalized with respect $S_{<\mathrm{ld}(p)}$, we only need to normalize our polynomials as described in the following definition.

Definition 3.26. We call a polynomial $p \in R$ **monic** over R if either $\mathrm{init}(p) = 1 \in K$ or $\mathrm{init}(p) \notin K$ is monic. We call a simple system **normalized** if for each variable x the following conditions hold.

1. S_x is **monic** considered as a polynomial in R.
2. S_x is **primitive** considered as a univariate polynomial in the variable x, i.e. $S_x \in R_{<x}[x]$.
3. S_x is **canonicalized** modulo $S_{<x}$ where we consider $S_{<x}$ as a simple system over $R_{\leq x}$. ◁

This definition defines a canonical form for simple systems.

Corollary 3.27. *Let S, T be normalized simple systems over R. Then $\mathcal{L}(S) = \mathcal{L}(T)$ if and only if $S = T$.*

Proof. For a single variable, the statement is trivial.

Now consider two systems S, T with highest variable x and assume that the statement holds for the systems $S_{<x}$ and $T_{<x}$. From Remark (3.25), we know that there are $c, d \in K[U]$, with U defined as in Remark (3.25), such that $c \cdot S_x = d \cdot T_x$. However, since both S_x and T_x are primitive as polynomials in x, we get $c, d \in K^*$. Since both polynomials are monic, we get $c = d = 1$ and the statement follows. □

Example 3.28. The simple $S = \{(y\underline{x}^2 - 1)_=, (\underline{y}^2 + 1)_=\}$ system from Example 3.23 is fully coefficient-reduced, but not normalized, as $\deg_y(S_{\underline{x}}) > 0$ but S_y is an equation. We have

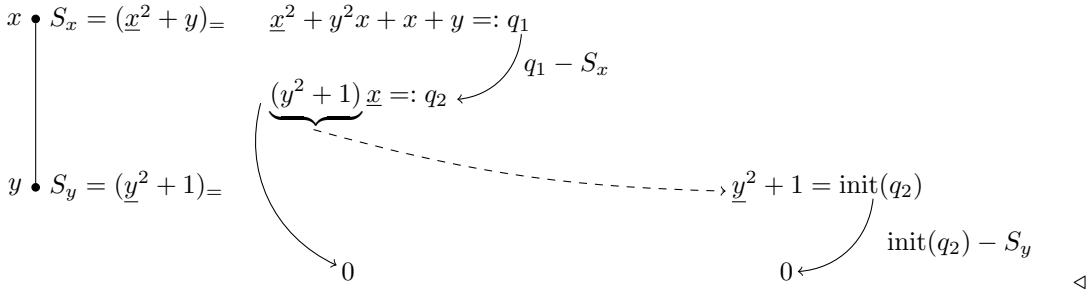
$$-y \cdot y + 1 \cdot \left(y^2 + 1\right) = 1 \ .$$

Thus we replace S_x with

$$\mathsf{prem}(-y \cdot (y\underline{x}^2 - 1), y^2 + 1, y) = \mathsf{prem}(-y^2\underline{x}^2 + y), \underline{y}^2 + 1, y) = \underline{x}^2 + y \ .$$

We get the system $S' = \{(\underline{x}^2 + y)_=, (\underline{y}^2 + 1)_=\}$, which is normalized and $\mathcal{L}(S) = \mathcal{L}(S')$.

As in Example (3.23), we reduce $q_1 := x^2 + y^2x + x + y$ modulo this new simple system.



◁

3.2.5 Splitting systems

We now examine all splitting methods needed for the decomposition algorithm. We will use the following one-liner as subalgorithm in all of them.

Algorithm 3.29 (Split)**.** *Input: A system S, a polynomial $p \in R$*
Output: The disjoint decomposition $(S \cup \{p_{\neq}\}, S \cup \{p_=\})$ of S.
Algorithm:

1: ***return*** $((S_T, S_Q \cup \{p_{\neq}\}), (S_T, S_Q \cup \{p_=\}))$

Please note that this method returns the system containing the inequation in the first component and the system containing the equation in the second component. New polynomials are always added to S_Q, since without further computation it is unknown how they fit into the triangular structure of S_T.

For a better understanding of the following splitting subalgorithms we first need to explain how they are applied in the main algorithm. Each step of the algorithm treats a system S as follows. An equation or inequation q is chosen and removed from the queue S_Q. Then we reduce q modulo S_T. For the simplicity properties to hold w.r.t. q it is necessary to add inequations to S. To accomplish this, we pass S together with q to the splitting subalgorithms. Each such subalgorithm returns two systems. The first system S_1 contains an additional inequation. The second system S_2 contains a complementary equation, q is added back into the queue of S_2, and S_2 is put aside for later treatment. In each case $(S_1 \cup \{q\}, S_2)$ is a disjoint decomposition of the original system $S \cup \{q\}$. Then S_1 and q may be subjected to further splitting algorithms and eventually q is added into the candidate simple system.

The first splitting algorithm we consider is InitSplit, which is concerned with property (3.8)(2).

Algorithm 3.30 (InitSplit)**.** *Input: A system S, an equation or inequation q with $\mathrm{ld}(q) = x$.*
Output: Two systems S_1 and S_2, where $(S_1 \cup \{q\}, S_2)$ is a disjoint decomposition of $S \cup \{q\}$. Moreover, $\phi_{\mathbf{a}}(\mathrm{init}(q)) \neq 0$ holds for all $\mathbf{a} \in \mathcal{L}(S_1)$ and $\phi_{\mathbf{a}}(\mathrm{init}(q)) = 0$ for all $\mathbf{a} \in \mathcal{L}(S_2)$.
Algorithm:

1: $(S_1, S_2) \leftarrow \mathsf{Split}(S, \mathrm{init}(q))$
2: $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
3: ***return*** (S_1, S_2)

3.2.6 Subresultants

For the further splitting algorithms, we need some preparation. In Definition (3.8) we consider a multivariate polynomial p as the family of univariate polynomials $\phi_{<\mathrm{ld}(p),\mathbf{a}}(p)$. For ensuring triangularity and square-freeness, we have to compute the gcd (greatest common divisor) of two polynomials, which in general depends on $\mathbf{a}$. This dependency can be expressed in terms of resultants and subresultants.

The **subresultant chain** of two polynomials p_1, p_2 with respect to x_i is a sequence of polynomials with decreasing degree in x_n that refines the EUCLIDean algorithm in the following sense. When substituting any values for the variables $x_1, \ldots, x_{i-1}$ into the subresultant, the result is (up to multiplication with non-zero constants) the sequence of polynomials obtained by first performing the same substitution on p_1, p_2 and then performing the EUCLIDean algorithm on the result. In particular, we can determine how the degree of the greatest common divisor depends on the parameters we substitute for $x_1, \ldots, x_{i-1}$.

Applying a similar method to a polynomial p and its partial derivative $\frac{\partial}{\partial x_i} p$ results in the **subdiscriminant chain** of p, which determines the dependency of the number of multiple roots on the parameters. Instead of the subdiscriminant chain, we use the subresultant chain of p and $\frac{\partial}{\partial x_i} p$, which only differs from the subdiscriminant chain by factors that are powers of $\mathrm{init}(p)$.

In [Tho37], resultants, discriminants and other related polynomials are computed as determinants of modified versions of the SYLVESTER matrix. These methods have since then been superseded by polynomial remainder sequences.

Example 3.31. The following polynomials form a subresultant chain with respect to x.

$$
\begin{aligned}
p_1 &= a_2 x^2 + a_1 x + a_0 \\
p_2 &= b_2 x^2 + b_1 x + b_0 \\
p_3 &= (a_1 b_2 - a_2 b_1)\, x + a_0 b_2 - a_2 b_0 \\
p_4 &= a_0^2 b_2^2 - a_0 a_1 b_1 b_2 - 2 a_0 a_2 b_0 b_2 + a_0 a_2 b_1^2 + a_1^2 b_0 b_2 a_1 a_2 b_0 b_1 + a_2^2 b_0^2
\end{aligned}
$$

Choosing the parameters as $a_2 = 1, b_2 = 1, a_1 = -1, a_0 = -1, b_1 = 1, b_0 = 1$ results in the chain

$$\begin{aligned} & x^2 - x - 1 \\ & x^2 + x + 1 \\ & -2x - 2 \\ & 4 \end{aligned}$$

indicating that p_1 and p_2 specialized with these parameters do not have a common divisor. Instead, we now choose a root of p_4 that is not a root of $\mathrm{lcoeff}(p_3, x)$, for example $a_2 = 1, b_2 = 1, a_1 = 1, b_1 = 2, b_0 = 1, a_0 = 0$. This results in the chain

$$\begin{aligned} & x^2 + x \\ & x^2 + 2x + 1 \\ & -x - 1 \\ & 0 \end{aligned}$$

which indicates that this specialization leads to polynomials with a common divisor of degree one. If we choose $a_2 = 1, b_2 = 2, a_1 = 1, b_1 = 2, b_0 = 2, a_0 = 1$, a common root of p_4 and $\mathrm{lcoeff}(p_3, x)$, the result is

$$\begin{aligned} & x^2 + x + 1 \\ & 2x^2 + 2x + 2 \\ & 0 \\ & 0 \end{aligned}$$

and the polynomials have a common divisor of degree two. ◁

We now cite two important definitions from [Mis93, Chap. 7.6], adapted for our special case.

Definition 3.32. Let x be a variable and $p_1, p_2 \in R$ with $\mathrm{ld}(p_1) = \mathrm{ld}(p_2) \leq x$. We call p_1, p_2 **similar** with respect to x, denoted by $p_1 \sim_x p_2$, if there are $a, b \in R_{<x} \setminus \{0\}$ such that $ap_1 = bp_2$. For $\mathrm{ld}(p_1) = \mathrm{ld}(p_2) = x$ with $\deg_x(p_1) \geq \deg_x(p_2)$, the sequence $p_1, \ldots, p_r$ is called **polynomial remainder sequence**, or PRS, if for $i = 3, \ldots, r$ we have

$$p_i \sim_x \mathsf{prem}\,(p_{i-2}, p_{i-1}, x) \neq 0$$

and $\mathsf{prem}\,(p_{r-1}, p_r, x) = 0$. ◁

It is obvious that $\mathrm{ld}(p_i) = x$ for $i = 1, \ldots, r-1$ and $\mathrm{ld}(p_r) \leq x$.

Denote by pr the classical pseudo remainder, in particular, for $p, q \in R$ with $\deg_x(p) \geq \deg_x(q)$,

$$\mathrm{pr}(p, q, x) = \mathrm{rem}\left(\mathrm{lcoeff}_x(q)^{\deg_x(p)-\deg_x(q)+1} p, q, x\right) .$$

Definition 3.33. Let $p_1, p_2 \in R$ with $\mathrm{ld}(p_1) = \mathrm{ld}(p_2) = x$. Set the initial values

$$\begin{aligned} a_1 &= \deg_x(p_1) & a_2 &= \deg_x(p_2) \\ \Delta_1 &= 0, & \Delta_2 &= a_1 - a_2 + 1 \\ b_1 &= 1, & b_2 &= \mathrm{init}(p_2) \\ \psi_1 &= 1, & \psi_2 &= (b_2)^{\Delta_2 - 1} \\ \beta_1 &= \beta_2 = 1 \end{aligned}$$

and define a polynomial remainder sequence $p_1, \ldots, p_r$ recursively as follows. For $i = 3, \ldots, k$, let

$$\beta_i = (-1)^{\Delta_{i-1}} (\psi_{i-2})^{\Delta_{i-1}-1} b_{i-2}$$

$$\begin{aligned} p_i &= \frac{\mathrm{pr}\,(p_{i-2}, p_{i-1}, x)}{\beta_i} \\ a_i &= \deg_x(p_i) \\ \Delta_i &= a_{i-1} - a_i + 1 \\ b_i &= \mathrm{init}(p_i) \\ \psi_i &= \psi_{i-1} \left(\frac{b_i}{\psi_{i-1}} \right)^{\Delta_i - 1} \end{aligned}$$

and let r such that $\mathrm{pr}(p_{r-1}, p_r, x) = 0$. This sequence is called **subresultant polynomial remainder sequence** or SPRS. ◁

Remark 3.34. Using the notation of Definition (3.33) let

$$p_i^* = \left(\frac{b_i}{\psi_{i-1}} \right)^{\Delta_i - 2} p_i \ .$$

For $i = 3, \ldots, r$, define $\mathrm{SubRes}_{a_{i-1}-1}(p_1, p_2, x) = p_i$ and $\mathrm{SubRes}_{a_i}(p_1, p_2, x) = p_i^*$. Obviously, if $a_{i-1} - 1 = a_i$ then $\Delta_i - 2 = a_{i-1} - a_i - 1 = 0$ and thus $p_i^* = p_i$. Set $\mathrm{SubRes}_j(p_1, p_2, x) = 0$ for all j for which it has not been defined yet. Then $(p_1, p_2, \mathrm{SubRes}_{a_2-1}(p_1, p_2, x), \ldots, \mathrm{SubRes}_0(p_1, p_2, x))$ is the **subresultant chain** of p_1 and p_2 with respect to x. The **subresultant** p_i^* is called **regular** of degree a_i. If $p_i \neq p_i^*$, then p_i is called **defective** of degree a_i. ◁

The above coincides with the classical definition of the subresultant chain as can be seen in [Mis93, Thm. 7.9.1] and [Mis93, Thm. 7.9.4]. The above definition gives a nice way of computing the subresultant chain using pseudo remainders. For a complete overview of subresultants and polynomial remainder sequences, we refer to [Mis93, Chap. 7] or [Yap00, Chap. 3]. We will now continue constructing our splitting algorithms and refer to [Mis93, Chap. 7] for the necessary proofs.

Definition 3.35. Let $p, q \in R$ with $\mathrm{ld}(p) = \mathrm{ld}(q) = x$, $\deg_x(p) = d_p \geq \deg_x(q) = d_q$. We denote $\mathrm{RRes}_i(p, q, x) = \mathrm{SubRes}_i(p, q, x)$, $i < d_q$ if it is a *regular* subresultant of degree i, otherwise $\mathrm{RRes}_i(p, q, x) = 0$. Furthermore, $\mathrm{RRes}_{d_q}(p, q, x) := q$ and if $d_q < d_p$ then $\mathrm{RRes}_{d_p}(p, q, x) := p$ and $\mathrm{RRes}_i(p, q, x) := 0$, $d_q < i < d_p$.

Define $\mathrm{res}_i(p, q, x) := \mathrm{init}\,(\mathrm{RRes}_i\,(p, q, x))$ for $0 < i < d_p$, $\mathrm{res}_{d_p}(p, q, x) := 1$ and $\mathrm{res}_0(p, q, x) := \mathrm{RRes}_0\,(p, q, x)$. ◁

The initials of the subresultants provide conditions to determine the degrees of all possible gcds. Using these conditions, we describe the splittings necessary to determine degrees of polynomials within one system as follows. For a system S and two given polynomials p_1, p_2 with leader x, we first determine the minimal possible i such that the degree of the gcd of $\phi_{<x,\mathbf{a}}(p_1)$ and $\phi_{<x,\mathbf{a}}(p_2)$ is i for some solution $\mathbf{a}$ of $S_{<x}$. We then split into two systems: The generic system, where this property holds for *all* solutions $\mathbf{a}$, and the special system, where the degree of the gcd is always greater than i. In the generic case, we can directly compute a polynomial g with $\mathrm{mdeg}(g) = i$ such that $\phi_{<x,\mathbf{a}}(g)$ is the gcd.

The following definition formalizes these notions. Algorithms (3.40), (3.41), (3.42) and (3.43) will demonstrate the computations.

Definition 3.36. Let S be a system and $p_1, p_2 \in R$ with $\mathrm{ld}(p_1) = \mathrm{ld}(p_2) = x$. If $|\mathcal{L}(S_{<x})| > 0$, we call

$$i := \min \{ i \in \mathbb{Z}_{\geq 0} \mid \exists\ \mathbf{a} \in \mathcal{L}(S_{<x}) \text{ such that } \deg_x(\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))) = i \}$$

the **minimal fiber cardinality** of p_1 and p_2 w.r.t. S. Moreover, if $(S_Q)^{=}_{<x} = \emptyset$, then

$$i' := \min\{ i \in \mathbb{Z}_{\geq 0} \mid \mathsf{Reduce}(S_T, \mathrm{res}_j(p_1, p_2, x)) = 0 \ \forall\ j < i \text{ and } \mathsf{Reduce}(S_T, \mathrm{res}_i(p_1, p_2, x)) \neq 0 \}$$

is the **minimal quasi fiber cardinality** of p_1 and p_2 w.r.t. S. A disjoint decomposition $(S_1, S_2) \in \mathcal{S}^2$ of S such that

1. $\deg_x(\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))) = i \ \forall\ \mathbf{a} \in \mathcal{L}\left((S_1)_{<x}\right)$
2. $\deg_x(\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))) > i \ \forall\ \mathbf{a} \in \mathcal{L}\left((S_2)_{<x}\right)$

is called i-th **fibration split** of p_1 and p_2 w.r.t. S. A polynomial $r \in R$ with $\mathrm{ld}(r) = x$ such that $\deg_x(r) = i$ and

$$\phi_{<x,\mathbf{a}}(r) \sim \gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2)) \ \forall\ \mathbf{a} \in \mathcal{L}\left((S_1)_{<x}\right)$$

is called i-th **conditional greatest common divisor** of p_1 and p_2 w.r.t. S, where $p \sim q$ if and only if $p \in \overline{K}^* q$. Furthermore, $q \in R$ with $\mathrm{ld}(q) = x$ and $\deg_x(q) = \deg_x(p_1) - i$ such that

$$\phi_{<x,\mathbf{a}}(q) \sim \frac{\phi_{<x,\mathbf{a}}(p_1)}{\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))} \ \forall\ \mathbf{a} \in \mathcal{L}\left((S_1)_{<x}\right)$$

is called i-th **conditional quotient** of p_1 by p_2 w.r.t. S.

If the characteristic of K is zero, using $p_2 := \frac{\partial}{\partial x} p_1$ yields an i-th **square-free split** and i-th **conditional square-free part** of p_1 w.r.t. S. ◁

Here is an example that demonstrates how these concepts will be utilized in the Decompose algorithm.

Example 3.37. Consider the system S with $S_T := \left\{\left(\underline{x}^3 + y\right)_=\right\}$ and $S_Q := \{y_{\neq}\}$ and the polynomial $q := \underline{x}^2 + x + y + 1$ with $y < x$. Computation shows

$$\begin{aligned}
\mathrm{res}_0(S_x, q, x) &= \underline{y}^3 + 7y^2 + 5y + 1 \\
\mathrm{res}_1(S_x, q, x) &= -\underline{y} \\
\mathrm{res}_2(S_x, q, x) &= 1\ .
\end{aligned}$$

Since $(S_T)_y$ is empty, we cannot reduce $\mathrm{res}_0(S_x, q, x)$ and the minimal quasi fiber cardinality of S_x and q w.r.t. S is 0. A zeroth fibration split is given by

$$\begin{aligned}
(S_1)_T &:= S_T & (S_1)_Q &:= S_Q \cup \left\{(\mathrm{res}_0(S_x, q, x))_{\neq}\right\} \\
(S_2')_T &:= S_T & (S_2')_Q &:= S_Q \cup \left\{(\mathrm{res}_0(S_x, q, x))_=\right\}\ .
\end{aligned}$$

A zeroth conditional gcd of S_x and q w.r.t. S is 1, thus a zeroth conditional quotient of S_x and q is S_x.

During the Decompose algorithm presented later, the system S_2' will be modified and eventually become the system S_2 with $(S_2)_T := \left\{\left(\underline{x}^3 + y\right)_=, \mathrm{res}_0(S_x, q, x)_=\right\}$ and $(S_2)_Q := \emptyset$. Since $\mathrm{res}_0(S_x, q, x)$ reduces to 0 modulo $(S_2)_T$ and $\mathrm{res}_0(S_x, q, x)$ does not, the minimal quasi fiber cardinality of S_x and q w.r.t. S_2 is 1. A first fibration split is given by

$$\begin{aligned}
(S_{2,1})_T &:= (S_2)_T & (S_{2,1})_Q &:= (S_2)_Q \cup \left\{\left(-\underline{y}\right)_{\neq}\right\} \\
(S_{2,2}')_T &:= (S_2)_T & (S_{2,2}')_Q &:= (S_2)_Q \cup \left\{\left(-\underline{y}\right)_=\right\}\ .
\end{aligned}$$

A first conditional gcd of S_x and q w.r.t. S_2 is $-y\underline{x} + 2y + 1$ and a first conditional quotient is $y^2\underline{x}^2 + (2y^2 + y)x + 4y^2 + 4y + 1$.

The system $S_{2,2}'$ is inconsistent and will eventually be discarded. ◁

In this case, the minimal quasi fiber cardinality and the minimal fiber cardinality were identical. In general, the minimal quasi fiber cardinality might be strictly smaller than the minimal fiber cardinality and our methods cannot detect this situation. However, in this case, the corresponding fibration split will lead to one inconsistent system and one where the minimal quasi fiber cardinality is increased, which is sufficient for our purposes.

Lemma 3.38. *Let $|\mathcal{L}(S_{<x})| > 0$ and $(S_Q)^{=}_{<x} = \emptyset$. For p_1, p_2 as in Definition (3.36) with $\phi_{\mathbf{a}}(\mathrm{init}(p_1)) \neq 0 \ \forall\ \mathbf{a} \in \mathcal{L}(S_{<x})$ and $\mathrm{mdeg}(p_1) > \mathrm{mdeg}(p_2)$, let i be the minimal fiber cardinality of p_1 and p_2 w.r.t. S and i' the corresponding minimal quasi fiber cardinality. Then*

$$i' \leq i$$

where the equality holds if and only if $|\mathcal{L}\left(S_{<x} \cup \{\mathrm{res}_{i'}(p_1, p_2, x)_{\neq}\}\right)| > 0$.

Proof. Let $\mathbf{a} \in \mathcal{L}(S_{<x})$, $d_{p_1} := \deg_x(p_1) = \deg_x(\phi_{<x,\mathbf{a}}(p_1))$, $d_{p_2} := \deg_x(p_2)$ and $d_{p_2,\mathbf{a}} := \deg_x(\phi_{<x,\mathbf{a}}(p_2))$. For $k < \max(d_{p_1}, d_{p_2,\mathbf{a}}) - 1 = d_{p_1} - 1$ then [Mis93, Thm. 7.8.1] implies

$$\phi_{<x,\mathbf{a}}(\mathrm{RRes}_k(p_1, p_2, x)) \sim \mathrm{RRes}_k(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2), x) \tag{3.3}$$

and

$$\phi_{\mathbf{a}}(\mathrm{res}_k(p_1, p_2, x)) = 0 \Longleftrightarrow \mathrm{res}_k(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2), x) = 0\ . \tag{3.4}$$

Conditions (3.3) and (3.4) by definition also hold for the trivial cases $d_{p_2} \leq k \leq d_{p_1}$.

For all indices $j < i'$, Corollary (3.20) and the fact $\mathsf{Reduce}(S_T, \mathrm{res}_j(p_1, p_2, x)) = 0$ imply $\phi_{\mathbf{a}}(\mathrm{res}_j(p_1, p_2, x)) = 0$. By (3.3) and (3.4), $\mathrm{res}_j(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2), x) = 0$ follows. We apply [Mis93, Thm. 7.10.5] successively and get $\mathrm{RRes}_j(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2), x) = 0$. Thus,

$$\deg_x(\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))) \geq i' \tag{3.5}$$

holds. This implies $i' \leq i$.

Equality in (3.5) holds if and only if there exists $\mathbf{a} \in \mathcal{L}(S_{<x})$ such that $\phi_{\mathbf{a}}(\mathrm{res}_{i'}(p_1, p_2, x)) \neq 0$. Therefore, $i = i'$ if and only if $|\mathcal{L}\left(S_{<x} \cup \{\mathrm{res}_{i'}(p_1, p_2, x)_{\neq}\}\right)| > 0$. □

The above lemma does not apply if both polynomials have the same degree. In this case, both polynomials must have non-vanishing initials, as shown in the following corollary.

Corollary 3.39. *Let $|\mathcal{L}(S_{<x})| > 0$ and $(S_Q)^{=}_{<x} = \emptyset$. For polynomials p_1, p_2 as in Definition (3.36) with $\phi_{\mathbf{a}}(\mathrm{init}(p_1)) \neq 0 \ \forall\ \mathbf{a} \in \mathcal{L}(S_{<x})$, let i be the minimal fiber cardinality of p_1 and p_2 w.r.t. S and i' the minimal quasi fiber cardinality of p_1 and $\mathsf{prem}(p_2, p_1, x)$ w.r.t. S. Then*

$$i' \leq i$$

with equality if and only if $|\mathcal{L}\left(S_{<x} \cup \{\mathrm{res}_{i'}(p_1, \mathsf{prem}(p_2, p_1, x), x)_{\neq}\}\right)| > 0$.

Proof. Let $\mathbf{a} \in \mathcal{L}(S_{<x})$. By the assumption on the initial of p_1, [Mis93, Cor. 7.5.6] implies

$$\phi_{<x,\mathbf{a}}(\mathsf{prem}(p_2, p_1, x)) = \mathsf{prem}(\phi_{<x,\mathbf{a}}(p_2), \phi_{<x,\mathbf{a}}(p_1), x)\ .$$

The univariate polynomials $\phi_{<x,\mathbf{a}}(p_1)$ and $\phi_{<x,\mathbf{a}}(p_2)$ have the same greatest common divisor as $\phi_{<x,\mathbf{a}}(p_1)$ and $\mathsf{prem}(\phi_{<x,\mathbf{a}}(p_2), \phi_{<x,\mathbf{a}}(p_1), x)$. We can therefore replace p_2 with $\mathsf{prem}(p_2, p_1, x)$ in Lemma (3.38). □

The following algorithm computes the minimal quasi fiber cardinality of two polynomials.

Algorithm 3.40 (ResSplit). *Input: A system S with $(S_Q)^{=}_{<x} = \emptyset$, two polynomials $p, q \in R$ with $\mathrm{ld}(p) = \mathrm{ld}(q) = x$, $\mathrm{mdeg}(p) > \mathrm{mdeg}(q)$ and $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$.*
Output: The quasi minimal fiber cardinality i of p and q w.r.t. S and an i-th fibration split (S_1, S_2) of p and q w.r.t. S.
Algorithm:

1: $i \leftarrow \min\{i \in \mathbb{Z}_{\geq 0} \mid \mathsf{Reduce}(S_T, \mathrm{res}_j(p, q, x)) = 0 \ \forall\ j < i \text{ and } \mathsf{Reduce}(S_T, \mathrm{res}_i(p, q, x)) \neq 0\}$
2: ***return*** $(i, S_1, S_2) := (i, \mathsf{Split}(S, \mathrm{res}_i(p, q, x)))$

Proof of Correctness. Assume $|\mathcal{L}((S_l)_{<x})| > 0$, $l = 1, 2$, as the statement is trivial otherwise.

Let $\mathbf{a} \in \mathcal{L}((S_1)_{<x})$. The polynomial $g := \mathrm{RRes}_i(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q), x)$ is not identically zero due to $(\mathrm{init}(g))_{\neq} = (\mathrm{res}_i(p, q, x))_{\neq} \in (S_1)_Q$. The degree of g is i and $g \sim \gcd(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q))$, as discussed in the proof of Lemma (3.38).

Let $\mathbf{a} \in \mathcal{L}((S_2)_{<x})$. [Mis93, Thm. 7.10.5] and $(\mathrm{init}(g))_{=} = (\mathrm{res}_i(p, q, x))_{=} \in (S_2)_Q$ imply $g \equiv 0$. Therefore, $\deg_x(\gcd(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q))) > i$. □

We apply the minimal fiber cardinality and fibration split to compute a greatest common divisor of a polynomial in S_T and another polynomial.

Algorithm 3.41 (ResSplitGCD). *Input: A system S with $(S_Q)^{=}_{<x} = \emptyset$, where $(S_T)_x$ is an equation, and an equation $q_=$ with $\mathrm{ld}(q) = x$. Furthermore, $\mathrm{mdeg}(q) < \mathrm{mdeg}((S_T)_x)$.*
Output: Two systems S_1 and S_2 and an equation $\widetilde{q}_=$ such that:

a) $S_2 = \widetilde{S_2} \cup \{q\}$ where $\left(S_1, \widetilde{S_2}\right)$ is an i-th fibration split of $(S_T)_x$ and q w.r.t. S,

b) $\widetilde{q}$ is an i-th conditional gcd of $(S_T)_x$ and q w.r.t. S,

where i is the minimal quasi fiber cardinality of p and q w.r.t. S.
Algorithm:

1: $(i, S_1, S_2) \leftarrow \mathsf{ResSplit}\,(S, (S_T)_x, q)$
2: $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
3: ***return*** $S_1, S_2, \mathrm{RRes}_i((S_T)_x, q, x)_=$

Proof of Correctness. Property a) follows from Algorithm (3.40) and line 2. Property b) was already shown in the correctness proof of Algorithm (3.40). □

Note that $i > 0$ is required in this case, as $i = 0$ would yield an inconsistency. Therefore, before calling ResSplitGCD, we will always ensure this condition in the main algorithm by incorporating the resultant of two equations into the system.

The following algorithm is similar, but instead of the gcd, it returns the first input polynomial divided by the gcd.

Algorithm 3.42 (ResSplitDivide). *Input: A system S with $(S_Q)^{=}_{<x} = \emptyset$ and two polynomials p, q with $\mathrm{ld}(p) = \mathrm{ld}(q) = x$ and $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$.*
Output: Two systems S_1 and S_2 and a polynomial $\widetilde{p}$ such that:

a) $S_2 = \widetilde{S_2} \cup \{q\}$ where $\left(S_1, \widetilde{S_2}\right)$ is an i-th fibration split of p and q' w.r.t. S,

b) $\widetilde{p}$ is an i-th conditional quotient of p by q' w.r.t. S,

where i is the minimal quasi fiber cardinality of p and q' w.r.t. S, with $q' = q$ for $\mathrm{mdeg}(p) > \mathrm{mdeg}(q)$ and $q' = \mathsf{prem}(q, p, x)$ otherwise.
Algorithm:

1: ***if*** $\mathrm{mdeg}(p) \leq \mathrm{mdeg}(q)$ ***then***
2: ***return*** $\mathsf{ResSplitDivide}(S, p, \mathsf{prem}(q, p, x))$
3: ***else***
4: $(i, S_1, S_2) \leftarrow \mathsf{ResSplit}\,(S, p, q)$
5: ***if*** $i > 0$ ***then***
6: $\widetilde{p} \leftarrow \mathsf{pquo}(p, \mathrm{RRes}_i(p, \mathsf{prem}(q, p, x), x), x)$
7: ***else***
8: $\widetilde{p} \leftarrow p$
9: ***end if***
10: $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
11: ***return*** $S_1, S_2, \widetilde{p}$
12: ***end if***

Proof of Correctness. According to Corollary (3.39), we can without loss of generality assume $\mathrm{mdeg}(p) > \mathrm{mdeg}(q)$.

Property a) follows from Algorithm (3.40) and line 10. For all $\mathbf{a} \in \mathcal{L}(S_1)$ the following holds: If $i = 0$ then $\deg_x(\gcd(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q'))) = 0$ and thus $\phi_{<x,\mathbf{a}}(p)$ shares no roots with $\phi_{<x,\mathbf{a}}(q')$. Now let $i > 0$. Formula (3.2) implies

$$m \cdot p = \widetilde{p} \cdot \mathrm{RRes}_i\,(p, q', x) + \mathsf{prem}\,(p, \mathrm{RRes}_i\,(p, q', x)\,, x)\ .$$

Due to [Mis93, Cor. 7.5.6] and (3.3), (3.4) there exist $k_1, k_2 \in \overline{K} \setminus \{0\}$ such that

$$\begin{aligned}
&\underbrace{\phi_{\mathbf{a}}(m)}_{\neq 0} \cdot \phi_{<x,\mathbf{a}}(p) \\
=&\phi_{<x,\mathbf{a}}(\widetilde{p}) \cdot \phi_{<x,\mathbf{a}}\left(\mathrm{RRes}_i\left(p,q,x\right)\right) + \phi_{<x,\mathbf{a}}\left(\mathsf{prem}(p, \mathrm{RRes}_i\left(p,q,x\right), x)\right) \\
=&\phi_{<x,\mathbf{a}}(\widetilde{p}) \cdot k_1\, \mathrm{RRes}_i\left(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q), x\right) + k_2 \mathsf{prem}(\phi_{<x,\mathbf{a}}(p), \underbrace{\mathrm{RRes}_i\left(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q), x\right)}_{\text{divides } \phi_{<x,\mathbf{a}}(p)}, x) \\
=&\phi_{<x,\mathbf{a}}(\widetilde{p}) \cdot k_1 \gcd(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q)) + 0\ .
\end{aligned}$$

Thus, we obtain property b) from

$$\phi_{<x,\mathbf{a}}(\widetilde{p}) \sim \frac{\phi_{<x,\mathbf{a}}(p)}{\gcd(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q))}$$

and $\deg_x(\phi_{<x,\mathbf{a}}(\widetilde{p})) = \deg_x(\phi_{<x,\mathbf{a}}(p)) - \deg_x(\gcd(\phi_{<x,\mathbf{a}}(p), \phi_{<x,\mathbf{a}}(q))) = \deg_x(p) - i$. □

Applying the last algorithm to a polynomial p and $\frac{\partial}{\partial \mathrm{ld}(p)} p$ yields an algorithm to make p square-free. We present it separately for better readability of the main algorithm.

Algorithm 3.43 (ResSplitSquareFree)**.** *Let the characteristic of K be zero.*
Input: A system S with $(S_Q)^{=}_{<x} = \emptyset$ and a polynomial p with $\mathrm{ld}(p) = x$ and $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$.
Output: Two systems S_1 and S_2 and a polynomial r such that:

a) $S_2 = \widetilde{S_2} \cup \{p\}$ where $\left(S_1, \widetilde{S_2}\right)$ is an i-th square-free split of p w.r.t. S,

b) r is an i-th conditional square-free part of p w.r.t. S,

where i is the minimal quasi fiber cardinality of p and $\frac{\partial}{\partial x} p$ w.r.t. S.
Algorithm:

1: $(i, S_1, S_2) \leftarrow \mathsf{ResSplit}\left(S, p, \frac{\partial}{\partial x} p\right)$
2: ***if*** $i > 0$ ***then***
3: $\quad r \leftarrow \mathsf{pquo}\left(p, \mathrm{RRes}_i\left(p, \frac{\partial}{\partial x} p, x\right), x\right)$
4: ***else***
5: $\quad r \leftarrow p$
6: ***end if***
7: $(S_2)_Q \leftarrow (S_2)_Q \cup \{p\}$
8: ***return*** S_1, S_2, r

Proof of Correctness. Since $\phi_{<x,\mathbf{a}}(\frac{\partial}{\partial x} p) = \frac{\partial}{\partial x} \phi_{<x,\mathbf{a}}(p)$, an i-th square-free split of p is an i-th fibration split of p and $\frac{\partial}{\partial x} p$. The rest follows from the proof of Algorithm (3.42). □

This algorithm is obviously not sufficient for ground fields of positive characteristic. We will consider the problem of square-freeness in positive characteristic in section 3.3.

In all ResSplit-based algorithms, $(S_Q)^{=}_{<x} = \emptyset$ is required. This ensures that all equations of a smaller leader than x can be used for reduction modulo S_T. The order in which polynomials are treated by the main algorithm must therefore be restricted.

3.2.7 Selection Strategy

While the order in which we treat elements of S_Q is restricted, some freedom remains. In order to implement our decomposition algorithm, it is necessary to choose a selection strategy.

Definition 3.44 (Select)**.** Let $\mathbb{P}_{\text{finite}}(M)$ be the set of all finite subsets of a set M. A **selection strategy** is a map

$$\begin{aligned}\mathsf{Select} : \mathbb{P}_{\text{finite}}\left(\{p_=, p_{\neq} \mid p \in R\}\right) &\longrightarrow \{p_=, p_{\neq} \mid p \in R\} : \\ Q &\longmapsto q \in Q\end{aligned}$$

with the following properties:

1. If $\mathsf{Select}(Q) = q_=$ is an equation, then $Q^{=}_{<\mathrm{ld}(q)} = \emptyset$.
2. If $\mathsf{Select}(Q) = q_{\neq}$ is an inequation, then $Q^{=}_{\leq \mathrm{ld}(q)} = \emptyset$. ◁

We demonstrate that these conditions are necessary for termination of our approach by giving an example where we violate them.

Example 3.45. Consider $R := K[a, x]$ with $a < x$ and the system S with $S_T := \emptyset$ and $S_Q := \left\{(x^2 - a)_=\right\}$. To insert $(x^2 - a)_=$ into S_T, we need to apply the ResSplitSquareFree algorithm: We calculate $\mathrm{res}_0(x^2 - a, 2x, x) = -4a$, $\mathrm{res}_1(x^2 - a, 2x, x) = 2$ and $\mathrm{res}_2(x^2 - a, 2x, x) = 1$ according to Definition (3.35). The minimal quasi fiber cardinality is 0 and we get the two new systems S_1, S_2 with

$$(S_1)_T = \{(x^2 - a)_=\}, (S_1)_Q = \{(-4a)_{\neq}\} \text{ and } (S_2)_T = \emptyset, (S_2)_Q = \{(x^2 - a)_=, (-4a)_=\} .$$

We now consider what happens with S_2: If we select $(x^2 - a)_=$ as the next equation to be treated, in violation of the properties in Definition (3.44), ResSplitSquareFree will split up S_2 into $S_{2,1}$, $S_{2,2}$ with

$$(S_{2,1})_T = \{(x^2 - a)_=\}, (S_{2,1})_Q = \{(-4a)_{\neq}, (-4a)_=\}$$

and

$$(S_{2,2})_T = \emptyset, (S_{2,2})_Q = \{(x^2 - a)_=, (-4a)_=, (-4a)_=\} .$$

As $S_2 = S_{2,2}$, this will lead to an endless loop. ◁

3.2.8 Main Algorithm

The following algorithm inserts a new equation into S_T. In particular, it replaces the equation or inequation of the same leader in S_T, putting it back into S_Q.

Algorithm 3.46 (InsertEquation)**.**
Input: A system S and an equation $r_=$ with $\mathrm{ld}(r) = x$ satisfying $\phi_{\mathbf{a}}(\mathrm{init}(r)) \neq 0$ and $\phi_{<x,\mathbf{a}}(r)$ square-free for all $\mathbf{a} \in \mathcal{L}(S_{<x})$.
Output: A system S where $r_=$ is inserted into S_T.
Algorithm:

1: ***if*** $(S_T)_x$ *is not empty* ***then***
2: $\quad S_T \leftarrow (S_T \setminus \{(S_T)_x\})$
3: ***end if***
4: $S_T \leftarrow S_T \cup \{r_=\}$
5: ***return*** S

Now we present the main algorithm. The general structure is as follows: In each iteration, a system S is selected from a list P of unfinished systems. An equation or inequation q is chosen from the queue S_Q according to the selection strategy. Then q is reduced modulo S_T and incorporated into the candidate simple system S_T using the splitting algorithms described above. In doing so, the algorithm may add new systems S_i to P. As soon as the algorithm produces a system containing an equation $c_=$ for $c \in K \setminus \{0\}$ or the inequation $0_{\neq}$, this system is discarded.

Algorithm 3.47 (Decompose)**.** *The algorithm is printed on page 51.*

Algorithm 3.47 (Decompose)
Input: A system S' with $(S')_T = \emptyset$.
Output: A Thomas decomposition of S'.
Algorithm:

$P \leftarrow \{S'\}$; *Result* $\leftarrow \emptyset$
while $|P| > 0$ **do**
  Choose $S \in P$; $P \leftarrow P \setminus \{S\}$
  if $|S_Q| = 0$ **then**
    Result $\leftarrow$ *Result* $\cup \{S\}$
  else
    $q \leftarrow \mathsf{Select}(S_Q)$; $S_Q \leftarrow S_Q \setminus \{q\}$
    $q \leftarrow \mathsf{Reduce}(S_T, q)$; $x \leftarrow \mathrm{ld}(q)$
    if $q \notin \{0_{\neq}, c_{=} \mid c \in F \setminus \{0\}\}$ **then**
      if $x \neq 1$ **then**
        if q is an equation **then**
          if $(S_T)_x$ is an equation **then**
            if $\mathsf{Reduce}(S_T, \mathrm{res}_0((S_T)_x, q, x)) = 0$ **then**
              $(S, S_1, p) \leftarrow \mathsf{ResSplitGCD}(S, q)$; $P \leftarrow P \cup \{S_1\}$
              $S \leftarrow \mathsf{InsertEquation}(S, p_{=})$
            else
              $S_Q \leftarrow S_Q \cup \{q_{=}, \mathrm{res}_0((S_T)_x, q, x)_{=}\}$
            end if
          else
            if $(S_T)_x$ is an inequation[a] **then**
              $S_Q \leftarrow S_Q \cup \{(S_T)_x\}$; $S_T \leftarrow S_T \setminus \{(S_T)_x\}$
            end if
            $(S, S_2) \leftarrow \mathsf{InitSplit}(S, q)$; $P \leftarrow P \cup \{S_2\}$
            $(S, S_3, p) \leftarrow \mathsf{ResSplitSquareFree}\,(S, q)$; $P \leftarrow P \cup \{S_3\}$
            $S \leftarrow \mathsf{InsertEquation}(S, p_{=})$
          end if
        else if q is an inequation **then**
          if $(S_T)_x$ is an equation **then**
            $(S, S_4, p) \leftarrow \mathsf{ResSplitDivide}\,(S, (S_T)_x, q)$; $P \leftarrow P \cup \{S_4\}$
            $S \leftarrow \mathsf{InsertEquation}(S, p_{=})$
          else
            $(S, S_5) \leftarrow \mathsf{InitSplit}(S, q)$; $P \leftarrow P \cup \{S_5\}$
            $(S, S_6, p) \leftarrow \mathsf{ResSplitSquareFree}\,(S, q)$; $P \leftarrow P \cup \{S_6\}$
            if $(S_T)_x$ is an inequation **then**
              $(S, S_7, r) \leftarrow \mathsf{ResSplitDivide}\,(S, (S_T)_x, p)$; $P \leftarrow P \cup \{S_7\}$
              $(S_T)_x \leftarrow (r \cdot p)_{\neq}$
            else if $(S_T)_x$ is empty **then**
              $(S_T)_x \leftarrow p_{\neq}$
            end if
          end if
        end if
      end if
      $P \leftarrow P \cup \{S\}$
    end if
  end if
end while
return *Result*

[a] Remember that $(S_T)_x$ might be empty, and thus neither an equation nor an inequation.

We demonstrate the algorithm with a simple example. Note, that we will omit systems which are obviously inconsistent.

Example 3.48. Let $S = (S_T, S_Q) := (\emptyset, \{(x^2+x+1)_=, (x+a)_\neq\})$ with $a < x$. According to Select, $q := (x^2+x+1)_=$ is chosen. As $\text{init}(q) = 1$ and $\text{res}_0(q, \frac{\partial}{\partial x}q, x) = 1$, the original system S is replaced by $\big(\{(x^2+x+1)_=\}, \{(x+a)_\neq\}\big)$.

Now, $q := (x+a)_\neq$ is selected and ResSplitDivide$(S, (S_T)_x, q)$ computes $\text{res}_0((S_T)_x, q, x) = \text{prem}((S_T)_x, q, x) = a^2 - a + 1$, $\text{res}_1((S_T)_x, q, x) = \text{init}(q) = 1$, and $\text{res}_2((S_T)_x, q, x) = 1$. As S_T contains no equation of leader a, none of these polynomials can be reduced. We decompose S into

$$S := (\underbrace{\{(x^2+x+1)_=, (a^2-a+1)_\neq\}}_{=S_T}, \underbrace{\{\}}_{=S_Q}) ,$$

which is already simple, and

$$S_1 := (\underbrace{\{(x^2+x+1)_=\}}_{=(S_1)_T}, \underbrace{\{(x+a)_\neq, (a^2-a+1)_=\}}_{=(S_1)_Q}) .$$

We replace S_1 by

$$S_1 := \big(\{(x^2+x+1)_=, (a^2-a+1)_=\}, \{(x+a)_\neq\}\big)$$

and apply ResSplitDivide$(S_1, ((S_1)_T)_x, q)$ to S_1 again. This time, Reduce$((S_1)_T, a^2-a+1) = 0$ holds and S_1 is replaced with

$$S_1 := (\{\underbrace{(x-a+1)_=}_{\text{pquo}(x^2+x+1, x+a, x)}, (a^2-a+1)_=\}, \{1_\neq\}) .$$

Finally, a Thomas decomposition of S is:

$$\big(\{(x^2+x+1)_=, (a^2-a+1)_\neq\}, \{(x-a+1)_=, (a^2-a+1)_=\}\big) . \qquad \triangleleft$$

Proof of Algorithm (3.47) (Correctness). First, note that it is easily verified that the input specifications of all subalgorithms are fulfilled (in particular, for lines 14 and 29, cf. Remark (3.19)(1)).

The correctness of the Decompose algorithm is proved by verifying two loop invariants:

1. $P \cup \mathit{Result}$ is a disjoint decomposition of the input S'.
2. For all systems $S \in P \cup \mathit{Result}$, S_T is triangular and
   (a) $\phi_{<x,\mathbf{a}}(p)$ is square-free and
   (b) $\phi_{\mathbf{a}}(\text{init}(p)) \neq 0$

   for all $p \in S_T$ with $\text{ld}(p) = x$ and all $\mathbf{a} \in \mathcal{L}((S_T)_{<x} \cup (S_Q)_{<x})$.

We begin with proving the first loop invariant. Assume that $P \cup \mathit{Result}$ is a disjoint decomposition of S' at the beginning of the main loop. It suffices to show that all systems we add to P or *Result* add up to a disjoint decomposition of the system S, that is chosen in line 3. If $S_Q = \emptyset$ holds in line 4, the algorithm just moves S from P to *Result*.

In line 17, adding $\text{res}_0((S_T)_x, q, x)_=$ to S does not change the solutions of S, as for each $\mathbf{a} \in \overline{F}^n$, $\phi_{<x,\mathbf{a}}((S_T)_x) = 0$ and $\phi_{<x,\mathbf{a}}(q) = 0$ imply $\phi_{\mathbf{a}}(\text{res}_0((S_T)_x, q, x)) = 0$ (cf. [Mis93, Lemma 7.2.3]).

Note now that if (S, S_i) is the output of any of the ResSplitGcd, InitSplit, ResSplitSquareFree and ResSplitDivide algorithms, then $(S \cup \{q\}, S_i)$ is a disjoint decomposition of $S_0 \cup \{q\}$, where S_0 is the input of the respective algorithm. It remains to be shown that the actions performed in lines 15, 25, 30, 36 and 38 are equivalent to putting q back into the system S.

Let $\mathbf{a} \in \mathcal{L}(S_{<x})$. In the context of line 15, Algorithm (3.41) guarantees

$$\phi_{<x,\mathbf{a}}(p) = 0 \iff \phi_{<x,\mathbf{a}}((S_T)_x) = 0 \text{ and } \phi_{<x,\mathbf{a}}(q) = 0 .$$

In the context of line 30, Algorithm (3.42) ensures that

$$\phi_{<x,\mathbf{a}}(p) = 0 \iff \phi_{<x,\mathbf{a}}((S_T)_x) = 0 \text{ and } \phi_{<x,\mathbf{a}}(q) \neq 0 \ .$$

In lines 25, 36 and 38, p has the same solutions as q, due to Algorithm (3.43) and

$$\phi_{<x,\mathbf{a}}(p) \sim \frac{\phi_{<x,\mathbf{a}}(q)}{\gcd(\phi_{<x,\mathbf{a}}(q), \phi_{<x,\mathbf{a}}(\frac{\partial}{\partial x}q))} = \frac{\phi_{<x,\mathbf{a}}(q)}{\gcd(\phi_{<x,\mathbf{a}}(q), \frac{\partial}{\partial x}\phi_{<x,\mathbf{a}}(q))} \ .$$

In addition, in line 36,

$$\phi_{<x,\mathbf{a}}(r) \sim \frac{\phi_{<x,\mathbf{a}}((S_T)_x)}{\gcd(\phi_{<x,\mathbf{a}}((S_T)_x), \phi_{<x,\mathbf{a}}(p))} \Longrightarrow \phi_{<x,\mathbf{a}}(r \cdot p) \sim \operatorname{lcm}(\phi_{<x,\mathbf{a}}((S_T)_x), \phi_{<x,\mathbf{a}}(p)) \ .$$

This concludes the proof of the first loop invariant.

Now, we prove the second loop invariant. At the beginning, the loop invariant holds because $S'_T = \emptyset$ holds for the input system S'. Assume that the second loop invariant holds at the beginning of the main loop.

One easily checks that all steps in the algorithm allow only one polynomial $(S_T)_x$ in S_T for each leader x, thus triangularity obviously holds.

We show that all polynomials added to S_T have non-zero initial and are square-free. For $\mathcal{L}(S_{<x}) = \emptyset$, the statement is trivially true. So, let $\mathbf{a} \in \mathcal{L}(S_{<x})$.

For the equation $p_= $ added as conditional gcd of $(S_T)_x$ and q in line 15, it holds that $\phi_{<x,\mathbf{a}}(p)$ is a divisor of $\phi_{<x,\mathbf{a}}((S_T)_x)$. As $\phi_{<x,\mathbf{a}}((S_T)_x)$ is square-free by assumption, so is $\phi_{<x,\mathbf{a}}(p)$. The inequation added to S in ResSplitGCD is by Definition (3.35) the initial of $p_=$.

The equation $p_=$ inserted into S_T in line 25 and the inequation $p_{\neq}$ inserted in line 38 are square-free due to Algorithm (3.43) and their initials are non-zero as p is either identical to q, or it is a pseudo quotient of q by $\operatorname{RRes}_i\left(q, \frac{\partial}{\partial x}q, x\right)$ for some $i > 0$. On the one hand, if p equals q, the call of InitSplit for q ensures a non-zero initial for p. On the other hand, the polynomial $\operatorname{RRes}_i\left(q, \frac{\partial}{\partial x}q, x\right)$ has initial $\operatorname{res}_i\left(q, \frac{\partial}{\partial x}q, x\right)$, which is added as an inequation by ResSplitSquareFree. This implies that the initial of the pseudo quotient is also non-zero.

The equation $p_=$ that replaces the old equation $(S_T)_x$ in line 30 is the quotient of $(S_T)_x$ by an inequation. It is square-free, because $\phi_{<x,\mathbf{a}}(p)$ is a divisor of $\phi_{<x,\mathbf{a}}((S_T)_x)$, which is square-free by assumption. Again, p is either identical to $(S_T)_x$ or a pseudo quotient of $(S_T)_x$ by $\operatorname{RRes}_i((S_T)_x, q, x)$ for some $i > 0$ and, using the same arguments as in the last paragraph, the initial of p does not vanish.

Finally, consider the inequation $(r \cdot p)_{\neq}$ added in line 36 as a least common multiple of $((S_T)_x)_{\neq}$ and $p_{\neq}$. The inequation $\phi_{<x,\mathbf{a}}(p)$ is square-free and has non-vanishing initial for the same reasons as before. Due to $\phi_{<x,\mathbf{a}}(r) \sim \frac{\phi_{<x,\mathbf{a}}((S_T)_x)}{\gcd(\phi_{<x,\mathbf{a}}((S_T)_x), \phi_{<x,\mathbf{a}}(p))}$, the polynomials $\phi_{<x,\mathbf{a}}(r)$ and $\phi_{<x,\mathbf{a}}(p)$ have no common divisors. As $\phi_{<x,\mathbf{a}}(r)$ divides $\phi_{<x,\mathbf{a}}((S_T)_x)$, using the same arguments as before, $\phi_{<x,\mathbf{a}}(r)$ is square-free and has a non-vanishing initial. This completes the proof of the second loop invariant.

It is obvious that a system S with $S_Q = \emptyset$ for which these loop invariants hold is simple. Thus the algorithm returns the correct result if it terminates. □

We now start showing termination. The system S chosen from P is treated in one of three ways: It is either discarded, added to *Result*, or replaced in P by at least one new system. To show that P is empty after finitely many iterations, we define an order on the systems and show that it is well-founded. Afterwards, we prove termination by detailing that the algorithm produces descending chains of systems.

Definition 3.49. For transitive and asymmetric[2] partial orders $<_i$ for $i = 1, \ldots, m$, we define the **composite order** " $<$ " $:= [<_1, \ldots, <_m]$ as follows: $a < b$ if and only if there exists $i \in \{1, \ldots, m\}$ such that $a <_i b$ and neither $a <_j b$ nor $b <_j a$ for $j < i$. The composite order is clearly transitive and asymmetric. An order $<$ is called **well-founded**, if each $<$-descending chain becomes stationary. ◁

[2] A relation $\prec$ is asymmetric, if $S \prec S'$ implies $S' \not\prec S$ for all S, S'. Asymmetry implies irreflexivity.

The following trivial statement will be used repeatedly:

Remark 3.50. If each $<_i$ is well-founded, then so is the composite order $<$, using the notation from Definition (3.49). ◁

Now we define the orders and show their well-foundedness:

Definition and Remark 3.51. Define $\prec$ as the composite order $[\prec_1, \prec_2, \prec_3, \prec_4]$ of the four orders on $\mathcal{S}$ defined below. It is well-founded since the $\prec_i$ are.

1. For $i = 1, \ldots, n$ define $\prec_{1,x_i}$ by $S \prec_{1,x_i} S'$ if and only if $\operatorname{mdeg}\left((S_T)^{=}_{x_i}\right) < \operatorname{mdeg}\left((S'_T)^{=}_{x_i}\right)$, with $\operatorname{mdeg}\left((S_T)^{=}_{x_i}\right) := \infty$ if $(S_T)^{=}_{x_i}$ is empty. Define the composite order $\prec_1$ as $[\prec_{1,x_1}, \ldots, \prec_{1,x_n}]$. Since degrees can only decrease finitely many times, the orders $\prec_{1,x_i}$ are clearly well-founded and, thus, $\prec_1$ is.

2. Define the map μ from the set of all systems over K to $\{1, x_1, \ldots, x_n, x_\infty\}$, where $\mu(S)$ is minimal such that there exists an equation $p \in (S_Q)^{=}_{\mu(S)}$ with $\mathsf{Reduce}(S_T, p) \neq 0$, or $\mu(S) = x_\infty$ if no such equation exists. Then, $S \prec_2 S'$ if and only if $\mu(S) < \mu(S')$ with $1 < x_i$ and $x_i < x_\infty$ for $i \in \{1, \ldots, n\}$. The order $\prec_2$ is well-founded since $<$ is well-founded on the finite set $\{1, x_1, \ldots, x_n, x_\infty\}$.

3. $S \prec_3 S'$ if and only if there is $p_{\neq} \in K^{\neq}$ and a finite (possibly empty) set $L \subset K^{\neq}$ with $\operatorname{ld}(q) < \operatorname{ld}(p)\ \forall\ q \in L$ such that $S_Q \uplus \{p_{\neq}\} = S'_Q \uplus L$ holds. We show well-foundedness by induction on the highest appearing leader x in $(S_Q)^{\neq}$: For $x = 1$ we can only make a system $S \prec_3$-smaller by removing one of the finitely many inequations in $(S_Q)^{\neq}$. Now assume that the statement is true for all indeterminates $y < x$. By the induction hypothesis we can only $\prec_3$-decrease S finitely many times without changing $(S_Q)^{\neq}_x$. To further $\prec_3$-decrease S, we have to remove an inequation from $(S_Q)^{\neq}_x$. As $(S_Q)^{\neq}_x$ is finite, this process can only be repeated finitely many times until $(S_Q)^{\neq}_x = \emptyset$. Now, the highest appearing leader in $(S_Q)^{\neq}$ is smaller than x and by the induction hypothesis, the statement is proved.

4. $S \prec_4 S'$ if and only if $|S_Q| < |S'_Q|$. ◁

The proof of termination uses this order. Every time that the Decompose algorithm modifies or splits a system, the resulting systems are strictly $\prec$-smaller. Since $\prec$ is well-founded, a strictly decreasing chain of elements of $\mathcal{S}$ must be finite. Therefore, we can modify or split a system only finitely many times until it is either inconsistent or simple.

Proof of Algorithm (3.47) (Termination). We will tacitly use the fact that reduction never makes polynomials bigger in the sense of Remark (3.19)(3).

We denote the system chosen from P in line 3 by $\widehat{S}$ and the system added to P in line 43 by S. We prove that the systems $S, S_1, \ldots, S_7$ generated from $\widehat{S}$ are $\prec$-smaller than $\widehat{S}$. For $i = 1, \ldots, 4$ we will use the notation $S \not\prec_i S'$ if neither $S \prec_i S'$ nor $S' \prec_i S$ holds.

For $j = 1, \ldots, 7$, $((S_j)_T)^{=} = (\widehat{S}_T)^{=}$ and thus $S_j \not\prec_1 \widehat{S}$. The properties of Select in Definition (3.44) directly require that there is no equation in $(\widehat{S}_Q)^{=}$ with a leader smaller than x. However, the equation added to the system S_j returned from InitSplit (3.30) is the initial of q, which has a leader smaller than x and does not reduce to 0 (cf. Remark (3.19)(2)). Furthermore, the equations added in one of the subalgorithms based on ResSplit (3.40) have a leader smaller than x and do not reduce to 0. In each case $S_j \prec_2 \widehat{S}$ is proved.

It remains to show $S \prec \widehat{S}$. If q is reduced to $0_{=}$, then it is omitted from S_Q and so $S \prec_4 \widehat{S}$. As the system is otherwise unchanged, $S \not\prec_i \widehat{S}, i = 1, 2, 3$ and therefore $S \prec \widehat{S}$ holds. If q is reduced to $c_{\neq}$ for some $c \in K \setminus \{0\}$, then $S \prec_3 \widehat{S}$ and $S \not\prec_i \widehat{S}, i = 1, 2$, since the only change was the removal of an inequation from S_Q. Otherwise, exactly one of the following cases will occur:

Lines 14-15 set $(S_T)_x$ to $p_{=}$ of smaller degree than $(\widehat{S}_T)_x$ and 20-25 add $(S_T)_x$ as a new equation. In both cases we get $S \prec_1 \widehat{S}$.

In line 17, $S_T = \widehat{S}_T$ implies $S \not\swarrow_1 \widehat{S}$. The polynomial q is chosen according to Select (cf. (3.44)(1)), which implies $(\widehat{S}_Q)^{=}_{<x} = \emptyset$ and $(S_Q)^{=}_{<x} = \{\mathrm{res}_0((S_T)_x, q, x)_=\}$. Line 13 ensures $\mathsf{Reduce}(S, \mathrm{res}_0((S_T)_x, q, x)) \neq 0$ and, thus, $S \prec_2 \widehat{S}$ follows.

Consider lines 29-30. If the degree of $(S_T)_x$ is smaller than the degree of $(\widehat{S}_T)_x$, then $S \prec_1 \widehat{S}$. In case the degree does not change, we have $S \not\swarrow_1 \widehat{S}$ and $(S_Q)^{=} = (\widehat{S}_Q)^{=}$ guarantees $S \not\swarrow_2 \widehat{S}$. However, q is removed from S_Q and replaced by an inequation of smaller leader, which implies $S \prec_3 \widehat{S}$.

In 31-39, obviously $S \not\swarrow_i \widehat{S}, i = 1, 2$. As before, q is removed from S_Q and replaced by an inequation of smaller leader, which once more implies $S \prec_3 \widehat{S}$. □

In conclusion, we have proved that every polynomial system over $R = K[x_1, \ldots, x_n]$ can be disjointly decomposed into simple systems if the characteristic of K is zero. For positive characteristic, we have to extend our notion of a polynomial system.

3.3 Square-freeness in positive characteristic

For this section, let $p > 0$ be a prime number, K a field of characteristic p and $R = K[x_1, \ldots, x_n]$. In this case, ensuring square-freeness is not as straightforward as before. We demonstrate the core of the newly arising problem in the following example.

Example 3.52. Let $x > y$ and consider the system $\{(x^p - y)_=\}$ over $K[x, y]$. For every $y \in \overline{K}$, the polynomial $x^p - y$ has exactly one root in $r(y) \in \overline{K}$. However, there is no polynomial in $q \in K[x, y]$ with $\deg_x(q) = 1$ such that $r(y)$ is the only root of $\phi_{<x,(y)}(q) \in \overline{K}[x]$. In particular, $r(y)$ is not a polynomial in y. ◁

For the zero-dimensional case, this problem has been solved in [LMW10]. The same authors also published an article on the positive-dimensional case, cf. [MWL13]. However, that article refers to a concept called "simple sets" which is (in positive dimension) not equivalent to that of a simple system. In particular, the system in the above example is a simple set according to the definition in [MWL13] and thus the counting polynomial cannot be read off from the degrees of its polynomials.

We will use some ideas from [LMW10] and an extension of our notion of a simple system to construct a decomposition of a polynomial system suitable to construct a counting polynomial, thus proving $(\overline{K}, n)$-enumerability of any simple system over $K[x_1, \ldots, x_n]$. We use the following well-known result.

Theorem 3.53. *The* Frobenius *maps*

$$R \to R : q \mapsto q^p$$

and

$$K \to K : q \mapsto q^p$$

are injective homomorphisms, i.e. monomorphisms.

Proof. Clearly, $0^p = 0$ and $1^p = 1$. Let $a, b \in R$ or $a, b \in K$. It is also obvious that $(ab)^p = a^p b^p$. For addition, we have

$$(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

since $p | \binom{p}{i}$ for $i \notin \{0, p\}$. This proves that the Frobenius map is an endomorphism. Since R and K have no zero divisors, the kernel of the Frobenius map is $\{0\}$. □

Corollary 3.54. *Let $a \in K$. If $x^p - a$ has a solution in K, then that solution is uniquely determined and we denote it by $a^{\frac{1}{p}}$ or $\sqrt[p]{a}$. It holds that*

$$\left(x - a^{\frac{1}{p}}\right)^p = x^p - a \ .$$

In particular, if K is either algebraic over $\mathbb{F}_p$ or algebraically closed, then the Frobenius *map on K is an isomorphism.*

Later, in particular in Remark (3.60), we may need to compute $a^{\frac{1}{p}}$ for some $a \in K$. From now on, assume that K is either algebraic over $\mathbb{F}_p$ or algebraically closed. Then $a^{\frac{1}{p}}$ is always an element of K.

Definition 3.55. Let $e_1, \ldots, e_n \in \mathbb{Z}$. Define the rings

$$R_{\sqrt{}}^{(e_1,\ldots,e_n)} := K\left[x_1^{\frac{1}{p^{e_1}}}, \ldots, x_n^{\frac{1}{p^{e_n}}}\right]$$

and

$$R_{\sqrt{}} := \bigcup_{(e_1,\ldots,e_n)\in\mathbb{Z}_{\geq 0}^n} R_{\sqrt{}}^{(e_1,\ldots,e_n)}$$

where the $x_i^{\frac{1}{p^{e_i}}}, i = 1, \ldots, n$ are algebraically independent and we write $\left(x_i^{\frac{1}{p^{e_i}}}\right)^p = x_i^{\frac{1}{p^{e_i-1}}}$. In particular, if $e_i > 0$, then we write $\left(x_i^{\frac{1}{p^{e_i}}}\right)^{p^{e_i}} = x_i$ and consider it an element of R. We call the elements of $R_{\sqrt{}}$ **polynomials with p-th roots**.

For $1 \leq i \leq n$ and $q \in R_{\sqrt{}}$, the minimal $e_i \in \mathbb{Z}$ such that there are $e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n \in \mathbb{Z}$ with $q \in R_{\sqrt{}}^{(e_1,\ldots,e_i,\ldots,e_n)}$ is called the **root degree** of q in x_i, denoted by $\operatorname{rdeg}_{x_i}(q)$. If $\operatorname{rdeg}_{x_i}(q) > 0$, then $\deg_{x_i}(q)$ is not defined, otherwise we can consider q a polynomial in x_i and define the degree as usual. ◁

If $e_i \geq 0, i = 1, \ldots, n$, the map $R \to R_{\sqrt{}}^{(e_1,\ldots,e_n)} : x_i \mapsto x_i$ is well-defined and injective, thus $R \subseteq R_{\sqrt{}}$. For any $q \in R_{\sqrt{}}$, it holds that $q \in R$ if and only if $\operatorname{rdeg}_{x_i}(q) \leq 0$ for all $i = 1, \ldots, n$.

Remark 3.56. Since $R_{\sqrt{}}$ is not finitely generated as a K-algebra, it is not noetherian. However, for all $(e_1, \ldots, e_n) \in \mathbb{Z}^n$, $R_{\sqrt{}}^{(e_1,\ldots,e_n)}$ is a polynomial ring in $x_1^{\frac{1}{p^{e_1}}}, \ldots, x_n^{\frac{1}{p^{e_n}}}$ and as such a noetherian ring. ◁

The Frobenius map is a monomorphism in the same way as shown in Theorem (3.53). If it is an isomorphism on K, it is an isomorphism on $R_{\sqrt{}}$, too, i.e. for any $q \in R_{\sqrt{}}$, it holds that $q^{\frac{1}{p}} \in R_{\sqrt{}}$. A polynomial system with roots is defined analogously to a polynomial system, with the ring R replaced with $R_{\sqrt{}}$, and the definition of the solution operator $\mathcal{L}$ remains the same. Due to Corollary (3.54), the solution operator is well-defined.

As in Definition (3.5), the leader of a polynomial $q \in R$ is the $<$-largest variable x_i such that $q \in K[x_1, \ldots, x_i]_{\sqrt{}} \setminus K[x_1, \ldots, x_{i-1}]_{\sqrt{}}$. If $\operatorname{rdeg}_{\operatorname{ld}(q)}(q) \leq 0$, then the main degree and initial of q are defined as in Definition (3.5), otherwise they are undefined.

We can now extend Definition (3.8) to fit into this context. For clarity, we repeat the entire definition here.

Definition 3.57. A polynomial system with p-th roots S over $K[x_1, \ldots, x_n]_{\sqrt{}}$ is called **simple** if it fulfills the following properties:

1. S is **triangular**, i.e. $|S_{x_i}| \leq 1$ for all $1 \leq i \leq n$ and $S \cap \{c_=, c_{\neq} | c \in K\} = \emptyset$.
2. For each $x \in \operatorname{ld}(S)$, we have $\operatorname{rdeg}_x(S_x) \leq 0$, i.e. S_x is a polynomial in x.

3. S has **non-vanishing initials**, i.e. $\phi_{\mathbf{a}}(\operatorname{init}(q)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x_i})$ and all $q \in S_{x_i}$, $1 < i \leq n$.

4. S is **square-free**, i.e. $\phi_{<x_i,\mathbf{a}}(q)$ is a square-free univariate polynomial in $\overline{K}[x_i]$ for all $\mathbf{a} \in \mathcal{L}(S_{<x_i})$ and all $q \in S_{x_i}$ for $1 \leq i \leq n$.

5. For each $x \in \operatorname{ld}(S^{=})$, we have $\operatorname{rdeg}_x(S_y) \leq 0$ for all $y \in \operatorname{ld}(S)$. ◁

In this definition, condition 2 is necessary to make reduction possible, since without it, the main degree and initial of S_x are undefined. Condition 5 is necessary to allow coefficient reduction. These conditions also ensure that roots of variables only occur when absolutely necessary.

Remark 3.58. Remark (3.10) and Theorem (3.16) hold for a simple system S with p-th roots. In particular, $\mathcal{L}(S)$ is elementary $(\overline{K}, n)$-enumerable with the same counting polynomial $c(S)$ as defined in (3.16). ◁

We will now state elementary facts which we will need when adjusting the Thomas decomposition algorithm for positive characteristic.

Remark 3.59. Let $q \in R_{\sqrt{}}$ with $\operatorname{ld}(q) = x$ and $r = \operatorname{rdeg}_x(q) > 0$. Then $\operatorname{rdeg}_x\left(q^{(p^r)}\right) = 0$ and for any $\mathbf{a} \in \overline{K}^n$, it holds that $\phi_{\mathbf{a}}(q) = 0$ if and only if $\phi_{\mathbf{a}}\left(q^{(p^r)}\right) = 0$. We can therefore transform any polynomial with p-th roots into a polynomial in its leader. ◁

This remark relates to Definition (3.57)2., as it makes it possible to transform the relevant polynomials with p-th roots into polynomials in their leader, thus giving us a well-defined main degree and initial.

Remark 3.60. Let $q \in R_{\sqrt{}}$ with $\operatorname{ld}(q) = x$ and $r = \operatorname{rdeg}_x(q)$. Then

$$q = \sum_{i=0}^{s} a_i x^{\frac{i}{p^r}}$$

for $a_i \in (R_{<x})_{\sqrt{}}$ and

$$q^{\frac{1}{p}} = \sum_{i=0}^{s} (a_i)^{\frac{1}{p}} x^{\frac{i}{p^{r+1}}} \ .$$

In particular, if $r \leq -1$, i.e. q is a polynomial in x^p, then $\operatorname{rdeg}_x\left(q^{\frac{1}{p}}\right) = 0$, i.e. $q^{\frac{1}{p}} \in R_{<x\sqrt{}}[x]$ is a polynomial in x. ◁

The last remark allows us to compute the p-th root of a polynomial. What's missing is a way to ensure (3.57)5. The following lemma is based on the method demonstrated in [LMW10, Example 4.1].

Lemma 3.61. *Let $q \in R_{\sqrt{}}$ with $\operatorname{ld}(q) = x$, $\operatorname{rdeg}_x(q) \leq 0$, $\operatorname{mdeg}(q) = d > 1$ and $\operatorname{disc}(q, x) \neq 0$, i.e. $q \in \left((R_{<x})_{\sqrt{}}\right)[x]$. Denote by A the smallest multiplicatively closed set containing $\operatorname{init}(q)$ and $\operatorname{disc}(q, x)$. Then there is an element $r \in \left(A^{-1}(R_{<x})_{\sqrt{}}\right)[x]$ with $0 < \deg_x(r) < d$ such that*

$$\operatorname{rem}(r^p, q, x) = x$$

*which we call the **p-th root of x modulo q**. In particular, $\operatorname{rem}\left(\phi_{<x,\mathbf{a}}(r^p), \phi_{<x,\mathbf{a}}(q), x\right) = x$ for all $\mathbf{a} \in \overline{K}^n \setminus \mathcal{L}(\{\operatorname{init}(q), \operatorname{disc}(q, x)\})$.*

Proof. Consider the ansatz $r = \sum_{i=0}^{d-1} a_i x^i$. Then $r^p = \sum_{i=0}^{d-1} a_i^p x^{p \cdot i} = \sum_{i=0}^{d-1} b_i x^{p \cdot i}$ by substituting $a_i^p \mapsto b_i$. The remainder $s = \operatorname{rem}(r^p, q, x) = \sum_{i=0}^{d-1} \operatorname{rem}\left(x^{p \cdot i}, q, x\right) \cdot b_i$ gives rise to the linear system of equations for $(b_0, \ldots, b_{d-1})$ given by the matrix

$$M = \left(\operatorname{coeff}\left(\operatorname{coeff}\left(s, x^i\right), b_j\right)\right)_{i,j=0,\ldots,d-1}$$

$$= \left(\operatorname{coeff}\left(\operatorname{rem}\left(x^{p\cdot j}, q, x\right), x^i\right)\right)_{i,j=0,\dots,d-1}$$

and the right-hand side $(0,1,0,\dots,0)^{\mathrm{tr}}$.

A unique solution of the problem in $\operatorname{Quot}\left(\left(R_{<x}\right)_{\sqrt{}}\right)[x]$ exists if and only if the determinant of M is a non-zero or, equivalently, if there is no linear dependence between $x^{0\cdot p}, \dots, x^{(d-1)\cdot p}$ modulo q. Assume that such a linear dependence exists, then

$$\sum_{i=0}^{d-1} c_i x^{i\cdot p} = s \cdot q$$

with $c_i \in \operatorname{Quot}\left(\left(R_{<x}\right)_{\sqrt{}}\right)$ and $s \in \operatorname{Quot}\left(\left(R_{<x}\right)_{\sqrt{}}\right)[x]$. Since the left-hand side is a polynomial in x^p, so is the right-hand side and there is t such that $t^p = s \cdot q$. However, q has a non-zero discriminant, thus all irreducible factors of q have exponent 1, which implies $q^{p-1} | s$. We conclude that $\deg_x(s \cdot q) \geq d + (p-1)\cdot d = p \cdot d > (d-1)\cdot p \geq \deg_x(\sum_{i=0}^{d-1} c_i x^{i\cdot p})$, a contradiction.

Since $\operatorname{disc}(q,x) \neq 0$ implies that our linear system of equations has a unique solution, it follows that $\det(M) = \frac{\operatorname{disc}(q,x)^a}{\operatorname{init}(q)^b}$ for some $a, b \in \mathbb{Z}_{\geq 0}$. Therefore, the b_i lie in $A^{-1}\left(\left(R_{<x}\right)_{\sqrt{}}\right)$ and the a_i can be obtained using Remark (3.60). □

Example 3.62. Consider $p = 5$, $q = yx^3 - yx^2 + 1$ with $x > y$. We want to compute the fifth root of x modulo q using Lemma (3.61). The ansatz from the proof results in the linear system

$$\begin{pmatrix} 1 & -\frac{1}{y} & \frac{-y^2+2}{y^3} \\ 0 & -\frac{1}{y} & \frac{-y^2-y-1}{y^3} \\ 0 & \frac{y-1}{y} & \frac{y^2-y+1}{y^2} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

with the unique solution

$$\frac{1}{(y+2)^2} \begin{pmatrix} -2y-2 \\ (y^2-y+1)y^2 \\ -(y-1)y^3 \end{pmatrix}.$$

The fifth root of x modulo q is thus

$$\begin{aligned} r &= \frac{\left(-y^{\frac{4}{5}} + y^{\frac{3}{5}}\right)x^2 + \left(y^{\frac{4}{5}} - y^{\frac{3}{5}} + y^{\frac{2}{5}}\right)x - \left(2y^{\frac{1}{5}} + 2\right)}{y^{\frac{2}{5}} - y^{\frac{1}{5}} - 1} \\ &= \frac{-\left(y^{\frac{1}{5}} - 1\right)y^{3/5}x^2 + \left(y^{2/5} - y^{\frac{1}{5}} + 1\right)y^{2/5}x - 2\left(y^{\frac{1}{5}} + 1\right)}{\left(y^{\frac{1}{5}} + 2\right)^2} \\ &= \frac{\left(y^{\frac{1}{5}} + 2\right)^3\left(-\left(y^{\frac{1}{5}} - 1\right)y^{3/5}x^2 + \left(y^{2/5} - y^{\frac{1}{5}} + 1\right)y^{2/5}x - 2\left(y^{\frac{1}{5}} + 1\right)\right)}{y+2}. \end{aligned}$$

Note that $y^{\frac{1}{5}}$ can only be simplified further if there is also a relation for y. ◁

It is apparent from the previous lemma and example that the p-th root r of x modulo q may have a denominator $d \in \left(R_{\sqrt{}}\right)_{<x}$. However, since this denominator originates from $\operatorname{disc}_x(q)$ and $\operatorname{init}(q)$, we can first substitute $x^{\frac{1}{p}} \mapsto r$ into any polynomial with roots f and then multiply by d to obtain an element in $f' \in R_{\sqrt{}}$ with $\operatorname{rdeg}_x(f') \leq 0$ such that the solutions of f and f' are the same.

Remark 3.63. Due to Lemma (3.61), for any system S, we can transform each polynomial with roots q into $\hat{q}$ such that

1. $\phi_{\mathbf{a}}(q) = 0$ if and only if $\phi_{\mathbf{a}}(\hat{q}) = 0$ for all $\mathbf{a} \in \mathcal{L}(S)$.

2. If $x \in \mathrm{ld}((S_T)^=)$, then $\mathrm{rdeg}_x(\hat{q}) \leq 0$.

Thus, we may without loss of generality assume $q \in R_{\sqrt{}}$ is a polynomial in the relevant variables used for reduction. In particular, Algorithms (3.17) and (3.22), as well as Proposition (3.18) and Remarks (3.19) and (3.21) apply. ◁

We use the following proposition, which is also stated in [LMW10, Prop. 4.1].

Proposition 3.64. *Let $q \in K[x]$ and denote by $q' \in K[x]$ the derivative of q with respect to x. There are polynomials $P_1, \ldots, P_k, Q \in K[x]$, unique up to units of K, such that*

1. $q = Q \prod_{i=1}^{k} P_i^i$,
2. $\gcd(P_i, P_i') = 1$ *for all* $i = 1, \ldots, k$,
3. $\gcd(P_i, P_j) = \gcd(P_i, Q) = 1$ *for all* $i \neq j$,
4. $Q' = 0$,
5. *If* $i \equiv 0 \mod p$ *then* $P_i = 1$.

The polynomial Q is the factor of q that makes square-freeness in positive characteristic more difficult. Since $Q' = 0$, we get

$$q' = Q' \prod_{i=1}^{k} P_i^i + Q \sum_{i=1}^{k} \left(P_i^{i-1} \prod_{\substack{j=1,\ldots,k \\ j \neq i}} P_j^j \right) = Q \prod_{i=1}^{n} P_i^{i-1} \sum_{i=1}^{k} P_i$$

which implies $\frac{q}{\gcd(q,q')} = \prod_{i=1}^{k} P_i$. However, the square-free part of q is $\widetilde{Q} \prod_{i=1}^{k} P_i$ where $\widetilde{Q}$ is the square-free part of Q. Therefore, after applying the same method that we used in characteristic 0, we need to find Q and determine its square-free part.

Remark 3.65. We can use Algorithm (3.43) with a polynomial with roots $q \in \left(R_{<x\sqrt{}}\right)[x]$ with $\mathrm{ld}(p) = x$ to compute polynomials with roots $q_s, q_d \in \left(R_{<x\sqrt{}}\right)[x]$ and a system S such that

$$\phi_{<x,\mathbf{a}}(q_s) \sim \frac{\phi_{<x,\mathbf{a}}(q)}{\gcd\left(\phi_{<x,\mathbf{a}}(q), \phi_{<x,\mathbf{a}}(q')\right)} \sim \frac{\phi_{<x,\mathbf{a}}(q)}{\phi_{<x,\mathbf{a}}(q_d)}$$

for all $\mathbf{a} \in \mathcal{L}(S)$. Write $\phi_{<x,\mathbf{a}}(q) = Q^{\mathbf{a}} \prod_{i=1}^{k} \left(P_i^{\mathbf{a}}\right)^i$ as in Proposition (3.64). Then

$$\phi_{<x,\mathbf{a}}(q_d) \sim \gcd\left(\phi_{<x,\mathbf{a}}(q), \phi_{<x,\mathbf{a}}(q')\right) \sim Q^{\mathbf{a}} \prod_{i=2}^{k} \left(P_i^{\mathbf{a}}\right)^{i-1}$$

and $\phi_{<x,\mathbf{a}}(q_s) \sim \prod_{i=1}^{k} P_i^{\mathbf{a}}$ for all $\mathbf{a} \in \mathcal{L}(S)$. If we keep dividing $\phi_{<x,\mathbf{a}}(q_d)$ by $\phi_{<x,\mathbf{a}}(q_s)$ until their greatest common divisor is a constant, we obtain $Q^{\mathbf{a}}$. ◁

Example 3.66. Consider $K = \mathbb{F}_5$ and

$$q := x^{16} + x^{14} + 2x^{12} + 3x^{10} + 3x^6 + 3x^4 + x^2 + 4 = \left(x^2+2\right)^3 \left(x^2+3\right)^5 \in K[x] \ .$$

Then $\frac{\partial}{\partial x} q = x^{15} + 4x^{13} + 4x^{11} + 3x^5 + 2x^3 + 2x = \left(x^2+2\right)^2 x \left(x^2+3\right)^5$ and $\frac{q}{\frac{\partial}{\partial x} q} = x^2 + 2$. However, the square-free part of q is $(x^2+2)(x^2+3)$. ◁

The definition of the i-th square-free split and i-th conditional square-free part from Definition (3.36) does not produce the correct results in positive characteristic. We provide an new algorithm that extends the existing ResSplit algorithm to ensure square-freeness in this case.

Algorithm 3.67 (ResSplitSquareFreePosChar)**.** *Input: A system S with $(S_Q)^{=}_{<x} = \emptyset$ and a polynomial q with $\mathrm{ld}(q) = x$ and $\phi_{\mathbf{a}}(\mathrm{init}(q)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x})$.*
Output: A system S_1, a set of systems T and a polynomial r such that

a) $\{S_1 \cup \{q\}\} \cup T$ is a disjoint decomposition of $S \cup \{q\}$

b) $\phi_{<x,\mathbf{a}}(r)$ is square-free and $\deg_x(\phi_{<x,\mathbf{a}}(r)) = \deg_x(r)$ for all $\mathbf{a} \in \mathcal{L}((S_1)_{<x})$.

c) $\phi_{<x,\mathbf{a}}(r) = 0$ if and only if $\phi_{<x,\mathbf{a}}(q) = 0$ for all $\mathbf{a} \in \mathcal{L}((S_1)_{<x})$.

Algorithm:

1: ***if*** $\mathrm{ld}\left(\frac{\partial}{\partial x}q\right) < x$ ***then*** $\{Case\ 1\}$
2: ***if*** $\frac{\partial}{\partial x}q = 0$ ***then*** $\{Case\ 1a\}$
3: $S_1 \leftarrow S$
4: $q_d \leftarrow q$
5: $q_s \leftarrow 1$
6: $T_1 \leftarrow \emptyset$
7: ***else*** $\{Case\ 1b\}$
8: $(S_1, S_2) \leftarrow \mathsf{Split}\left(S, \frac{\partial}{\partial x}q\right)$
9: $q_d \leftarrow 1$
10: $q_s \leftarrow q$
11: $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
12: $T_1 \leftarrow \{S_2\}$
13: ***end if***
14: ***else*** $\{Case\ 2\}$
15: $(i, S_1, S_2) \leftarrow \mathsf{ResSplit}\left(S, q, \frac{\partial}{\partial x}q\right)$
16: ***if*** $i > 0$ ***then*** $\{Case\ 2a\}$
17: $q_d \leftarrow \mathrm{RRes}_i(q, \frac{\partial}{\partial x}q, x)$
18: $q_s \leftarrow \mathsf{pquo}\,(q, q_d, x)$
19: ***else*** $\{Case\ 2b\}$
20: $q_d \leftarrow 1$
21: $q_s \leftarrow q$
22: ***end if***
23: $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
24: $T_1 \leftarrow \{S_2\}$
25: ***end if***
26: $q_t \leftarrow q_s$
27: ***while*** $\mathrm{ld}(q_t) = x$ *and* $\mathrm{ld}(q_d) = x$ ***do***
28: $(i, S_1, S_2) \leftarrow \mathsf{ResSplit}\,(S_1, q_d, q_t)$
29: $q_t \leftarrow \mathrm{RRes}_i\,(q_d, q_t, x)$
30: $q_d \leftarrow \mathsf{pquo}\,(q_d, q_t, x)$
31: $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
32: $T_1 \leftarrow T_1 \cup \{S_2\}$
33: ***end while***
34: ***if*** $\mathrm{ld}(q_d) = x$ ***then***
35: $(S_1, T_2, q_d) = \mathsf{ResSplitSquareFreePosChar}(S_1, {q_d}^{\frac{1}{p}})$
36: ***return*** $S_1, T_1 \cup T_2, q_s \cdot q_d$
37: ***else***
38: ***return*** S_1, T_1, q_s
39: ***end if***

Example 3.68. Let $p = 2$, $S = (S_T, S_Q) = (\emptyset, \emptyset)$ and $q = (x^4 + bx^3 + ax^2 + 1)_{=}$ with $x > b > a$. Then $\frac{\partial}{\partial x}q = 3bx^2$ and ResSplit in line 15 returns $i = 0$, $S_1 = \left(\emptyset, \left\{(b^4)_{\neq}\right\}\right)$ and $S_2 = \left(\emptyset, \left\{(b^4)_{=}\right\}\right)$. We then set $q_d = 1$, $q_s = q_t = q$ and $T_1 = \left\{\left(\{q\}, \left\{(b^4)_{=}\right\}\right)\right\}$. Since $\mathrm{ld}(q_d) = 1$, we are done and return S_1, T_1, q_s. If we continue treating S_1 and q_s as in Algorithm (3.47), we eventually get the

simple system

$$\{q, b_{\neq}\} \ .$$

Now consider the next step. After further treatment, the system T_1 becomes $\hat{S} = (\{b_=\}, \emptyset)$ with q as above, but reduced modulo $\hat{S}$, i.e. $q = (x^4 + ax^2 + 1)_=$. We have $\frac{\partial}{\partial x} q = 0$ and thus set $\hat{S}_1 = \hat{S}$, $q_d = q$ and $q_s = 1$. We get to line 35 where we first compute $q_d{}^{\frac{1}{2}} = x^2 + a^{\frac{1}{2}} x + 1$. Since $a^{\frac{1}{2}}$ has the same roots as a, the recursive call to ResSplitSquareFreePosChar returns $\hat{S}_1 = (\{b_=\}, \{a_{\neq}\})$, $\hat{T}_2 = \left\{\left(\{b_=\}, \{a_=, (x^2 + a^{\frac{1}{2}} x + 1)_=\}\right)\right\}$ and $q_d = x^2 + a^{\frac{1}{2}} x + 1$. The system $\hat{S}_1$ can now be combined with q_d, while the system $\hat{T}_2$ needs to be treated further. ◁

We will see the end result of this computation in Example (3.70). However, we first prove that the ResSplitSquareFreePosChar algorithm is correct.

Proof of Correctness of Algorithm (3.67). ad a) All modifications to S_1 and T are done using the Split and ResSplit algorithms, which produces only disjoint decompositions as was proved before. Therefore, $\{S_1 \cup \{q\}\} \cup T$ is clearly a disjoint decomposition of $S \cup \{q\}$.

ad b) We first analyze the polynomial q_s in the main algorithm. In case 1a, q_s is defined as 1, which is always square-free. In case 1b, q_s is q, however, $\phi_{<x,\mathbf{a}}\left(\frac{\partial}{\partial x} q\right) \neq 0$ for all $\mathbf{a} \in \mathcal{L}\left((S_1)_{<x}\right)$, meaning that the derivative of $\phi_{\mathbf{a}}(q)$ is a constant and therefore q_s is square-free.

Case 2b has $q_s = q$ again and the ResSplit algorithm ensures that $\gcd(\phi_{<x,\mathbf{a}}(q), \phi_{<x,\mathbf{a}}\left(\frac{\partial}{\partial x} q\right))$ is non-zero and has degree 0 for all $\mathbf{a} \in \mathcal{L}\left((S_1)_{<x}\right)$. In Case 2a, $\deg_x(\phi_{<x,\mathbf{a}}(q_s)) = \deg_x(q_s) = \deg_x(q) - i$ and ResSplit guarantees that $\phi_{<x,\mathbf{a}} q_s$ is square-free for all $\mathbf{a} \in \mathcal{L}\left((S_1)_{<x}\right)$ as seen in Remark (3.65).

Now consider q_d. In lines 27-33, all common divisors of q_s and q_d are removed from q_d, in the sense that for all $\mathbf{a} \in \mathcal{L}((S_1)_{<x})$, $\phi_{<x,\mathbf{a}}(q_s)$ and $\phi_{<x,\mathbf{a}}(q_d)$ are coprime. By a recursion argument, q_d in line 35 has the same solutions as before. Therefore, condition b) holds.

ad c) In line 25, $q_s \cdot q_d = q$ for cases 1a, 1b and 2b. For case 2a, clearly $\phi_{<x,\mathbf{a}}(q_d) | \phi_{<x,\mathbf{a}}(q)$ and thus $\phi_{<x,\mathbf{a}}(q_s) \cdot \phi_{<x,\mathbf{a}}(q_d) = \phi_{<x,\mathbf{a}}(q)$ for all $\mathbf{a} \in \mathcal{L}((S_1)_{<x})$.

In each iteration of lines 27-33, for all $\in \mathcal{L}((S_1)_{<x})$, $\phi_{<x,\mathbf{a}}(q_t)$ is a divisor of $\phi_{<x,\mathbf{a}}(q_s)$ and thus only roots of $\phi_{<x,\mathbf{a}}(q_s)$ are removed from $\phi_{<x,\mathbf{a}}(q_d)$. Therefore, in line 33, $\phi_{<x,\mathbf{a}}(q)$ has the same roots as $\phi_{<x,\mathbf{a}}(q_s) \cdot \phi_{<x,\mathbf{a}}(q_d)$ and statement c) follows.

It remains to show that $q_d^{\frac{1}{p}}$ computed in line 35 is a polynomial in x, i.e. that q_d is a polynomial in x^p. In case 1a, this is obvious since $q = q_d$ and $\frac{\partial}{\partial x} q = 0$ and in cases 1b and 2b, $q_d = 1$ and thus $\mathrm{ld}(q_d) \neq x$. In case 2a, for all $\mathbf{a} \in \mathcal{L}((S_1)_{<x})$, $\gcd(\phi_{<x,\mathbf{a}}(q_s), \phi_{<x,\mathbf{a}}(q_d)) = 1$, $\phi_{<x,\mathbf{a}}(q_s) \sim \frac{\phi_{<x,\mathbf{a}}(q)}{\gcd(\phi_{<x,\mathbf{a}}(q), \phi_{<x,\mathbf{a}}(\frac{\partial}{\partial x} q))}$ and $q_d | q$, thus $\frac{\partial}{\partial x} q_d = 0$ due to Proposition (3.64). □

Replacing the ResSplitSquareFree algorithm with ResSplitSquareFreePosChar in lines 24 and 33 of Decompose yields an algorithm for Thomas decomposition in positive characteristic.

Remark 3.69. In Algorithm (3.47), replace line 24 with

$(S, S_3, p) \leftarrow$ ResSplitSquareFreePosChar (S, q); $P \leftarrow P \cup S_3$

and line 33 with

$(S, S_6, p) \leftarrow$ ResSplitSquareFreePosChar (S, q); $P \leftarrow P \cup S_6$.

Furthermore, whenever an equation $q_=$ or inequation $q_{\neq}$ with $\mathrm{ld}(q) = x_i$ and $\mathrm{rdeg}_{x_i}(q) > 0$ is inserted into S_Q, replace q with $q^{\left(p^{\mathrm{rdeg}_{x_i}(q)}\right)}$ such that q is a polynomial in its leader.

Whenever a polynomial contains the root $y^{\frac{1}{p}}$ and an equation for y exists in S_T, the method described in the proof of Lemma (3.61) should be applied to ensure condition (3.57)5.

This yields a modified Decompose algorithm that performs a Thomas decomposition in positive characteristic. The correctness of the algorithm follows from the original proof and from the output conditions of Algorithm (3.67). The proof of termination holds unmodified, since the new systems

we put into S_3 and S_6 above are $\prec_2$-smaller than the original system S, with $\prec_2$ as defined in (3.51). ◁

Example 3.70. Let $S = \left\{(x^4 + bx^3 + ax^2 + 1)_=\right\}$ with $a < b < x$ as in Example (3.68). In characteristic 2, as demonstrated in Example (3.68), a THOMAS decomposition of S is given by

$$\begin{aligned}&\left\{(x^4 + bx^3 + ax^2 + 1)_=, b_\neq\right\},\\ &\left\{(x^2 + a^{\frac{1}{2}}x + 1)_=, b_=, a_\neq\right\},\\ &\left\{(x + 1)_=, b_=, a_=\right\}\ ,\end{aligned}$$

while in characteristic 3, a THOMAS decomposition is as follows.

$$\begin{aligned}&\left\{\left(x^4 + bx^3 + ax^2 + 1\right)_=, \left(a^3b^2 + 2a^4 + 2a^2 + 2\right)_\neq, \left(a^3 + 2a\right)_\neq\right\},\\ &\left\{\left(x^4 + bx^3 + ax^2 + 1\right)_=, b_\neq, \left(a^2 + 2\right)_=\right\},\\ &\left\{\left(x^4 + bx^3 + 1\right)_=, a_=\right\},\\ &\left\{\left(\left(a^3 + 2a\right)x^3 + \left(2a^3 + 2a\right)bx^2 + \left(2a^2 + 1\right)x + 2a^2b\right)_=, \left(a^3b^2 + 2a^4 + 2a^2 + 2\right)_=, \left(a^3 + 2a\right)_\neq\right\},\\ &\left\{\left(x^2 + 2a\right)_=, b_=, \left(a^2 + 2\right)_=\right\}\end{aligned}$$

In any other characteristic, the decomposition is the same as in characteristic 0.

Note that the result in characteristic 2 contains $a^{\frac{1}{2}}$ in one system while all other systems contain no p-th roots of variables. However, such roots may have occurred during computation but were removed later using Lemma (3.61). ◁

If the ground field is neither algebraic over $\mathbb{F}_p$ nor algebraically closed, in general we cannot decompose a system into simple systems over the same field. Here is a very simple example.

Example 3.71. Let $K = \mathbb{F}_2(t)$ and $n = 1$, i.e. $R = \mathbb{F}_2(t)[x]_{\sqrt{}}$. Consider $S = \{(x^2 + t)_=\}$. This is not a simple system, since the polynomial $x^2 + t = (x + t^{\frac{1}{2}})^2$ is not square-free over $\overline{\mathbb{F}_2(t)}[x]$.

The equivalent simple system $S' = \left\{\left(x + t^{\frac{1}{2}}\right)_=\right\}$ is a system over $\mathbb{F}_2\left(t^{\frac{1}{2}}\right)[x] \supsetneqq \mathbb{F}_2(t)[x]$. ◁

In practice, this restriction is not problematic, since for every fixed system S, the decomposition only requires performing a finitely generated field extension.

We have to extend the notation from Definition (3.14) slightly.

Definition 3.72. Let K be a field and $R = K[x_1, \ldots, x_n]$. If $\mathrm{char}(K) = 0$, define

$$\mathcal{P}_K^n := \left\{ \bigcup_{i=1}^{k} \mathcal{L}(S_i) \middle| k \in \mathbb{N}, S_i \text{ is a polynomial system over } R, i = 1, \ldots, k \right\}\ .$$

If $\mathrm{char}(K) = p > 0$ where K is either algebraic over $\mathbb{F}_p$ or algebraically closed, define

$$\mathcal{P}_K^n := \left\{ \bigcup_{i=1}^{k} \mathcal{L}(S_i) \middle| k \in \mathbb{N}, S_i \text{ is a polynomial system with } p\text{-th roots over } R_{\sqrt{}}, i = 1, \ldots, k \right\}\ .$$

Otherwise, define $\mathcal{P}_K^n := \mathcal{P}_{\overline{K}}^n$ where $\overline{K}$ is the algebraic closure of K. Furthermore, let $\mathcal{P}_K := \left(\mathcal{P}_K^i\right)_{i=0,\ldots,\infty}$.

If the field is known from the context, we write $\mathcal{P}^n$ for $\mathcal{P}_K^n$ and $\mathcal{P}$ for $\mathcal{P}_K$. ◁

Note that if $K \subsetneqq L$, the classes $\mathcal{P}_K$ and $\mathcal{P}_L$ differ. For example, let $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Then $\{\alpha\} \in \mathcal{P}_{\mathbb{F}_4}^1$, but $\{\alpha\} \notin \mathcal{P}_{\mathbb{F}_2}^1$, since $x + \alpha \in \mathbb{F}_4[x] \setminus \mathbb{F}_2[x]$. However, $\{\alpha, \alpha + 1\} \in \mathcal{P}_{\mathbb{F}_2}^1$ since $(x + \alpha)(x + \alpha + 1) = x^2 + x + 1 \in \mathbb{F}_2[x]$. In particular $\mathcal{P}_{\mathbb{F}_2}^i \subsetneqq \mathcal{P}_{\mathbb{F}_4}^i$ for all $i \geq 0$.

Theorem 3.73. *Let K be an arbitrary field and $\overline{K}$ an algebraically closed field containing K. Then $\mathcal{P}$ is a well-behaved class of enumerable sets over $\overline{K}$.*

Proof. We distinguish three cases:

1. If $\mathrm{char}(K) = 0$, then every polynomial system over $K[x_1, \ldots, x_n]$ can be disjointly decomposed into simple systems over $K[x_1, \ldots, x_n]$.
2. If $\mathrm{char}(K) = p > 0$ and K is algebraic over $\mathbb{F}_p$, then every polynomial system with p-th roots over $K[x_1, \ldots, x_n]_{\sqrt{}}$ can be disjointly decomposed into simple systems over $K[x_1, \ldots, x_n]_{\sqrt{}}$.
3. If $\mathrm{char}(K) = p > 0$ and K is not algebraic over $\mathbb{F}_p$, then every polynomial system with p-th roots over $K[x_1, \ldots, x_n]_{\sqrt{}}$ can be disjointly decomposed into simple systems over $\overline{K}[x_1, \ldots, x_n]_{\sqrt{}}$.

Furthermore, if S is a such a simple system, $\mathcal{L}(S)$ is elementary $(\overline{K}, n)$-enumerable. The statement thus follows from the arguments in Lemma (3.15). □

It is now possible to compute counting polynomials of polynomial systems in positive characteristic.

From now on, when we talk about systems over $K[x_1, \ldots, x_n]$ and $\mathrm{char}(K) > 0$, we implicitly include systems with p-th roots over $K[x_1, \ldots, x_n]_{\sqrt{}}$.

3.4 Set Operations on the Solution Sets of Simple Systems

For any field K, we consider sets from the class $\mathcal{P}_K$ (see Definition (3.72)). Since for any $V, W \in \mathcal{P}_K^n$, also $V \cap W, V \cup W, \overline{K}^n \setminus V, V \setminus W \in \mathcal{P}_K^n$, we want to be able to express them in terms of simple systems. This section shows how to easily achieve that using our decomposition algorithm.

We consider disjoint families of simple systems and their solution sets, cf. Definition (3.13). Since the representation of a subset of $\overline{K}^n$ via such a family is not unique, we consider two families S and T equivalent if $\mathcal{L}(S) = \mathcal{L}(T)$. For ease of notation, we write $S = T$ in this case.

Remark 3.74. For $m \leq n$, let S be a simple system over $K[x_1, \ldots, x_m]$ and T be simple systems over $K[x_1, \ldots, x_n]$. Define the family $\mathsf{Intersect}(S, T)$ of simple systems obtained by decomposing $S \cup T$ into simple systems. Then $\mathcal{L}(\mathsf{Intersect}(S, T)) = \mathcal{L}\left(S \times \overline{K}^{n-m}\right) \cap \mathcal{L}(T)$.

If S, T are disjoint families of simple systems over $K[x_1, \ldots, x_m]$ and $K[x_1, \ldots, x_n]$, respectively, then we define

$$\mathsf{Intersect}(S, T) = \{\mathsf{Intersect}(s, t) | s \in S, t \in T\}$$

and again $\mathcal{L}(\mathsf{Intersect}(S, T)) = \mathcal{L}(S) \cap \mathcal{L}(T)$ holds.

Naturally, $\mathsf{Intersect}$ can be extended to an arbitrary finite number of arguments using the property $\mathsf{Intersect}(S_1, S_2, S_3, \ldots, S_k) = \mathsf{Intersect}(\mathsf{Intersect}(S_1, S_2), S_3, \ldots, S_k)$. ◁

Remark 3.75. Let S be a simple system over $K[x_1, \ldots, x_n]$ with $S^= = \{g_1, \ldots, g_s\}$ and $U = \prod_{u \in S^\neq} u$. Define the systems

$$C_i = \left\{(g_1)_=, \ldots, (g_{i-1})_=, (g_i)_\neq\right\}$$

for $i = 1, \ldots, s$ and

$$C_{s+1} = \{(g_1)_=, \ldots, (g_s)_=, U_=\} \ .$$

It is apparent that the sets C_i are pairwise disjoint. Denote by D_i a Thomas decompositions of C_i and by $\mathsf{Complement}(S)$ the concatenation $(D_1, \ldots, D_{s+1})$. Then $\mathsf{Complement}(S)$ is a disjoint family of simple systems and $\mathcal{L}(\mathsf{Complement}(S)) = \overline{K}^n \setminus \mathcal{L}(S)$.

If $S = (S_1, \ldots, S_k)$ is a disjoint family of simple systems, we have

$$\overline{K}^n \setminus \bigcup_{i=1}^{k} \mathcal{L}(S_i) = \bigcap_{i=1}^{k} \left(\overline{K}^n \setminus \mathcal{L}(S_i) \right)$$

and thus

$$\mathsf{Complement}\,(S) = \mathsf{Intersect}\,(\mathsf{Complement}\,(S_1), \ldots, \mathsf{Complement}\,(S_k)) \ .$$

Furthermore, define

$$\mathsf{Difference}\,(S,T) = \mathsf{Intersect}\,(S, \mathsf{Complement}\,(T)) \ .$$

Clearly $\mathcal{L}(\mathsf{Difference}(S,T)) = \mathcal{L}(S) \setminus (\mathcal{L}(S) \cap \mathcal{L}(T)) = \mathcal{L}(S) \setminus \mathcal{L}(T)$. ◁

Remark 3.76. For S, T disjoint families of simple systems over $K[x_1, \ldots, x_n]$, define

$$\mathrm{Union}\,(S,T) = (S, \mathsf{Difference}\,(T,S)) \ .$$

Furthermore, recursively define

$$\mathrm{Union}\,(S_1, S_2, S_3, \ldots, S_k) = \mathrm{Union}\,(\mathrm{Union}\,(S_1, S_2), S_3, \ldots, S_k) \ . \qquad \triangleleft$$

To conclude this section, we offer a simple method of testing whether two disjoint families of simple systems are equivalent, i.e. if they have the same solution set.

Proposition 3.77. *Let S, T be disjoint families of simple systems over $K[x_1, \ldots, x_n]$.*

1. *$\mathcal{L}(S) \subseteq \mathcal{L}(T)$ if and only if $c\,(S) = c\,(\mathsf{Intersect}\,(S,T))$.*
2. *$\mathcal{L}(S) = \mathcal{L}(T)$ if and only if $c(S) = c(T) = c\,(\mathsf{Intersect}\,(S,T))$.*

Proof. It holds that $\mathcal{L}\,(\mathsf{Intersect}\,(S,T)) = \mathcal{L}(S) \cap \mathcal{L}(T) \subseteq \mathcal{L}(S)$.

If $\mathcal{L}(S) \subseteq \mathcal{L}(T)$, then $\mathcal{L}(S) \cap \mathcal{L}(T) = \mathcal{L}(S)$ and thus $c\,(S) = c\,(\mathcal{L}(S)) = c\,(\mathcal{L}(S) \cap \mathcal{L}(T)) = c\,(\mathsf{Intersect}\,(S,T))$.

If on the other hand $c\,(S) = c\,(\mathsf{Intersect}\,(S,T))$, then $\mathcal{L}(S) = \mathcal{L}\,(\mathsf{Intersect}\,(S,T))$ according to Lemma (2.17)3. This implies $\mathcal{L}(S) \subseteq \mathcal{L}(T)$.

The second part is an immediate consequence of the first part. □

It is however false that $c(S) = c(T)$ implies $\mathcal{L}(S) = \mathcal{L}(T)$. For instance, the families $S = (\{y_=\})$ and $T = (\{x_{\neq}, y_=\}, \{x_=, (y-1)_=\})$ over $K[x,y]$ both have the counting polynomial $c(S) = c(T) = u$.

3.5 Comprehensive Decomposition and Counting Trees

In this section we will show how to compute a hereditarily disjoint decomposition and the counting tree as defined in section 2.4.

It is a consequence of Corollary (3.11) that for every simple system S over $K[x_1, \ldots, x_n]$ and every $1 \leq i \leq n$, $S_{<x_i}$ is a simple system over $K[x_1, \ldots, x_{i-1}]$. Furthermore, for every $\mathbf{a} \in \mathcal{L}(S_{<x_i})$, $\phi_{<x_i,\mathbf{a}}(S_{\geq x_i})$ is a simple system over $\overline{K}[x_i, \ldots, x_n]$, as seen in Corollary (3.12).

When we have two disjoint systems S_1 and S_2 with $(S_1)_{<x_i} = (S_2)_{<x_i}$ and a solution $\mathbf{a} \in \mathcal{L}((S_1)_{<x_i})$, then the counting polynomial of (S_1, S_2) can be computed as

$$\begin{aligned} & c\left((S_1)_{<x_i}\right) \cdot \left(c\left(\phi_{<x_i,\mathbf{a}}\left((S_1)_{\geq x_i}\right)\right) + c\left(\phi_{<x_i,\mathbf{a}}\left((S_2)_{\geq x_i}\right)\right)\right) \\ = \ & c\left((S_2)_{<x_i}\right) \cdot \left(c\left(\phi_{<x_i,\mathbf{a}}\left((S_1)_{\geq x_i}\right)\right) + c\left(\phi_{<x_i,\mathbf{a}}\left((S_2)_{\geq x_i}\right)\right)\right) \end{aligned}$$

In practice, we do not need to know the solution, since we can determine the counting polynomial of $\phi_{<x_i,\mathbf{a}}\left((S_j)_{\geq x_i}\right)$ from $(S_j)_{\geq x_i}$ only.

Using this idea, we can define a set of parameters $\{x_1,\ldots,x_{i-1}\}$ and a set of variables $\{x_i,\ldots,x_n\}$ and determine the structure of the solution set for different parameter values. However, a THOMAS decomposition is not sufficient for this task, as the following example demonstrates.

Example 3.78. A THOMAS decomposition of $S=\left\{\left(y\left(x^2-a\right)\right)_=\right\}$ w.r.t. $a<y<x$ is given by

$$(S_1,S_2,S_3)=\left(\left\{\left(x^2-a\right)_=,y_\neq,a_\neq\right\},\{x_=,y_\neq,a_=\},\{y_=\}\right)\ .$$

However, the projection onto the first component

$$\left((S_1)_{<y},(S_2)_{<y},(S_3)_{<y}\right)=(\{a_\neq\},\{a_=\},\{\})$$

is not disjoint. Therefore, we cannot consider a as a parameter. Now consider the following decomposition instead:

$$(T_1,T_2,T_3,T_4)=\left(\left\{\left(x^2-a\right)_=,y_\neq,a_\neq\right\},\{y_=,a_\neq\},\{x_=,y_\neq,a_=\},\{y_=,a_=\}\right)\ .$$

The projection onto the first component is

$$\left((T_1)_{<y},(T_2)_{<y},(T_3)_{<y},(T_4)_{<y}\right)=(\{a_\neq\},\{a_\neq\},\{a_=\},\{a_=\})\ .$$

You see that for each pair of systems P_1,P_2 in the projection, either $\mathcal{L}(P_1)=\mathcal{L}(P_2)$ or $\mathcal{L}(P_1)\cap\mathcal{L}(P_2)=\emptyset$. ◁

The previous example shows a simple example of a **comprehensive** decomposition. It can be interpreted as follows: For any value of a that fulfills $a\neq 0$, a THOMAS decomposition of S is given by $\left(\left\{\left(x^2-a\right)_=,y_\neq\right\},\{y_=,\}\right)$. For $a=0$, this is not a THOMAS decomposition, but $(\{x_=,y_\neq\},\{y_=\})$ is.

Definition 3.79. A family of simple systems $S=(S_1,\ldots,S_k)$ over $K[x_1,\ldots,x_n]$ is called $(x_1,\ldots,x_i)$-**comprehensive** if for any $1\leq j,l\leq n$ either

$$\mathcal{L}\left((S_j)_{\leq x_i}\right)=\mathcal{L}\left((S_l)_{\leq x_i}\right)$$

or

$$\mathcal{L}\left((S_j)_{\leq x_i}\right)\cap\mathcal{L}\left((S_l)_{\leq x_i}\right)=\emptyset$$

holds. In this case, we denote by $S_{\leq x_i}$ a subset of $((S_1)_{\leq x_i},\ldots,(S_n)_{\leq x_i})$ such that all systems in $S_{\leq x_i}$ are disjoint and $\mathcal{L}(S_{\leq x_i})=\bigcup_{j=1}^{k}\mathcal{L}\left((S_i)_{\leq x_i}\right)$. ◁

This concept of a comprehensive decomposition is partially inspired by [CGL+07]. We will now provide an algorithm to decompose any disjoint family of simple systems into a comprehensive family. For a given family $(S_1,\ldots,S_k)$ of polynomial systems, we consider the family $((S_1)_{\leq x_i},\ldots,(S_k)_{\leq x_i})$ and transform it into a disjoint family $(D_1,\ldots,D_l)$ such that for every i,j either D_i and $(S_j)_{\leq x_i}$ are disjoint or D_i is a subset of $(S_j)_{\leq x_i}$. In the latter case, we can then determine a system $C_{i,j}$ with $\mathcal{L}(C_{i,j})=\left(\mathcal{L}(D_i)\times\overline{K}^{n-i}\right)\cap\mathcal{L}(S_j)$. We will use systems of this form to construct a comprehensive family.

Algorithm 3.80 (Comprehensive)**.** *Input: A disjoint family $S=(S_1,\ldots,S_k)$ of simple systems, a number $1\leq i<n$.*
Output: A disjoint, $(x_1,\ldots,x_i)$-comprehensive family $T=\mathsf{Comprehensive}(S,i)$ of simple systems with $\mathcal{L}(S)=\mathcal{L}(T)$.
Algorithm:

1: $P \leftarrow \{s_{\leq x_i} | s \in S\}$
2: $P \leftarrow$ *a maximal subset* $P' \subseteq P$ *such that* $\mathcal{L}(s) \neq \mathcal{L}(t)\ \forall\ s,t \in P'$
3: ***if*** $\mathcal{L}(s) \cap \mathcal{L}(t) = \emptyset\ \forall\ s,t \in P$ ***then***
4: ***return*** S
5: ***end if***
6: *Find* j,l *with* $\mathcal{L}(P_j) \cap \mathcal{L}(P_l) \neq \emptyset$
7: $D_1 \leftarrow \mathsf{Difference}(P_j, P_l)$
8: $D_2 \leftarrow \mathsf{Difference}(P_l, P_j)$
9: $I \leftarrow \mathsf{Intersect}(P_l, P_j)$
10: $T_1 \leftarrow \{s \in S | s_{\leq x_i} = P_j\}$
11: $T_2 \leftarrow \{s \in S | s_{\leq x_i} = P_l\}$
12: $N_1 \leftarrow \bigcup_{s \in T_1, t \in D_1 \cup I} \mathsf{Intersect}(s,t)$
13: $N_2 \leftarrow \bigcup_{s \in T_2, t \in D_2 \cup I} \mathsf{Intersect}(s,t)$
14: ***return*** $\mathsf{Comprehensive}\left(\left(S \setminus (T_1 \cup T_2)\right) \cup (N_1 \cup N_2), i\right)$

For a simple system d over $K[x_1, \ldots, x_i]$ and a simple system s over $K[x_1, \ldots, x_n]$ with $\mathcal{L}(d) \subset \mathcal{L}(s_{\leq x_i})$, the operation $\mathsf{Intersect}(s, d)$ can be performed by simply replacing all terms with leader $\leq x_i$ in s with the corresponding terms from d and, if applicable, applying coefficient reduction to simplify the system. This means that the result only contains a single simple system s' with $s'_{\leq x_i} = d$. We will assume that this method is used in lines 12 and 13 of the above algorithm. Note that applying the usual $\mathsf{Intersect}$ algorithm yields the same result when used in combination with the $\mathsf{Decompose}$ algorithm described here, but at a much higher cost.

This algorithm is analogous to the method described in the proof of Theorem (2.27).

Proof of Correctness. The algorithm decomposes systems in S further and it is easy to see that no solutions are added or omitted. Furthermore, when the algorithm terminates in line 4, the output is $(x_1, \ldots, x_i)$-comprehensive by definition. □

Proof of Termination. The arguments from the proof of Theorem (2.27) and Lemma (2.15) apply. □

3.5.1 Hereditarily Disjoint Decomposition

The process of making a family of systems comprehensive can also be iterated easily.

Proposition 3.81. *Let* $S = (S_1, \ldots, S_k)$ *be a disjoint family of simple systems and* $1 \leq i_1 < i_2 < n$. *Then* $\mathsf{Comprehensive}\left(\mathsf{Comprehensive}\left(S, i_2\right), i_1\right)$ *is both* $(x_1, \ldots, x_{i_1})$*-comprehensive and* $(x_1, \ldots, x_{i_2})$*-comprehensive.*

Proof. It is obvious that the result is $(x_1, \ldots, x_{i_1})$-comprehensive. The arguments in the second part of the proof of Theorem (2.27) show that it is also $(x_1, \ldots, x_{i_2})$-comprehensive. □

Corollary 3.82. *Let* S *be a disjoint family of simple systems that is* $\left(x_1, \ldots, x_{i_j}\right)$*-comprehensive for* $j = 1, \ldots, r$ *with* $i_1 < \ldots < i_r$. *Then for any* $i_0 < i_1$, $\mathsf{Comprehensive}(S, i_0)$ *is still* $\left(x_1, \ldots, x_{i_j}\right)$*-comprehensive for* $j = 1, \ldots, r$.

The following definition is analogous to Definition (2.25).

Definition 3.83. We call a disjoint family S of simple systems over $K[x_1, \ldots, x_n]$ **hereditarily disjoint** if it is $(x_1, \ldots, x_i)$-comprehensive for all $1 \leq i < n$. ◁

We will now use hereditarily disjoint decompositions to construct the counting tree as defined in section 2.4.

Lemma 3.84. *Let* $(S_1, \ldots, S_k)$ *be a hereditarily disjoint family of simple systems. Then the* $\mathcal{L}(S_i), i = 1, \ldots, k$ *are hereditarily disjoint as defined in Definition (2.25).*

Proof. Since the S_i are simple systems, their solution sets are non-empty and elementary $\left(\overline{K}, n\right)$-enumerable. The decomposition is hereditarily disjoint, thus

$$\{\pi_{n,l}\left(\mathcal{L}\left(S_i\right)\right) | i = 1, \ldots, k\} = \left\{\mathcal{L}\left(\left(S_i\right)_{\leq x_l}\right) \middle| i = 1, \ldots, k\right\}$$

is a set of pairwise disjoint elementary $\left(\overline{K}, l\right)$-enumerable sets for all $l = 1, \ldots, n$. □

The previous lemma shows that a hereditarily disjoint decomposition of a polynomial system S yields a pre-fibration tree and thus the counting tree of $\mathcal{L}(S)$.

Definition 3.85. Let S be a polynomial system over K. The counting tree of S is defined as the counting tree of $\mathcal{L}(S)$. ◁

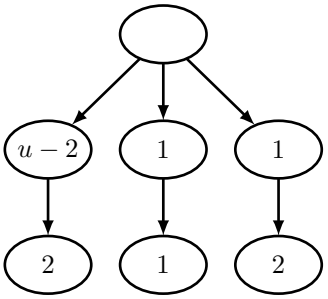
Example 3.86. Consider the system

$$S = \left\{\left(\left(x-1\right)\left(y+x^2-1\right)\left(x^2-y-1\right)\right)_=, \left(\left(y-1\right)\left(y+x^2-1\right)\left(x^2-y-1\right)\right)_=\right\}$$

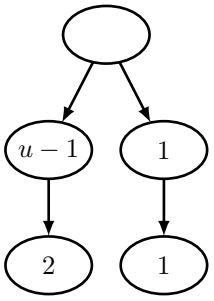
over $\mathbb{Q}[x, y]$ with $x < y$. A hereditarily disjoint decomposition into simple systems is given by

$$(S_1, S_2, S_3) = \left(\left\{\left(y^2-x^4+2x^2-1\right)_=, \left(x^2-1\right)_{\neq}\right\}, \{y_=, (x+1)_=\}, \left\{\left(y^2-y\right)_=, (x-1)_=\right\}\right)$$

The following pre-counting tree of S corresponds to this decomposition:



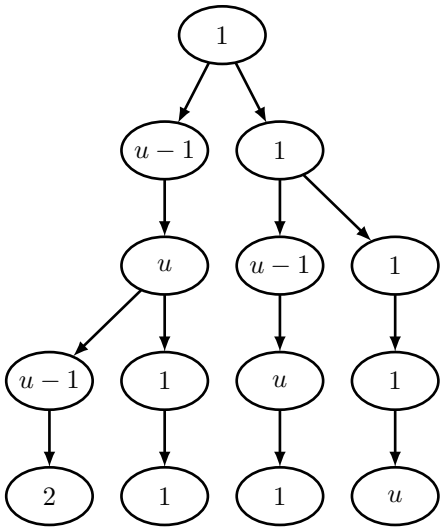
However, this is not a counting tree. In fact the counting tree of S is as follows:



The corresponding decomposition of $\mathcal{L}(S)$ into elementary $(\mathbb{C}, 2)$-enumerable sets is $(\mathcal{L}(S_1) \cup \mathcal{L}(S_3), \mathcal{L}(S_2))$. However, there is no polynomial system T over $\mathbb{Q}[x, y]$ or even $\mathbb{C}[x, y]$ such that $\mathcal{L}(T) = \mathcal{L}(S_1) \cup \mathcal{L}(S_3)$. ◁

To conclude this section, we now use a well-known example to demonstrate what information the counting tree contains about the structure of a solution set.

Example 3.87. Consider the system $\left\{\left(ax^2+bx+c\right)_=\right\}$ over $\mathbb{Q}[a, b, c, x]$ with $a < b < c < x$. We can visualize the counting tree as follows:



In section 3.7 we will show how this counting tree can be computed using our implementation of the THOMAS decomposition. We now interpret the four paths from the root to a leaf.

For all but one value for a and an arbitrary value for b, there are two possibilities. For all but one value for c, there are two values for x such that the equation is solved. For the one remaining value for c, there is one value for x that solves the equation.

Consider the one remaining value for a, which offers two possibilities. For all but one value for b and arbitrary c, there is one value for x that solves the equation. For the one remaining value for b, there is one value for c such that an arbitrary value for x solves the equation.

In all remaining cases, there is no solution. The counting tree does not show the exact values for a, b, c and x, but only their number. ◁

We already gave further examples in the introduction of section 2.4 and in Example (2.38).

3.6 Projection

Given a disjoint family of simple systems S over $K[x_1, \ldots, x_n]$ and $m < n$, an x_m-comprehensive decomposition provides a way to compute a family of simple systems P over $K[x_1, \ldots, x_m]$ such that $\pi_{n,m}(\mathcal{L}(S)) = \mathcal{L}(P)$. In particular, one needs to compute $(\mathsf{Comprehensive}(S, m))_{\leq x_m}$. However, the Comprehensive algorithm computes intersections in lines 12–13 that are unnecessary for computing the projection. Therefore, we present the following simplified method.

In order to make two sets M, N disjoint, it only uses the two sets M and $N \setminus (M \cap N)$ instead of computing the three sets $M \setminus (M \cap N)$, $N \setminus (M \cap N)$ and $M \cap N$.

Algorithm 3.88 (Project)**.** *Input: A disjoint family $S = (S_1, \ldots, S_k)$ of simple systems over $K[x_1, \ldots, x_n]$, a number $1 \leq m < n$.*
Output: A disjoint family of simple systems P over $K[x_1, \ldots, x_m]$ with $\pi_{n,m}(\mathcal{L}(S)) = \mathcal{L}(P)$.
Algorithm:

1: $P \leftarrow \{s_{\leq x_m} | s \in S\}$
2: $P \leftarrow$ *a maximal subset* $P' \subseteq P$ *such that* $\mathcal{L}(s) \neq \mathcal{L}(t)\ \forall\ s, t \in P'$
3: ***if*** $\mathcal{L}(s) \cap \mathcal{L}(t) = \emptyset\ \forall\ s, t \in P$ ***then***
4: ***return*** S
5: ***end if***
6: *Find* j, l *with* $\mathcal{L}(P_j) \cap \mathcal{L}(P_l) \neq \emptyset$
7: $D \leftarrow \mathsf{Difference}(P_j, P_l)$
8: ***return*** $\mathsf{Project}\,((S \setminus P_j) \cup D, m)$

Given any polynomial system S, we define $\mathsf{Project}(S, k) := \mathsf{Project}(\mathsf{Decompose}(S), k)$.

3.7 Implementation

The algorithms described here have been implemented and are available in the AlgebraicThomas package for MAPLE 11 and newer, cf. [BLH14]. In this section, we will demonstrate the capabilities of this package and explain in detail how to use it.

```
> restart:
> with(AlgebraicThomas):
```

We define a list of equations and possibly inequations.

```
> L := [ a*x^2 + b*x + c = 0 ];
```

$$L := [ax^2 + bx + c = 0]$$

In this example, we only entered one equation and no inequations. For equations, we can omit the suffix '$=\mathbf{0}$'.

```
> L := [ a*x^2 + b*x + c ];
```

$$L := [ax^2 + bx + c]$$

The ring is defined by giving a list of variables in decreasing order. This convention is consistent with other programs in MAPLE, but the order is reversed compared to the notation in this thesis.

```
> v := [x,c,b,a];
```

$$v := [x, c, b, a]$$

This defines the ring $\mathbb{Q}[a, b, c, x]$ since the characteristic is set to 0 by default. If we include unknowns $(t_1, \ldots, t_l)$ in the input that are not listed as variables, then $\mathbb{Q}(t_1, \ldots, t_l)[a, b, c, x]$ is used instead. The following command computes a THOMAS decomposition, cf. Algorithm (3.47):

```
> S := AlgebraicThomasDecomposition(L,v):
> printSystem(S, pretty=true);
```

$$[ax^2 + bx + c = 0, 4\,ca - b^2 \neq 0, a \neq 0]$$

$$[2\,xa + b = 0, 4\,ca - b^2 = 0, a \neq 0]$$

$$[bx + c = 0, b \neq 0, a = 0]$$

$$[c = 0, b = 0, a = 0]$$

We can display the counting polynomial of the result.

```
> countingPolynomial(S);
```

$$2\,u^3 - 2\,u^2 + u$$

We can also display the counting polynomials of the individual simple systems.

```
> countingPolynomials(S);
```

$$[[(2\,u - 2)\,u\,(u - 1)\,, u\,(u - 1)\,, u\,(u - 1)\,, u], 2\,u^3 - 2\,u^2 + u]$$

The counting tree shown in Example (3.87) can now be computed as follows:

```
> CountingTree(S);
```

$$[[u - 1, [[u, [[u - 1, [2]], [1, [1]]]]], [1, [[u - 1, [[u, [1]]]], [1, [[1, [u]]]]]]]$$

We want to project onto $\mathbb{Q}[a, b, c]$ in order to determine all parameters (a, b, c) such that the system has a solution, cf. Algorithm (3.88).

```
> Sp := Project(S, 3):
> printSystem(Sp, pretty=true);
```

$$[4\,ca - b^2 \neq 0, a \neq 0]$$

$$[b \neq 0, a = 0]$$

$$[4\,ca - b^2 = 0, a \neq 0]$$

$$[c = 0, b = 0, a = 0]$$

```
> countingPolynomial(Sp);
```

$$u^3 - u + 1$$

By computing the complement, we can determine when there is no solution, cf. Remark (3.75)..

```
> Complement(Sp);
> countingPolynomial(%);
```

$$[[c \neq 0, b = 0, a = 0]]$$

$$u - 1$$

Using comprehensive decomposition, we can even determine how many solutions the equation has depending on the parameters, cf. Algorithm (3.80).

```
> Sc := Comprehensive(S,3):
> printSystem(groupCounting(Sc),pretty=true);
```

$$[[[4\,ca - b^2 \neq 0, a \neq 0]], 2]$$

$$[[[4\,ca - b^2 = 0, a \neq 0], [b \neq 0, a = 0]], 1]$$

$$[[[c = 0, b = 0, a = 0]], u]$$

By changing the characteristic to 2, we can consider the same system as a system over $\mathbb{F}_2[a, b, c, x]$.

```
> AlgebraicThomasOptions("characteristic", 2);
> S_c2 := AlgebraicThomasDecomposition(L,v):
> printSystem(S_c2, pretty=true);
```

$$[ax^2 + bx + c = 0, b \neq 0, a \neq 0]$$

$$[\sqrt{a}x + \sqrt{c} = 0, b = 0, a \neq 0]$$

$$[bx + c = 0, b \neq 0, a = 0]$$

$$[c = 0, b = 0, a = 0]$$

Information about the characteristic is saved within the system, thus we can safely change the setting back to 0. More options can be set to influence the computation, please consult the help pages of the package for details.

```
> AlgebraicThomasOptions("characteristic", 0);
> countingPolynomial(S_c2);
```

$$2\,u^3 - 2\,u^2 + u$$

```
> Sc_c2 := Comprehensive(S_c2,3):
> printSystem(groupCounting(Sc_c2), pretty=true);
```

$$[[[b \neq 0, a \neq 0]], 2]$$

$$[[[b = 0, a \neq 0], [b \neq 0, a = 0]], 1]$$

$$[[[c = 0, b = 0, a = 0]], u]$$

To conclude this software demonstration, we demonstrate the computation of unions, intersections and set differences, cf. section 3.4.

```
> L1 := [ x^2+y^2-z^2-1 ];
```

$$L1 := [x^2 + y^2 - z^2 - 1]$$

```
> L2 := [ x^2-y^2+z^2+x ];
```

$$L2 := [x^2 - y^2 + z^2 + x]$$

```
> v := [x,y,z];
```

$$v := [x, y, z]$$

```
> AlgebraicThomasOptions("factor", false);
> S1 := AlgebraicThomasDecomposition(L1, v):
> S2 := AlgebraicThomasDecomposition(L2, v):
> printSystem(S1,pretty=true);
```

$$[x^2 + y^2 - z^2 - 1 = 0, y^2 - z^2 - 1 \neq 0, z^2 + 1 \neq 0]$$
$$[x^2 + y^2 = 0, y \neq 0, z^2 + 1 = 0]$$
$$[x = 0, y^2 - z^2 - 1 = 0, z^2 + 1 \neq 0]$$
$$[x = 0, y = 0, z^2 + 1 = 0]$$

```
> printSystem(S2,pretty=true);
```

$$[x^2 - y^2 + z^2 + x = 0, 4\,y^2 - 4\,z^2 + 1 \neq 0, 4\,z^2 - 1 \neq 0]$$
$$[4\,x^2 - 4\,y^2 + 4\,x + 1 = 0, y \neq 0, 4\,z^2 - 1 = 0]$$
$$[2\,x + 1 = 0, 4\,y^2 - 4\,z^2 + 1 = 0, 4\,z^2 - 1 \neq 0]$$
$$[2\,x + 1 = 0, y = 0, 4\,z^2 - 1 = 0]$$

These systems represent two surfaces in $\mathbb{C}^3$.

```
> countingPolynomial(S1);
```

$$2\,u^2 - 2\,u + 2$$

```
> countingPolynomial(S2);
```

$$2\,u^2 - 2\,u + 2$$

```
> S12u := SolUnion(S1, S2):
> countingPolynomial(S12u);
```

$$4\,u^2 - 8\,u + 7$$

This system represents their union, which is still a surface.

```
> S12i := SolIntersect(S1, S2):
> countingPolynomial(S12i);
```

$$4\,u - 3$$

Their intersection is a curve. We can also compute their set difference.

```
> S1mS2 := SolDifference(S1, S2):
> countingPolynomial(S1mS2);
```

$$2\,u^2 - 6\,u + 5$$

This package will be used again in later Examples.

Chapter 4

Transformations and Generic Positions

In Example (2.7) we saw that (K, n)-enumerability may change when applying certain bijections of K^n to a subset. For polynomial systems over $K[x_1, \ldots, x_n]$, Theorem (3.73) shows that they are always $\left(\overline{K}, n\right)$-enumerable. However, the counting polynomial may still change when applying bijections of $\overline{K}^n$. In this section, we will analyze the effect of linear transformations on counting polynomials and counting trees.

Let $R = \overline{K}[x_1, \ldots, x_n]$ if $\mathrm{char}(K) = 0$ and $R = \overline{K}[x_1, \ldots, x_n]_{\sqrt{}}$ otherwise.

Definition 4.1. Let $T \in \overline{K}^{n \times n}$ with $\det(T) \neq 0$. We call the map

$$R \to R : x_i \mapsto \sum_{j=1}^{n} T_{n-i+1, n-j+1} x_j$$

the **linear transformation** induced by T. For $p \in R$, we denote the transformed polynomial by p^T. ◁

Using the formula above instead of $x_i \mapsto \sum_{j=1}^{n} T_{i,j} x_j$ may seem confusing at this point, but will greatly simplify later considerations.

Remark 4.2. For $T_1, T_2 \in \overline{K}^{n \times n}$ and $p \in R$, it holds that $p^{T_1 T_2} = \left(p^{T_1}\right)^{T_2}$. ◁

When given a polynomial system S, the transformed system S^T is the system containing the equations $(p^T)_=$ for all $p_= \in S^=$ and the inequations $(p^T)_{\neq}$ for all $p_{\neq} \in S^{\neq}$. The following simple example will begin to demonstrate the effects of transformations on polynomial systems.

Example 4.3. Consider the system $S = \{(xy - 1)_=\}$ with $x < y$ and the matrix $T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. A transformed system is given by $S^T = \{(x^2 + xy - 1)_=\}$. We have the counting polynomials $c(S) = u - 1$ and $c(S^T) = 2u - 2$.

Now consider the set of invertible 2×2-matrices

$$\mathrm{GL}_2\left(\overline{K}\right) = \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \middle| a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2} \in \overline{K}, a_{1,1}a_{2,2} - a_{1,2}a_{2,1} \neq 0 \right\} .$$

For each $M \in \mathrm{GL}_2\left(\overline{K}\right)$, the system S^M has counting polynomial $u - 1$ if $a_{1,1}a_{2,1} = 0$ and $2u - 2$ otherwise. ◁

Definition 4.4. 1. Let S be a system over $K[x_1, \ldots, x_n]$. Let $L = K\left(a_{i,j} | i, j = 1, \ldots, n\right)$ and consider the matrix $T = (a_{i,j})_{i,j=1,\ldots,n} \in L^{n \times n}$. The system S^T is a system over $L[x_1, \ldots, x_n]$ and we call its counting polynomial and counting tree the **generic counting polynomial** and **generic counting tree** of S, respectively.

2. A system is **in generic position** if its counting tree is isomorphic to its generic counting tree. ◁

We are of course interested in the transformations defined over K or $\overline{K}$ instead of the larger field L. In the following proposition we will see that there are finitely many different positions and that we can describe the corresponding transformations as enumerable subsets of $\mathrm{GL}_n\left(\overline{K}\right)$.

Proposition 4.5. *Let S be a polynomial system over $K[x_1,\ldots,x_n]$ and consider the set $\mathcal{G}(S) = \left\{S^T \middle| T \in \mathrm{GL}_n\left(\overline{K}\right)\right\}$.*

1. *There are finitely many isomorphism classes of counting trees of systems in $\mathcal{G}(S)$.*

2. *For each isomorphism class of counting trees T, the subset*

$$\left\{g \in \mathrm{GL}_n\left(\overline{K}\right) \middle| \text{the counting tree of } S^g \text{ is in } T\right\} \subseteq \mathrm{GL}_n\left(\overline{K}\right)$$

is an element of $\mathcal{P}^{\left(n^2\right)}$, i.e. $\left(\overline{K}, n^2\right)$-enumerable.

Proof. Consider the polynomial ring $K\left[a_{i,j} | i,j = 1,\ldots,n\right][x_1,\ldots,x_n]$ with a ranking such that $a_{i,j} < x_k$ for all $i,j,k = 1,\ldots,n$. For $A = (a_{i,j})$, let D be a decomposition of S^A into simple systems that is both $(a_{i,j}|i,j=1,\ldots,n)$-comprehensive and $((a_{i,j}|i,j=1,\ldots,n),x_1,\ldots,x_k)$-comprehensive for $k = 1,\ldots,n-1$. Note that such a decomposition exists due to Proposition (3.81). Note that the order of the $a_{i,j}$ in the chosen ranking does not matter.

By construction, $D_{<x_1}$ is a disjoint family of simple systems over $K\left[a_{i,j}|i,j=1,\ldots,n\right]$. If we choose a fixed $G \in D_{<x_1}$, every solution of G can be interpreted as a matrix in $\mathrm{GL}_n\left(\overline{K}\right)$.

We claim that for two such matrices $g_1, g_2 \in \mathcal{L}(G)$, the systems S^{g_1} and S^{g_2} have the same counting tree. To prove that, consider $T_G = \{s \in D | s_{<x_1} = G\}$. According to Corollary (3.12), $\phi_{<x_1,\mathbf{a}}(s)$ is a simple system over $\overline{K}[x_1,\ldots,x_n]$ for all $\mathbf{a} \in \mathcal{L}(G)$ and all $s \in T_G$. In particular, this holds for the solutions $\mathbf{b}_1, \mathbf{b}_2$ that correspond to the matrices g_1, g_2. Since substituting these solutions into simple systems does not change leaders or main degrees, both $S^{g_1} = \phi_{<x_1,\mathbf{b}_1}(S^A)$ and $S^{g_2} = \phi_{<x_1,\mathbf{b}_2}(S^A)$ yield the same counting trees. These can immediately be read off the systems in T_G because $\phi_{<x_1,\mathbf{b}_1}(T_G)$ and $\phi_{<x_1,\mathbf{b}_2}(T_G)$ are hereditarily disjoint (cf. Lemma (3.84) and Theorem (2.35)). Since $D_{<x_1}$ is finite, this proves 1.

As noted before, $D_{<x_1}$ is a disjoint family of simple systems over $K\left[a_{i,j}|i,j=1,\ldots,n\right]$. The set from 2. is a finite union of solution sets of elements of $D_{<x_1}$ and therefore an element of $\mathcal{P}^{n^2}$. □

For a further analysis of different positions, we first need to know more about the counting polynomial of $\mathrm{GL}_n\left(\overline{K}\right)$. We will only choose projections such that the entries of the matrices are the components. We have certain degrees of freedom in choosing the exact order of the entries in the ranking.

Proposition 4.6. *For $k \leq n$, consider $R_{k,n} = K\left[a_{i,j}|i=1,\ldots,k, j=1,\ldots,n\right]$ and the matrix $T = (a_{i,j})_{i=1,\ldots,k,j=1,\ldots,n} \in R_{k,n}^{k\times n}$. Furthermore, choose a ranking on $R_{k,n}$ such that if $a_{i_1,j_1} < a_{i_2,j_2}$ for some $1 \leq i_1, i_2 \leq k$, $1 \leq j_1, j_2 \leq n$, then $a_{i_1,j_1'} < a_{i_2,j_2'}$ for all $j_1', j_2' = 1,\ldots,n$.*

Then the set

$$\mathcal{M}_{k,n} = \left\{\mathbf{a} = (a_{i,j}|i=1,\ldots,k,j=1,\ldots,n) \in \overline{K}^{n^2} \middle| \mathrm{rk}\left(\phi_{\mathbf{a}}(T)\right) = k\right\}$$

can be described using $\binom{n}{k}$ disjoint polynomial systems and has counting polynomial

$$\prod_{i=0}^{k-1} u^n - u^i \ .$$

Proof. Consider set $M = \left\{m_1, \ldots, m_{\binom{n}{k}}\right\}$ of the $k \times k$ minors of T. Then

$$\mathcal{M}_{k,n} = \biguplus_{i=1}^{\binom{n}{k}} \mathcal{L}\left(\{\det(m_i) \neq 0, \det(m_j) = 0 \text{ for all } j < i\}\right)$$

and thus the first statement holds.

In order to determine the counting polynomial, let $k > 1$ and $M \in \overline{K}^{k-1\times n}$ be a fixed matrix with rank $k-1$. Let $\{i_1, \ldots, i_n\} = \{1, \ldots, n\}$ and consider

$$\overline{M} = \begin{pmatrix} & M & \\ x_{i_1} & \cdots & x_{i_n} \end{pmatrix} \in \overline{K}[x_1, \ldots, x_n]^{k\times n}$$

with $x_1 < \ldots < x_n$. For ease of notation, we index the i_j-th column of M or $\overline{M}$ with j instead of i_j.

Write the determinant $\det_C(M) = \det\left(M_{|\underline{k-1}\times C}\right)$ for all $C \in \mathrm{Pot}_{k-1}(\underline{n})$ and $\det_C\left(\overline{M}\right) = \det\left(\overline{M}_{|\underline{k}\times C}\right)$ for all $C \in \mathrm{Pot}_k(\underline{n})$. Define the order $\prec$ on $\mathrm{Pot}_{k-1}(\underline{n})$ via $C \prec C'$ if and only if $\min(C \setminus C') < \min(C' \setminus C)$. Clearly $\prec$ is a strict total order.

Now let $\mathbf{a} \in \overline{K}^n$ and set $C = \min_{\prec}\{C' \in \mathrm{Pot}_{k-1}(\underline{n}) | \det_{C'}(M) \neq 0\}$. Then the matrix $\phi_{\mathbf{a}}\left(\overline{M}_{|\underline{k}\times C}\right)$ has rank $k-1$. For the matrix $\phi_{\mathbf{a}}\left(\overline{M}\right)$ to have rank $k-1$, all other columns must be linearly dependent on the columns C. Therefore $\mathrm{rk}\left(\phi_{\mathbf{a}}\left(\overline{M}\right)\right) = k-1$ if and only if $\phi_{\mathbf{a}}\left(\det_{C'}\left(\overline{M}\right)\right) = 0$ for all $C' \in \mathrm{Pot}_k(\underline{n})$ with $C \subseteq C'$.

Thus, consider the system

$$\left\{\det_{C'}\left(\overline{M}\right)_{=} \middle| C \subseteq C' \subseteq \underline{n}, |C'| = k\right\}$$

over $\overline{K}[x_1, \ldots, x_n]$. Assume $C' = C \cup \{i\}$ for some $i \notin C$ and write

$$\det_{C'}\left(\overline{M}\right) = \det_C(M)x_i + \sum_{j\in C} \det_{C'\setminus\{j\}}(M)x_j \ .$$

For each $j \in C$ with $i < j$ and thus $x_i < x_j$, we get $C' \setminus \{j\} \prec C$. Thus, by construction, $\det_{C'\setminus\{j\}}(M) = 0$ and therefore x_i is the leader of $\det_{C'}\left(\overline{M}\right)$. As a consequence, the initial of $\det_{C'}\left(\overline{M}\right)$ is $\det_C(M)$ which is non-zero.

In summary, this means that each of the variables $x_j, j \notin C$ is restricted with an equation of degree 1 and the $x_j, j \in C$ are free. Therefore,

$$c\left(\left\{\mathbf{a} \in \overline{K}^n \middle| \phi_{\mathbf{a}}\left(\mathrm{rk}\left(\overline{M}\right)\right) = k-1\right\}\right) = c\left(\left\{\det_{C'}\left(\overline{M}\right)_{=} \middle| C \subseteq C' \subseteq \underline{n}, |C'| = k\right\}\right) = u^{k-1}$$

and for its complement, the following holds:

$$c\left(\left\{\mathbf{a} \in \overline{K}^n \middle| \phi_{\mathbf{a}}\left(\mathrm{rk}\left(\overline{M}\right)\right) = k\right\}\right) = u^n - u^{k-1}$$

Since this formula is true for any $M \in \overline{K}^{k-1\times n}$, Proposition (2.39) implies that

$$c\left(\mathcal{M}_{k,n}\right) = c\left(\mathcal{M}_{k-1,n}\right) \cdot \left(u^n - u^{k-1}\right)$$

for $k > 1$. For $k = 1$, consider the counting polynomial $c\left(\left\{M \in \overline{K}^{1\times n} \middle| \mathrm{rk}(M) = 1\right\}\right) = c\left(\{\{0\}\}\right) = 1$. Thus, $c(\mathcal{M}_{1,n}) = u^n - 1$ and the statement holds with some restrictions on the ranking.

This proof implies that in the chosen ranking on $R_{k,n}$ we may change the order of the variables in each row and the order of the rows altogether without changing the resulting counting polynomial. □

Corollary 4.7. *Let $n \in \mathbb{N}$, define $R_{n,n}$ as in Proposition (4.6) and let $T = (a_{i,j})_{i,j=1,\dots,n}$. Choose a ranking on $R_{n,n}$ such that either*

1. *there are i_1, i_2, j_1, j_2 with $1 \leq i_1, i_2 \leq k, 1 \leq j_1, j_2 \leq n$ such that $a_{i_1,j_1} < a_{i_2,j_2}$ implies $a_{i_1,j_1'} < a_{i_2,j_2'}$ for all $j_1', j_2' = 1, \dots, n$*

or

2. *there are i_1, i_2, j_1, j_2 with $1 \leq i_1, i_2 \leq k, 1 \leq j_1, j_2 \leq n$ such that $a_{i_1,j_1} < a_{i_2,j_2}$ implies $a_{i_1',j_1} < a_{i_2',j_2}$ for all $i_1', i_2' = 1, \dots, n$.*

Then $c(\{\det(T)_{\neq}\}) = \prod_{i=0}^{n-1} u^n - u^i$.

We conjecture that the results of Proposition (4.6) and Corollary (4.7) are entirely independent of the ranking. Despite being unable to prove it, we have not found any counterexamples. Whenever we use the system from Corollary (4.7) below, we implicitly assume that the ranking used fulfills the conditions of (4.7).

Lemma 4.8. *Let S be a system of equations and inequations with $\mathcal{L}(S) \neq \emptyset$ and $T \in \mathrm{GL}_n\left(\overline{K}\right)$. Then $\mathcal{L}(S^T) \neq \emptyset$.*

Proof. Let $\mathrm{rev}((a_1, \dots, a_n)) = (a_n, \dots, a_1)$. If $\mathbf{a} = (a_1, \dots, a_n) \in \overline{K}^n$ is a solution of S, then $\mathrm{rev}\left(T^{-1}\,\mathrm{rev}(\mathbf{a})\right)$ is a solution of S^T. □

Theorem 4.9. *Let T, S be as in Definition (4.4). There is a family of simple systems G over $K[a_{i,j} | i, j = 1, \dots, n]$ such that $\deg(c(G)) = n^2$ and $S^{\phi_{\mathbf{a}}(T)}$ is in generic position if and only if $\mathbf{a} \in \mathcal{L}(G)$.*

Proof. Let D be as in the proof of Proposition (4.5) and let $G \subseteq D_{<x_1}$ be the set of systems that yield the generic counting tree.

Due to Lemma (4.8) and Corollary (4.7), we know that $\deg\left(c\left(D_{<x_1}\right)\right) = n^2$ and the leading coefficient of $c\left(D_{<x_1}\right)$ is 1. Since $D_{<x_1}$ is finite, there must be exactly one system $g_1 \in D_{<x_1}$ with $\deg(c(g_1)) = n^2$.

Note that g_1 only contains inequations. This means that when the decomposition into D is performed, each polynomial that occurs which only depends on $a_{i,j}$ is added as an inequation into g_1. For the polynomials with leaders $x_1, \dots, x_n$, this yields the same results as if the $a_{i,j}$ were assumed to be field elements. Therefore, the counting tree that corresponds to the solutions of g_1 is the generic counting tree, which implies $g_1 \in G$. Since $\deg(c(g_1)) = n^2$, it also holds that $\deg(c(G)) = n^2$. □

Example 4.10. Let $\mathrm{char}(K) = 0$ and consider the system $S = \{(x^2 + y^2 - 1)_=, (z - x + y)_=\}$ with $x > y > z$ and find all counting trees. Choose the ranking $a_{1,1} < a_{1,2} < a_{1,3} < a_{2,1} < a_{2,2} < a_{2,3} < a_{3,1} < a_{3,2} < a_{3,3}$ for the transformation. We get 5 different counting trees:

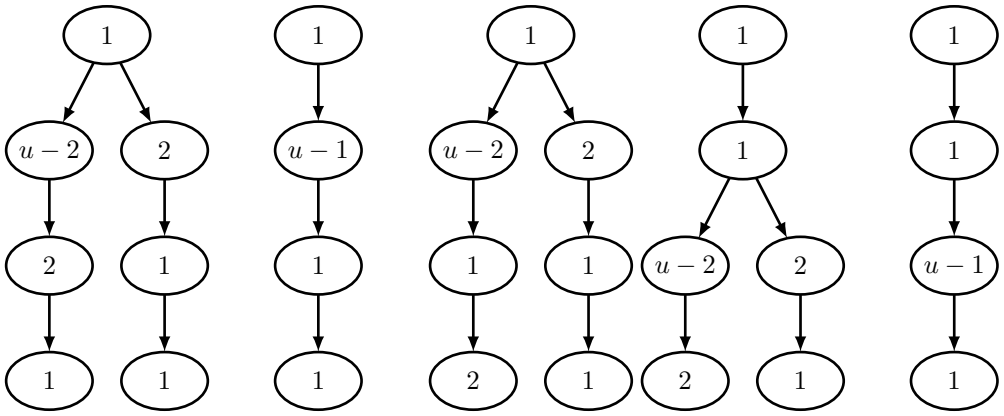
1. $c\left(\left\{g \in \mathrm{GL}_3\left(\overline{K}\right) \middle| S^g \text{ has counting tree } T_1\right\}\right) = c(G) = u^9 - 4u^8 + 6u^7 - 4u^6 + u^5$ where G is from Theorem (4.9) and T_1 is the generic counting tree. The counting polynomial is $c(S^g) = 2u - 2$ in this case.

2. $c\left(\left\{g \in \mathrm{GL}_3\left(\overline{K}\right) \middle| S^g \text{ has counting tree } T_2\right\}\right) = 2u^8 - 4u^7 + 4u^5 - 2u^4$, $c(S^g) = u - 1$.

3. $c\left(\left\{g \in \mathrm{GL}_3\left(\overline{K}\right) \middle| S^g \text{ has counting tree } T_3\right\}\right) = u^8 - 4u^7 + 6u^6 - 4u^5 + u^4$, $c(S^g) = 2u - 2$.

4. $c\left(\left\{g \in \mathrm{GL}_3\left(\overline{K}\right) \middle| S^g \text{ has counting tree } T_4\right\}\right) = u^7 - 4u^6 + 6u^5 - 4u^4 + u^3$, $c(S^g) = 2u - 2$.

5. $c\left(\left\{g \in \mathrm{GL}_3\left(\overline{K}\right) \middle| S^g \text{ has counting tree } T_5\right\}\right) = 2u^6 - 6u^5 + 6u^4 - 2u^3$, $c(S^g) = u - 1$.



(a) T_1 (b) T_2 (c) T_3 (d) T_4 (e) T_5

For example, one solution of case 5. is the matrix

$$h = \begin{pmatrix} 1 & 1 & 0 \\ \alpha & 0 & 0 \\ 1-\alpha & 1 & 1 \end{pmatrix}$$

where $\alpha \in \overline{K}$ fulfills $\alpha^2 + 1 = 0$. The system S^h has the THOMAS decomposition

$$\left(\left\{\left(2yx + y^2 - 1\right)_=, y_{\neq}, z_=\right\}\right) \ .$$

It is easy to see that the counting tree of this decomposition is T_5.

Note that S is in generic position, since its THOMAS decomposition

$$\left(\left\{(x-y-z)_=, \left(2y^2+2zy+z^2-1\right)_=, \left(z^2-2\right)_{\neq}\right\}, \left\{(2x-z)_=, (2y+z)_=, \left(z^2-2\right)_=\right\}\right)$$

admits the generic counting tree T_1.

This can be computed in MAPLE as follows.

```
> restart;
> with(AlgebraicThomas):
> L:= [ x^2+y^2-1, z-(x-y) ];
```

$$L := [x^2 + y^2 - 1, z - x + y]$$

```
> M := Matrix(3,symbol=a);
```

$$M := \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$$

```
> sl := [x,y,z]=~convert(M.<x,y,z>,list);
```

$$sl := [x = xa_{1,1} + ya_{1,2} + za_{1,3}, y = xa_{2,1} + ya_{2,2} + za_{2,3}, z = xa_{3,1} + ya_{3,2} + za_{3,3}]$$

```
> LG := [op(subs(sl,L)),LinearAlgebra[Determinant](M)<>0]:
> vg := [x,y,z,op(ListTools[Reverse]([op(indets(M))]))];
```

$$vg := [x, y, z, a_{3,3}, a_{3,2}, a_{3,1}, a_{2,3}, a_{2,2}, a_{2,1}, a_{1,3}, a_{1,2}, a_{1,1}]$$

```
> SG := AlgebraicThomasDecomposition(LG, vg):
> SG_T := ParametricCountingTree(SG, 9):
> nops(SG_T);
```

5

T_1 :

```
> countingPolynomial(SG_T[1][1]);
> SG_T[1][2];
> countingPolynomialFromCountingTree(SG_T[1][2]);
```

$$u^9 - 4\,u^8 + 6\,u^7 - 4\,u^6 + u^5$$
$$[[u-2,[[2,[1]]]],[2,[[1,[1]]]]]$$
$$-2 + 2\,u$$

T_2 :

```
> countingPolynomial(SG_T[2][1]);
> SG_T[2][2];
> countingPolynomialFromCountingTree(SG_T[2][2]);
```

$$2\,u^8 - 4\,u^7 + 4\,u^5 - 2\,u^4$$
$$[[u-1,[[1,[1]]]]]$$
$$u - 1$$

T_3 :

```
> countingPolynomial(SG_T[3][1]);
> SG_T[3][2];
> countingPolynomialFromCountingTree(SG_T[3][2]);
```

$$u^8 - 4\,u^7 + 6\,u^6 - 4\,u^5 + u^4$$
$$[[u-2,[[1,[2]]]],[2,[[1,[1]]]]]$$
$$-2 + 2\,u$$

T_4 :

```
> countingPolynomial(SG_T[4][1]);
> SG_T[4][2];
> countingPolynomialFromCountingTree(SG_T[4][2]);
```

$$u^7 - 4\,u^6 + 6\,u^5 - 4\,u^4 + u^3$$
$$[[1,[[u-2,[2]],[2,[1]]]]]$$
$$-2 + 2\,u$$

T_5 :

```
> countingPolynomial(SG_T[5][1]);
> SG_T[5][2];
> countingPolynomialFromCountingTree(SG_T[5][2]);
```

$$2\,u^6 - 6\,u^5 + 6\,u^4 - 2\,u^3$$
$$[[1,[[u-1,[1]]]]]$$
$$u - 1$$

◁

The previous computation can be simplified. In particular, we will now show that upper triangular matrices have no influence on the position. Therefore, the LU-decomposition of a matrix gives us a way to determine all positions by only considering lower triangular matrices and permutations.

Lemma 4.11. *Let S be a domain and $p \in S[x]$ with $d = \deg_x(p) > 1$ and $\frac{\partial}{\partial x}p \neq 0$. Then for every $s \in S$, $\operatorname{disc}_x(p) = \operatorname{disc}_x\left(p_{|x=x+s}\right)$.*

Proof. Let $q = p_{x=x+s}$. Interpret p and q as polynomials in $F = \overline{\operatorname{Quot}(S)}[x]$. Then there are $a, r_i \in F, i = 1, \ldots, d$ with $p = a\prod_{i=1}^{d} x - r_i$ and $q = a\prod_{i=1}^{d} x - (r_i - s)$. Then

$$\operatorname{disc}_x(p) = (-1)^{\frac{d(d-1)}{2}} a^{2(d-1)} \prod_{i=1,\ldots,d} \prod_{\substack{j=1,\ldots,d \\ j\neq i}} (r_i - r_j)$$

$$= (-1)^{\frac{d(d-1)}{2}} a^{2(d-1)} \prod_{i=1,\dots,d} \prod_{\substack{j=1,\dots,d \\ j\neq i}} ((r_i - s) - (r_j - s))$$

$$= \operatorname{disc}_x(q) \ .$$

Since $\operatorname{disc}_x(p)$ and $\operatorname{disc}_x(q)$ are polynomials in the coefficients of p and q, respectively, this is an equality in S. □

Proposition 4.12. *Let $g \in \mathrm{GL}_n\left(\overline{K}\right)$ be an upper triangular matrix.*

1. *If S is a system and $\operatorname{char}(K) = 0$, then S is simple if and only S^g is simple. If $\operatorname{char}(K) > 0$, then the process described in Lemma (3.61) reduces S to a simple system if and only if it reduces S^g to a simple system.*

2. *If S is any system, then the counting trees of S and S^g are the same.*

Proof. 1. First note that the inverse of an upper triangular matrix is again upper triangular. For an upper triangular matrix g, we have

$$R \to R : x_i \mapsto \sum_{j=1}^{n} g_{n-i+1,n-j+1} x_j = \sum_{j=1}^{i} g_{n-i+1,n-j+1} x_j$$

with $g_{i,i} \neq 0$ for $i = 1, \dots, n$. This implies that S is triangular if and only if S^g is triangular.

We also have $\operatorname{init}(p^g) = g_{i,i}^{d_i} \cdot \operatorname{init}(p)^g$ for all $p \in R$ with $\operatorname{ld}(p) = x_i$ and $\deg_{x_i}(p) = d_i$. Thus, S^g has non-vanishing initials if and only if S has them.

Since S is square-free, for each polynomial $p \in S$ with $\operatorname{ld}(p) = x_i$, we have that $\frac{\partial}{\partial x_i}(p) \neq 0$ and if $\operatorname{mdeg}(p) > 1$, $\phi_{<x_i,\mathbf{a}}(\operatorname{disc}_x(p)) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S_{<x_i})$. If g only affects variables smaller than x_i, then we clearly have $\operatorname{disc}_x(p)^g = \operatorname{disc}_x(p^g)$ and thus S^g is square-free again.

Now consider the transformation $x_i \mapsto r x_i + \sum_{j<i} a_j x_j$ and $x_j \mapsto x_j, j \neq i$ with $a_j \in \overline{K}, j < i$ and $r \in \overline{K} \setminus \{0\}$. First consider the case $a_j = 0, j < i$ and consider $\operatorname{disc}_{x_i}(p^g) = \operatorname{disc}_{x_i}\left(p_{|x_i = r x_i}\right)$. If $p = \sum_{j=0}^{d} c_j x_i^j$ with $c_j \in R_{<x_i}$, the discriminant of p^g is $\frac{\det(M)}{r^d c_d}$ where M is the matrix

$$\begin{pmatrix}
r^d c_d & r^{d-1} c_{d-1} & \cdots & r c_1 & c_0 & & \\
 & r^d c_d & r^{d-1} c_{d-1} & \cdots & r c_1 & c_0 & \\
 & \ddots & \ddots & \ddots & \ddots & \ddots & \\
 & & r^d c_d & r^{d-1} c_{d-1} & \cdots & r c_1 & c_0 \\
d r^d c_d & (d-1) r^{d-1} c_{d-1} & \cdots & r c_1 & & & \\
 & d r^d c_d & (d-1) r^{d-1} c_{d-1} & \cdots & r c_1 & & \\
 & & \ddots & \ddots & \ddots & \ddots & \\
 & & & d r^d c_d & (d-1) r^{d-1} c_{d-1} & \cdots & r c_1
\end{pmatrix} .$$

The determinant is given by

$$\sum_{\sigma \in S_{2d-1}} \operatorname{sign}(\sigma) \det_\sigma(M) := \sum_{\sigma \in S_{2d-1}} \operatorname{sign}(\sigma) \prod_{j=1}^{2d-1} M_{j,\sigma(j)} \ .$$

In this sum, the term $(d r^d c_d)^d \cdot c_0^{d-1} = d^d r^{\binom{d^2}{}} c_d^d c_0^{d-1}$ occurs, which has degree d^2 in r. Consider any two non-zero terms in this sum corresponding to two permutations σ_1 and σ_2 with $\sigma_2 = \sigma_1 \cdot \tau$ for $\tau \in S_{d(d-1)}$. Then $\det_{\sigma_1}(M) = \prod_{j=1}^{2d-1} M_{j,\sigma_1(j)}$ and

$$\det_{\sigma_2}(M) = \prod_{j=1}^{2d-1} M_{j,\sigma_2(j)}$$

$$= \prod_{j=1}^{2d-1} \begin{cases} M_{j,\sigma_1(j)} & \tau(j) = j \\ M_{j,\sigma_1(\tau(j))} & \tau(j) \neq j \end{cases}$$

If both M_{j,k_1} and M_{j,k_2} are non-zero, then $\deg_r(M_{j,k_1}) - \deg_r(M_{j,k_2}) = k_2 - k_1$, which is apparent by the structure of the matrix. This means that

$$\begin{aligned} \deg_r\left(\det_{\sigma_2}(M)\right) &= \deg_r\left(\det_{\sigma_1}(M)\right) + \sum_{\substack{j \in \underline{d(d-1)} \\ \tau(j) \neq j}} \left(\deg_r\left(M_{j,\sigma_1(\tau(j))}\right) - \deg_r\left(M_{j,\sigma_1(j)}\right)\right) \\ &= \deg_r\left(\det_{\sigma_1}(M)\right) + \sum_{\substack{j \in \underline{d(d-1)} \\ \tau(j) \neq j}} \sigma_1(j) - \sigma_1(\tau(j)) \\ &= \deg_r\left(\det_{\sigma_1}(M)\right) \ . \end{aligned}$$

Therefore, all the $\det_\sigma(M)$ have the same degree in r and thus $\operatorname{disc}_{x_i}(p^g) = r^{d(d-1)} \cdot g \operatorname{disc}_{x_i}(g)$. In conclusion, we may without loss of generality assume $r = 1$.

It remains to consider the transformation $x_i \mapsto x_i + P$ with $\operatorname{ld}(P) < x_i$. In this case, $\operatorname{disc}_x(p^g) = \operatorname{disc}_x(p) = \operatorname{disc}_x(p)^g$ due to Lemma (4.11).

If $\operatorname{char}(K) > 0$, for $p \in S$ with $\operatorname{ld}(p) = x_i$ and $\operatorname{rdeg}_{x_i}(p) \leq 0$, it holds that $\operatorname{rdeg}_{x_i}(p^g) \leq 0$ since the transformation cannot contain roots.

2. If D is a hereditarily disjoint decomposition of S into simple systems, then $D^g = \{s^g | s \in D\}$ is a hereditarily disjoint decomposition of S^g. Since applying g does not change the main degrees of equations or inequations and every system in D^g is still simple, the counting tree does not change. □

Remark 4.13. The previous proposition suggests that in positive characteristic, transforming a simple system with an upper triangular matrix may not yield a simple system immediately. As an example, consider $K = \mathbb{F}_5$ and the simple system $S = \left\{\left(x + y^{\frac{1}{5}}\right)_=, \left(z^3 + 1\right)_=\right\}$ with $x > y > z$. Let $g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ which yields the transformation $x \mapsto x, y \mapsto y + z, z \mapsto z$. Then the system $S^g = \left\{\left(x + y^{\frac{1}{5}} + z^{\frac{1}{5}}\right)_=, \left(z^3 + 1\right)_=\right\}$ is not simple, because it contains $z^{\frac{1}{5}}$ in a polynomial although there is an equation with leader z. However, it can be transformed to a simple system using Lemma (3.61), which results in

$$\left\{\left(x + y^{\frac{1}{5}} + 4z^2\right)_=, \left(z^3 + 1\right)_=\right\}$$

with the same solutions as S^g. ◁

In light of Proposition (4.12), we can improve the computation of all counting trees and their corresponding positions in $\mathrm{GL}_n\left(\overline{K}\right)$. Every invertible matrix $g \in \mathrm{GL}_n(K)$ can be written as $g = LPU$ where $L \in \mathrm{GL}_n(K)$ is a lower-triangular matrix with $L_{i,j} = 0$ if $i < j$ and $L_{i,i} = 1$, $P \in \mathrm{GL}_n(K)$ is a permutation matrix and $U \in \mathrm{GL}_n(K)$ is an upper-triangular matrix with $L_{i,j} = 0$ if $i > j$ and $L_{i,i} \neq 0$. Thus, we can obtain all positions by considering only the transformations $g = LP$ for permutation matrices P and lower-triangular matrices L with all diagonal entries equal to 1. Note that this is only possible due to $p^{LPU} = \left(p^{LP}\right)^U$ where U has no influence on the counting tree as seen above.

However, if we want to compute the counting polynomial of the set of matrices that yield a certain position, we need to know the counting polynomial of the set

$$\begin{aligned} \mathrm{GL}_n^P\left(\overline{K}\right) = \{M \in \mathrm{GL}_n(K) | M = LPU, L, U \in \mathrm{GL}_n\left(\overline{K}\right), \\ L \text{ lower-triangular}, U \text{ upper-triangular}, \operatorname{diag}(L) = (1, \ldots, 1)\} \subseteq \mathrm{GL}_n\left(\overline{K}\right) \end{aligned}$$

for every permutation matrix P. This has been analyzed to an extent in [Ple09b].

Remark 4.14. Following [Ple09b, Def. 2.5], we compute the counting polynomial of $\mathrm{GL}_n^P\left(\overline{K}\right)$ for a given permutation matrix P. Let $\Sigma(P)$ be the $n \times n$ matrix of the symbols 0, $*$ and $\bullet$ as follows. Put a $\bullet$ in every position of $\Sigma(P)$ where P has a 1. Then, for $i = 1, \ldots, n$, find the $\bullet$ in the i-th row. Fill in $*$'s in each position right of and below the $\bullet$ and fill in 0 in each position left of the $\bullet$ that has not already been assigned a $*$. Now, let m be the number of $*$'s in the matrix. Then $c\left(\mathrm{GL}_n^P\left(\overline{K}\right)\right) = (u-1)^n u^m$.

For example, let $n = 3$ and

$$(P_1, \ldots, P_6) = \Big(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \Big) .$$

Then we get

$$(\Sigma(P_1), \ldots, \Sigma(P_6)) = \Big(\begin{pmatrix} \bullet & * & * \\ * & \bullet & * \\ * & * & \bullet \end{pmatrix}, \begin{pmatrix} \bullet & * & * \\ * & 0 & \bullet \\ * & \bullet & * \end{pmatrix}, \begin{pmatrix} 0 & \bullet & * \\ \bullet & * & * \\ * & * & \bullet \end{pmatrix}, \begin{pmatrix} 0 & \bullet & * \\ 0 & * & \bullet \\ \bullet & * & * \end{pmatrix}, \begin{pmatrix} 0 & 0 & \bullet \\ \bullet & * & * \\ * & \bullet & * \end{pmatrix}, \begin{pmatrix} 0 & 0 & \bullet \\ 0 & \bullet & * \\ \bullet & * & * \end{pmatrix} \Big) .$$

Thus, the counting polynomials are $\left(c\left(\mathrm{GL}_n^{P^i}\left(\overline{K}\right)\right)\right)_{i=1,\ldots,6} = (u-1)^3 \cdot \left(u^6, u^5, u^5, u^4, u^4, u^3\right)$. The sum of these is in fact $c\left(\mathrm{GL}_n\left(\overline{K}\right)\right) = u^9 - u^8 - u^7 + u^5 + u^4 - u^3$.

Now let

$$\mathrm{GL}_n^{P,\mathrm{low}}\left(\overline{K}\right) = \{M \in \mathrm{GL}_n(K) | M = LP, L \in \mathrm{GL}_n\left(\overline{K}\right), \\ L \text{ lower-triangular}, \mathrm{diag}(L) = (1, \ldots, 1)\} \subseteq \mathrm{GL}_n^P\left(\overline{K}\right) .$$

Then $\frac{\mathrm{GL}_n^P\left(\overline{K}\right)}{\mathrm{GL}_n^{P,\mathrm{low}}\left(\overline{K}\right)} = (u-1)^n u^{m-\frac{n(n-1)}{2}}$. By multiplying this value with the counting polynomial of a subset $B \subseteq \mathrm{GL}_n^{P,\mathrm{low}}\left(\overline{K}\right)$, we get the counting polynomial of $B \cap \mathrm{GL}_n^P\left(\overline{K}\right)$. ◁

This remark also simplifies finding the generic counting polynomial and generic counting tree. We know from Theorem (4.9) that there is a set of matrices with counting polynomial of degree n^2 that yields the generic counting tree. Remark (4.14) states that the counting polynomial of $\mathrm{GL}_n^P\left(\overline{K}\right)$ has degree smaller than n^2 unless P is the identity. In order to get the generic position we can therefore use lower triangular matrices in Definition (4.4) and Theorem (4.9).

We reconsider Example (4.10) to simplify the computation.

Example 4.15. Let K, S and $T_1, \ldots, T_5$ be as in Example (4.10) and $P_i, i = 1, \ldots, 6$, $\mathrm{GL}_n^{P,\mathrm{low}}\left(\overline{K}\right)$ as in Remark (4.14). Define $c_{i,j} = c\left(\left\{g \in \mathrm{GL}_3^{P_i,\mathrm{low}}\left(\overline{K}\right) \middle| S^g \text{ has counting tree } T_j\right\}\right)$. Then

$$(c_{i,j}) = \begin{pmatrix} u^3 - 3u^2 + 4u - 2 & 2u^2 - 2u & u^2 - 3u + 2 & u - 2 & 2 \\ u^3 - 3u^2 + 2u & 2u^2 & u^2 - 2u & 0 & 0 \\ u^3 - 3u^2 + 2u & 2u^2 - 2u & u^2 - u & u & 0 \\ u^3 - 2u^2 & 2u^2 & 0 & 0 & 0 \\ u^3 - u^2 & 0 & u^2 & 0 & 0 \\ u^3 & 0 & 0 & 0 & 0 \end{pmatrix} .$$

Multiplying the row vector $(u-1)^3 \cdot \left(u^3, u^2, u^2, u, u, 1\right)$ with the previous matrix results in the same counting polynomials as in Example (4.10). However, the computation there took significantly longer. We demonstrate again how this is done in MAPLE.

```
> restart;
> with(AlgebraicThomas):
> with(LinearAlgebra):
> P := map[2](SubMatrix, IdentityMatrix(3), combinat[permute](3), 1..-1):
> v := [x,y,z];
```

$$v := [x, y, z]$$

```
> L := [ x^2+y^2-1, z-x+y ];
```

$$L := [x^2 + y^2 - 1, z - x + y]$$

```
> LM := Matrix(3, (i,j)->if i<j then 0 elif i=j then 1 else l[i,j] fi);
```

$$LM := \begin{bmatrix} 1 & 0 & 0 \\ l_{2,1} & 1 & 0 \\ l_{3,1} & l_{3,2} & 1 \end{bmatrix}$$

```
> vg := [op(v),op(indets(LM))];
```

$$vg := [x, y, z, l_{2,1}, l_{3,1}, l_{3,2}]$$

```
> sl := p->v=~convert(LM.p.Vector(v), list):
> S := map(p->
>    ParametricCountingTree(
>       AlgebraicThomasDecomposition(subs(sl(p), L), vg),
>       nops(indets(LM))
>    ), P):
> T := ListTools[MakeUnique](map(t->op(map(s->s[2], t)), S)):
> nops(T);
```

5

Using this computation, the counting trees are listed in a different order than before, thus we reorder them to match what we had in the previous example.

```
> T := T[[1,3,4,2,5]]:
> Xlow := Matrix(map(s->map(t->
>    countingPolynomial(map(op, map(a->if a[2]=t then a[1] fi, s))),
>    T), S));
```

$$Xlow := \begin{bmatrix} u^3 - 3\,u^2 + 4\,u - 2 & 2\,u^2 - 2\,u & u^2 - 3\,u + 2 & u - 2 & 2 \\ u^3 - 3\,u^2 + 2\,u & 2\,u^2 & u^2 - 2\,u & 0 & 0 \\ u^3 - 3\,u^2 + 2\,u & 2\,u^2 - 2\,u & u^2 - u & u & 0 \\ u^3 - 2\,u^2 & 2\,u^2 & 0 & 0 & 0 \\ u^3 - u^2 & 0 & u^2 & 0 & 0 \\ u^3 & 0 & 0 & 0 & 0 \end{bmatrix}$$

```
> w := (u-1)^3*<u^3|u^2|u^2|u|u|1>;
```

$$w := \begin{bmatrix} (u-1)^3\,u^3 & (u-1)^3\,u^2 & (u-1)^3\,u^2 & (u-1)^3\,u & (u-1)^3\,u & (u-1)^3 \end{bmatrix}$$

```
> T[1];
> expand(w.Column(Xlow,1));
```

$$[[u - 2, [[2, [1]]]], [2, [[1, [1]]]]]$$

$$u^9 - 4\,u^8 + 6\,u^7 - 4\,u^6 + u^5$$

```
> T[2];
> expand(w.Column(Xlow,2));
```

$$[[u-1,[[1,[1]]]]]$$
$$2\,u^8-4\,u^7+4\,u^5-2\,u^4$$

```
> T[3];
> expand(w.Column(Xlow,3));
```

$$[[u-2,[[1,[2]]]],[2,[[1,[1]]]]]$$
$$u^8-4\,u^7+6\,u^6-4\,u^5+u^4$$

```
> T[4];
> expand(w.Column(Xlow,4));
```

$$[[1,[[u-2,[2]],[2,[1]]]]]$$
$$u^7-4\,u^6+6\,u^5-4\,u^4+u^3$$

```
> T[5];
> expand(w.Column(Xlow,5));
```

$$[[1,[[u-1,[1]]]]]$$
$$2\,u^6-6\,u^5+6\,u^4-2\,u^3$$

These results are the same as in Example (4.10). ◁

Since the first case is called the generic position, we often call the last case a "special position".

Example 4.16. In Examples (4.10) and (4.15), consider the position that leads to the counting tree T_5. This position is given by the following set.

$$\left\{(t_{i,j})_{i,j=1,2,3}\in \mathrm{GL}_3\left(\overline{K}\right)\middle| t_{1,1}-t_{2,1}-t_{3,1}=0, t_{1,2}-t_{2,2}-t_{3,2}=0, 2t_{1,1}^2-2t_{1,1}t_{3,1}+t_{3,1}^2=0\right\}$$
$$=\left\{\begin{pmatrix}1&0&0\\1-l_{3,1}&1&0\\l_{3,1}&-1&1\end{pmatrix}\begin{pmatrix}u_{1,1}&u_{1,2}&u_{1,3}\\0&u_{2,2}&u_{2,3}\\0&0&u_{3,3}\end{pmatrix}\middle| u_{1,1}u_{2,2}u_{3,3}\neq 0, l_{3,1}^2-2l_{3,1}+2=0\right\}$$

From the last description, the counting polynomial $2(u-1)^3u^3$ computed in Example (4.15) is also apparent.

One matrix from that set is

$$M=\begin{pmatrix}\frac{1}{4}&1&0\\-\frac{1}{4}i&i&0\\\frac{1+i}{4}&1-i&1\end{pmatrix}$$

where $i\in\overline{K}$ such that $i^2+1=0$. Comparing the resulting system $S^M=\{(xy-1)_=, z_=\}$ with $S=\{(x^2+y^2-1)_=,(z-x+y)_=\}$ gives the impression that special positions yield less complicated systems.

A simple system representing $\mathcal{L}\left(S^M\right)$ is $\{(xy-1)_=, y_{\neq}, z_=\}$, which clearly yields T_5 as counting tree. ◁

The analysis of the determinant in Proposition (4.6) is another example for the importance of a non-generic position. In this particular case, the counting polynomial yields a well-known formula related to the general linear group, while the generic counting polynomial has no apparent meaning. We show both polynomials in the following computation.

```
> restart:
> with(AlgebraicThomas):
> with(LinearAlgebra):
> A := Matrix(2,symbol=a);
```

$$A:=\begin{bmatrix}a_{1,1}&a_{1,2}\\a_{2,1}&a_{2,2}\end{bmatrix}$$

```
> T := Matrix(4,(i,j)->if i<j then 0 elif i=j then 1 else t[i,j] fi);
```

$$T := \begin{bmatrix} 1 & 0 & 0 & 0 \\ t_{2,1} & 1 & 0 & 0 \\ t_{3,1} & t_{3,2} & 1 & 0 \\ t_{4,1} & t_{4,2} & t_{4,3} & 1 \end{bmatrix}$$

```
> v := [op(indets(A))];
```

$$v := [a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2}]$$

```
> s := v=~convert(T.Vector(v),list);
```

$$s := [a_{1,1} = a_{1,1}, a_{1,2} = a_{1,1}t_{2,1} + a_{1,2}, a_{2,1} = a_{1,1}t_{3,1} + a_{1,2}t_{3,2} + a_{2,1}, a_{2,2} = a_{1,1}t_{4,1} + a_{1,2}t_{4,2} + a_{2,1}t_{4,3} + a_{2,2}]$$

```
> L := [Determinant(A)<>0]:
> Lg := [subs(s,Determinant(A))<>0]:
> countingPolynomial(AlgebraicThomasDecomposition(L, v));
```

$$u^4 - u^3 - u^2 + u$$

```
> countingPolynomial(AlgebraicThomasDecomposition(Lg, v));
```

$$u^4 - 2\,u^3 + 2\,u^2 - 2\,u + 1$$

We will give a rigorous definition of a special position in section 5.2. Some of the systems considered in chapter 6 are in special position as well.

Chapter 5

Algebraic Varieties via Simple Systems

The set $\overline{K}^n$ is an affine algebraic variety, in particular, we identify it with the affine n-space $\mathbb{A}^n(\overline{K})$. The solution sets of polynomial systems can be considered as constructible subsets of $\overline{K}^n$. If the polynomial system only contains equations, the solution set is clearly an affine subvariety.

Note that the given embedding of such a constructible set into $\overline{K}^n$ determines a coordinate system and thus also determines the projections $\pi_i, i = 1, \ldots, n$. Therefore, a change of coordinates of $\overline{K}^n$ is a change of position in the sense of chapter 4.

Let $k \geq 1$ and $S = (S_1, \ldots, S_k)$ be a disjoint family of simple systems over $R = K[x_1, \ldots, x_n]$ if the characteristic of K is 0, and over $R_{\sqrt{}}$ otherwise.

5.1 The ideal of a polynomial system

To make a connection between affine algebraic geometry and polynomial systems, we assign an ideal to each simple system and consequently to each polynomial system. This ideal is in fact the vanishing ideal of the closure of $\mathcal{L}(S)$ and many of its properties have been considered in [Hub03a] and related literature.

Definition 5.1. For each i, let $U(S_i) := \prod_{q \in (S_i)^{\neq}} q$. Define the ideal of S_i as

$$I(S_i) := (\langle (S_i)^{=} \rangle : U(S_i)^{\infty}) \cap R \ .$$

Define the ideal of S as $I(S) := \bigcap_{i=1}^{k} I(S_i)$. ◁

Note that if the characteristic of K is 0, then the intersection with R is unnecessary. In positive characteristic, $(\langle (S_i)^{=} \rangle : U(S_i)^{\infty})$ is an ideal of a finitely generated sub-K-algebra of $R_{\sqrt{}}$ and needs to be intersected with R.

In particular, let $e_j = \max\left\{0, \mathrm{rdeg}_{x_j}(q) | q \in S_i, i = 1, \ldots, k\right\}$. Then, $I(S_i)$ and $I(S)$ can be computed over the noetherian ring $R_{\sqrt{}}^{(e_1, \ldots, e_n)}$ (cf. Remark (3.56)).

If we denote by $\mathcal{U}(S_i)$ the multiplicatively closed set defined by all the irreducible factors of the polynomials in $(S_i)^{\neq}$, then it is obvious that $I(S_i) = \mathcal{U}(S_i)^{-1}\langle (S_i)^{=} \rangle \cap R$.

Lemma 5.2. *Let R be a ring, $I \trianglelefteq R$ be an ideal and $u \in R$. If $s|u$, then for every $e \geq 0$, it holds that $I : u^{\infty} = I : (s^e u)^{\infty}$. In particular, for every $e > 0$, $I : u^{\infty} = I : (u^e)^{\infty}$.*

Proof. It holds that

$$I : u^{\infty} = \left\{ p \in R \middle| \exists d \in \mathbb{N} : u^d p \in I \right\}$$

and

$$I : (s^e u)^{\infty} = \left\{ p \in R \middle| \exists d \in \mathbb{N} : (s^e u)^d p \in I \right\} \ .$$

If $u^d p \in I$, then clearly $(s^e u)^d p = s^{ed} u^d p \in I$. Conversely, if $(s^e u)^d p \in I$ and since $s|u$, then $u^{(e+1)d} p = u^{ed} u^d p = \left(\frac{u}{s}\right)^{ed} s^{ed} u^d p = \left(\frac{u}{s}\right)^{ed} (s^e u)^d p \in I$. □

We need to consider a few subtle points that are trivial in characteristic zero, but important for positive characteristic.

Lemma 5.3. *In the notation of Definition (5.1), it holds that* $I(S_i) = (\langle (S_i)^= \rangle \cap R) : (U(S_i)^e)^\infty$ *with* $e > 0$ *such that* $U(S_i)^e \in R$.

Proof. In characteristic 0, this obviously holds for $e = 1$, so let the characteristic of K be positive.

$$\begin{aligned} I(S_i) &= \left\{ p \in R_{\sqrt{}} \;\middle|\; \exists d \in \mathbb{N} : U(S_i)^d p \in \langle (S_i)^= \rangle \right\} \cap R \\ &= \left\{ p \in R \;\middle|\; \exists d \in \mathbb{N} : U(S_i)^d p \in \langle (S_i)^= \rangle \right\} \end{aligned}$$

Due to the same arguments as in the proof of Lemma (5.2), we can take the e-th power of $U(S_i)$.

$$\begin{aligned} &= \left\{ p \in R \;\middle|\; \exists d \in \mathbb{N} : (U(S_i)^e)^d p \in \langle (S_i)^= \rangle \right\} \\ &= (\langle (S_i)^= \rangle \cap R) : (U(S_i)^e)^\infty \end{aligned}$$ □

If $\mathrm{char}(K) = 0$, for ease of notation, we set $R_{\sqrt{}} = R$ and $\mathrm{rdeg}(p) = 0$ for all $p \in R$.

Lemma 5.4. *Let* S *be a simple system and* $p \in R_{\sqrt{}}$ *with* $\mathrm{rdeg}_y(p) \leq 0$ *for all* $y \in \mathrm{ld}(S^=)$ *(we can transform any* $p \in R_{\sqrt{}}$ *into this form according to Remark (3.63)).*

If $\phi_{\mathbf{a}}(p) = 0$ *for all* $\mathbf{a} \in \mathcal{L}(S)$*, then there are* $q, r_g \in R_{\sqrt{}}$ *such that*

$$qp = \sum_{g \in S^=} r_g g \ . \tag{5.1}$$

In this situation, we can choose q *such that*

1. q *is a product of powers of initials of equations in* $S^=$

or

2. q *is a product of powers of elements from* $S^{\neq}$.

Proof. Since $\phi_{\mathbf{a}}(q) = 0$ for all $\mathbf{a} \in \mathcal{L}(S)$, Corollary (3.21) implies that $\mathsf{Reduce}(S, p) = 0$. Part 1. is apparent from the way Reduce works.

For part 2., take q from part 1. and note that $\phi_{\mathbf{a}}(q) \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S)$. We can use the techniques from Algorithm (3.24) to replace q by q' such that none of the variables in $\mathrm{ld}(S^=)$ appear in q' (changing the r_g on the right-hand-side of (5.1)). Since $\phi_{\mathbf{a}}(q') \neq 0$ for all $\mathbf{a} \in \mathcal{L}(S)$ and $y = \mathrm{ld}(q') \notin \mathrm{ld}(S^=)$, we now either have $y = 1$ or $S_y^{\neq} = S_y \neq \emptyset$ and the roots of $\phi_{<y,\mathbf{a}}(q')$ form a subset of the roots of $\phi_{<y,\mathbf{a}}(S_y)$ for all $\mathbf{a} \in \mathcal{L}(S_{<y})$. Therefore, there exist $t_1, t_2, s_g \in R_{<y}, e \in \mathbb{N}$ with $\phi_{<y,\mathbf{a}}(t_1) \neq 0 \neq \phi_{<y,\mathbf{a}}(t_2) \forall \mathbf{a} \in \mathcal{L}(S_{<y})$ such that $t_1 \cdot q' - \sum_{g \in S^=_{<y}} s_g g \mid t_2 \cdot (S_y)^e$. This gives another representation

$$q'' p = \sum_{g \in S^=} r'_g g \ ,$$

with $q'' | t_2 (S_y)^e$. Since t_2 has a leader smaller than y, we can iterate this process until we have $\overline{q}$ and $r \in \mathbb{N}$ such that $\overline{q} | U(S)^r$ and $\overline{q} p = \sum_{g \in S^=} \overline{r}_g g$. □

Theorem 5.5. *Let* $S = (S_1, \ldots, S_k)$ *be a disjoint family of simple systems.*

1. $\overline{\mathcal{L}(S)} = V(I(S))$*, where* $\overline{\ }$ *denotes the* Zariski*-closure.*

2. $I(S)$ *is a radical ideal.*

Proof. 1. Since $I(S) = \bigcap_{i=1}^{k} I(S_i)$ and $I(\mathcal{L}(S)) = \bigcap_{i=1}^{k} I(\mathcal{L}(S_i))$, we may assume $k = 1$, i.e. S is a single simple system. Define $G = \langle S^{=} \rangle \cap R$, then there is $e \in \mathbb{N}$ such that $V(S) = G : (U(S)^e)^\infty$, cf. Lemma (5.3).

Let $p \in I(S)$, i.e. there exists $d \in \mathbb{N}$ such that $(U(S)^e)^d p \in G$. Therefore, for every $\mathbf{a} \in \mathcal{L}(S)$ we have $\phi_{\mathbf{a}}(U(S)^d p) = 0$. Since $\phi_{\mathbf{a}}(U(S)) \neq 0$ also holds, we can conclude $\phi_{\mathbf{a}}(p) = 0$ and thus $p \in I(\mathcal{L}(S))$. This implies $\overline{\mathcal{L}(S)} \subseteq V(G : (U(S)^e)^\infty) = V(I(S))$.

Now let $p \in I(\mathcal{L}(S))$. If $p \in G$, then obviously $p \in G : (U(S)^e)^\infty$, so assume $p \notin G$. Since S is simple and $\phi_{\mathbf{a}}(p) = 0$ for all $\mathbf{a} \in \mathcal{L}(S)$, according to Corollary (3.21), it holds that $\mathsf{Reduce}(S, p) = 0$. Therefore, due to Lemma (5.4), there is a q with $q | U(S)^e$ such that $qp \in G$, implying $p \in I(S)$. This implies $V(I(S)) \subseteq \overline{\mathcal{L}(S)}$.

2. The proof of 1 shows that $I(S) = I(\mathcal{L}(S))$ and the latter is radical by definition. □

Note that in the proof of Theorem (5.5)1., the square-freeness property of simple systems plays a very subtle role, as it is necessary for Corollary (3.21).

The following lemma first appeared in [Rob12] for the case of characteristic 0. It is easy to see that it also holds in the case of positive characteristic.

Lemma 5.6. *Let S be a simple system. Denote by $L(S)$ the set of leading coefficients of all elements of $S^{=}$ and let $I'(S) := (\langle (S)^{=} \rangle : L(S)^\infty) \cap R$. Then $I(S) = I'(S)$.*

Proof. There are $e_1, e_2 > 0$ such that

$$I(S) = \left\{ p \in R \;\middle|\; \exists d \in \mathbb{N} : (U(S)^{e_1})^d p \in \langle (S)^{=} \rangle \right\}$$

and

$$I'(S) = \left\{ p \in R \;\middle|\; \exists d \in \mathbb{N} : (L(S)^{e_2})^d p \in \langle (S)^{=} \rangle \right\} .$$

If $(L(S)^{e_1})^d p \in \langle (S)^{=} \rangle$ then there is $d' \in \mathbb{N}$ such that $(U(S)^{e_2})^{d' d} p \in \langle (S)^{=} \rangle$ as has been demonstrated in the proof of Lemma (5.4), thus $I'(S) \subseteq I(S)$.

Conversely, if $p \in I(S)$, then (as seen in the proof of Theorem (5.5)) $\phi_{\mathbf{a}}(p) = 0$ for all $\mathbf{a} \in \mathcal{L}(S)$ and thus according to Corollary (3.21) $\mathsf{Reduce}(S, p) = 0$. Due to the way Reduce works, there are q, r_g such that $qp = \sum_{g \in S^{=}} r_g g$ where q divides a power of $L(S)$. This implies $I(S) \subseteq I'(S)$. □

From the previous lemma we also get the following corollary:

Corollary 5.7. *Let S be a simple system. The initials of the elements of $S^{=}$ are invertible in $\mathcal{U}(S_i)^{-1} R$.*

Finally, we get a connection between the counting polynomial and the dimension of its solution set as an affine algebraic variety.

Theorem 5.8. *Let $S = (S_1, \ldots, S_k)$ be a disjoint family of simple systems.*

1. $\dim(\mathcal{L}(S)) = \dim\left(\overline{\mathcal{L}(S)}\right) = \deg(c(S))$.
2. *If $k = 1$, then $\mathcal{L}(S)$ is unmixed dimensional (i.e. all its associated primes have the same dimension).*

Proof. Since the dimension of the disjoint union of sets is the maximum of their dimensions, we may assume that $k = 1$ and we only have a single simple system S. Taking the closure of $\mathcal{L}(S)$ does not change the dimension, thus the first equality holds.

Consider the set of free variables $v = \{x_1, \ldots, x_n\} \setminus \mathrm{ld}(S^{=})$. Clearly, $\deg(c(s)) = |v|$. Since $\mathcal{L}(S) \neq \emptyset$, we have $1 \notin I(S)$. Therefore and due to Lemma (5.6) and Corollary (5.7), the first part of the proof of [Hub03a, Thm. 4.4] is applicable to our case. This implies that the dimension of $V(I(S)) = \overline{\mathcal{L}(S)}$ is $|v|$ and that $I(S)$ is unmixed dimensional. □

Example 5.9. We demonstrate how to compute ideal and dimension the solution set of a polynomial system in MAPLE.

```
> restart:
> with(AlgebraicThomas):
> L := [ (z+1)*x^2+x*y, -y^2+z+1, y<>0 ];
```

$$L := [(z+1)\,x^2 + xy, -y^2 + z + 1, y \neq 0]$$

```
> v := [x,y,z];
```

$$v := [x, y, z]$$

```
> S := AlgebraicThomasDecomposition(L,v);
```

$$S := [[x = 0, y^2 - z - 1 = 0, z + 1 \neq 0], [(z+1)\,x + y = 0, y^2 - z - 1 = 0, z + 1 \neq 0]]$$

```
> countingPolynomial(S);
```

$$4\,u - 4$$

The following procedure computes the dimension of the solution set (cf. Theorem (5.8)).

```
> Dimension(S);
```

$$1$$

We can compute the ideal of a polynomial system (cf. Definition (5.1)) which gives the closure of the solution set (cf. Theorem (5.5)).

```
> Ideal(S);
```

$$[x^2y + x, y^2 - z - 1, x^2z + x^2 + xy]$$

```
> Sc := Closure(S):
> printSystem(Sc, pretty=true);
```

$$[x = 0, y^2 - z - 1 = 0, z + 1 \neq 0]$$

$$[x = 0, y = 0, z + 1 = 0]$$

$$[(z+1)\,x + y = 0, y^2 - z - 1 = 0, z + 1 \neq 0]$$

```
> countingPolynomial(Sc);
```

$$4\,u - 3$$

This shows that taking the closure only adds one additional point.

```
> SolDifference(Sc,S);
```

$$[[x = 0, y = 0, z + 1 = 0]]$$

This example also shows that it is not sufficient to omit the inequation to determine the closure.

```
> countingPolynomial(AlgebraicThomasDecomposition(L[1..-2],v));
```

$$5\,u - 4$$

◁

5.2 Transformations and Special Positions

Using the concept of closure, we can extend on chapter 4 and rigorously define a "special" position. We first need an order on the subsets of a given set V.

Definition 5.10. Let $V \in \mathcal{P}_K^n$. Define a partial order $\prec$ on a partition of V such that $M \prec N$ if and only if $M \subseteq \overline{N} \cap V$, i.e. if M is contained in the closure of N in V. ◁

In Proposition (4.5), we considered all isomorphism classes of counting trees of the transformations of a given system S and showed that the set of all matrices that give isomorphic counting trees is in $\mathcal{P}_K^{n^2}$. This yields a partition $P(S) \subseteq \mathcal{P}_K^{n^2}$ of $\mathrm{GL}_n\left(\overline{K}\right)$ where for each $g_1, g_2 \in \mathrm{GL}_n\left(\overline{K}\right)$, g_1 and g_2 are in the same class if and only if the counting trees of S^{g_1} and S^{g_2} are isomorphic. We call this partition the set of all positions of S.

Definition 5.11. A position $p \in P(S)$ is **special** if p is $\prec$-minimal in $P(S)$. ◁

If a position $p \in P(S)$ is ZARISKI-closed, there can be no other position p' with $p' \prec p$ since $P(S)$ is a partition. We again reconsider Example (4.10).

Example 5.12. Following the computation in Example (4.10), the following code finds the inclusions with respect to $\prec$.

```
> contains := (i,j)->evalb(
>    countingPolynomial(SG_T[j][1])
>     =
>    countingPolynomial(SolIntersect(SG_T[j][1], Closure(SG_T[i][1])))
> ):
> map(i->op(map(j->
>    if i<>j and contains(i,j) then [i,j] fi,
> [$1..5])), [$1..5]);
```

$$[[1,2],[1,3],[1,4],[1,5],[2,4],[2,5],[3,4],[3,5],[4,5]]$$

In particular, the position belonging to the counting tree T_5 is the only special position. ◁

As another example, we consider the determinant of a symmetric 2×2 matrix.

Example 5.13. We demonstrate the example in MAPLE.

```
> restart:
> with(AlgebraicThomas):
> with(LinearAlgebra):
> n:=2:
> A:=Matrix(n,symbol=a,shape=symmetric);
```

$$A := \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{bmatrix}$$

```
> v := [op(indets(A))];
```

$$v := [a_{1,1}, a_{1,2}, a_{2,2}]$$

```
> T := Matrix(n*(n+1)/2,symbol=t);
```

$$T := \begin{bmatrix} t_{1,1} & t_{1,2} & t_{1,3} \\ t_{2,1} & t_{2,2} & t_{2,3} \\ t_{3,1} & t_{3,2} & t_{3,3} \end{bmatrix}$$

```
> vt := [op(indets(T))];
```

$$vt := [t_{1,1}, t_{1,2}, t_{1,3}, t_{2,1}, t_{2,2}, t_{2,3}, t_{3,1}, t_{3,2}, t_{3,3}]$$

```
> s := convert(v=~T.Vector(v),list):
> L := [subs(s,Determinant(A)<>0),Determinant(T)<>0]:
> Sg := AlgebraicThomasDecomposition(L, [op(v),op(vt)]):
> Sgt := ParametricCountingTree(Sg,9):
> nops(Sgt);
```

4

There are four different possible counting trees. As in the previous example, we determine the special position.

```
> contains := (i,j)->evalb(
>    countingPolynomial(Sgt[j][1])
>     =
>    countingPolynomial(SolIntersect(Sgt[j][1], Closure(Sgt[i][1])))
> ):
```

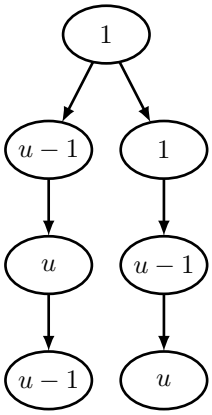
```
> map(i->op(map(j->
>    if i<>j and contains(i,j) then [i,j] fi,
> [$1..4])), [$1..4]);
```

$$[[1,4],[2,1],[2,3],[2,4],[3,4]]$$

The fourth system gives the only special position with the following counting tree.

```
> Sgt[4][2];
```

$$[[u-1,[[u,[u-1]]]],[1,[[u-1,[u]]]]]$$



Since there is only one special position, the set describing this position must be closed in the general linear group.

```
> Ti:=AlgebraicThomasDecomposition([Determinant(T)<>0],[op(indets(T))]):

> evalb(
> countingPolynomial(Sgt[4][1])
>    =
> countingPolynomial(SolIntersect(Closure(Sgt[4][1]),Ti))
> );
```

true

Therefore, we can determine defining equations for this set.

```
> Ideal(Sgt[4][1]);
```

$$[t_{1,1}t_{3,1}-{t_{2,1}}^2,{t_{1,2}t_{3,1}}^2+{t_{2,1}}^2t_{3,2}-2\,t_{2,1}t_{2,2}t_{3,1},t_{1,1}t_{3,2}+t_{1,2}t_{3,1}-2\,t_{2,1}t_{2,2}]$$

We want to verify that the determinant is already in this position before applying a transformation. In order to do so, we test whether the set of matrices yielding the special position contains the identity.

```
> Id := convert(T-IdentityMatrix(3),list):

> countingPolynomial(SolIntersect(Sgt[4][1], Id));
```

1

The intersection is non-empty, thus the identity matrix is a solution of one of our systems. ◁

We conclude this section with a statement regarding the systems describing the rank of a matrix which we are unable to prove.

Conjecture 5.14. *Consider the set $\mathcal{M}_{k,n}$ from Proposition (4.6) describing the $k \times n$-matrices of rank k with respect to a ranking fulfilling the conditions given there. Then $\mathcal{M}_{k,n}$ is in special position.*

5.3 Projective Varieties and Projective Counting Polynomials

We now consider subsets of the projective n-space $\mathbb{P}^n\left(\overline{K}\right)$. We describe these sets as sets of rays in $\mathbb{A}^n\left(\overline{K}\right)$, i.e. as solution sets of systems of homogeneous equations and inequations without the origin, where we identify two such solutions $\mathbf{a_1}, \mathbf{a_2}$ whenever there is a $k \in \overline{K}^*$ with $k\mathbf{a_1} = \mathbf{a_2}$. The following proposition was first stated in [Ple09a].

Proposition 5.15. *Let L be a polynomial system over $K[x_0, \ldots, x_n]$ containing only homogeneous equations and inequations.*

1. *There is a* THOMAS *decomposition $S = (S_1, \ldots, S_k)$ of L such that every polynomial occurring in S is homogeneous.*
2. $c\left(\mathcal{L}(L) \setminus \{(0, \ldots, 0)\}\right) = \begin{cases} c(L) - 1 & (0, \ldots, 0) \in \mathcal{L}(L) \\ c(L) & (0, \ldots, 0) \notin \mathcal{L}(L) \end{cases}$ *is divisible by $u - 1$.*

Proof. 1. Let $n = 0$. All homogeneous polynomials in $K[x_0]$ are $x_0^d, d \geq 0$. If a system contains both equations and inequations of this form, it is inconsistent, and a THOMAS decomposition contains no systems. If a system contains only equations, it is equivalent to the simple system $\{(x_0)_=\}$ and if it contains only inequations, it is equivalent to the simple system $\{(x_0)_\neq\}$.

Assume that x_0 is the smallest variable and let $n > 0$. Clearly, L is equivalent to $(L \cup \{(x_0)_=\}, L \cup \{(x_0)_\neq\})$. Let S^{hom} be a THOMAS decomposition of $L_{|x_0=0}$ over $K[x_1, \ldots, x_n]$. By induction, we can choose S^{hom} such that every polynomial appearing is homogeneous and thus $\{s \cup \{(x_0)_=\} | s \in S^{\text{hom}}\}$ is homogeneous, too.

For any (not necessarily simple) system s over $K[x_1, \ldots, x_n]$ denote by $h_{x_0}(s)$ the union of $\{(x_0)_\neq\}$ with the homogenization of s with x_0.

Since $h_{x_0}(s)$ is homogeneous, $\mathbf{a} \in \mathcal{L}(h_{x_0}(s))$ if and only if $k\mathbf{a} \in \mathcal{L}(h_{x_0}(s))$ for all $k \in \overline{K}^*$. Thus, if $(a_0, \ldots, a_n) \in \mathcal{L}(h_{x_0}(s))$, then $\left(1, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) \in \mathcal{L}(h_{x_0}(s))$ since $a_0 \neq 0$. Since $s = h_{x_0}(s)_{|x_0=1} \setminus \{1_\neq\}$, we see that $(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}) \in \mathcal{L}(s)$. On the other hand, if $(a_1, \ldots, a_n) \in \mathcal{L}(s)$, then $(a_0, a_0a_1, \ldots, a_0a_n) \in \mathcal{L}(h_{x_0}(s))$ for all $a_0 \in \overline{K}$.

If $t = (t_1, t_2)$ is a disjoint decomposition of s, then

$$\begin{aligned} \mathcal{L}(h_{x_0}(s)) &= \left\{(a_0, a_0a_1, \ldots, a_0a_n) \middle| (a_1, \ldots, a_n) \in \mathcal{L}(s) = \mathcal{L}(t_1) \uplus \mathcal{L}(t_2), a_0 \in \overline{K}\right\} \\ &= \biguplus_{i=1,2} \left\{(a_0, a_0a_1, \ldots, a_0a_n) \middle| (a_1, \ldots, a_n) \in \mathcal{L}(t_i), a_0 \in \overline{K}\right\} \\ &= \mathcal{L}(h_{x_0}(t_1)) \uplus \mathcal{L}(h_{x_0}(t_2)) \ . \end{aligned}$$

Now let S^{inhom} be a THOMAS decomposition of $L_{|x_0=1}$. Clearly, $(L \cup \{(x_0)_\neq\}) = h_{x_0}(L_{|x_0=1})$, thus

$$\mathcal{L}(L \cup \{(x_0)_\neq\}) = \mathcal{L}(h_{x_0}(L_{|x_0=1})) = \biguplus_{s \in S^{\text{inhom}}} \mathcal{L}(h_{x_0}(s)) \ .$$

This means that $\left(h_{x_0}(s) \middle| s \in S^{\text{inhom}}\right)$ is a disjoint decomposition of $\{L \cup \{(x_0)_\neq\}$.

It remains to show that is s is simple, then so is $h_{x_0}(s)$. Since x_0 is the smallest variable, the system obviously stays triangular. In positive characteristic, since homogenizing with x_0 does not change which roots of variables occur, the two extra properties that only affect positive characteristic stay untouched. Now let q be the initial or the discriminant of any polynomial in s. If there is a $(a_0, \ldots, a_n) \in \mathcal{L}(h_{x_0}(s))$ such that $\phi_{(a_0, \ldots, a_n)}(h_{x_0}(q)) = 0$, then the same holds for $\left(1, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right)$. However, this implies $\phi_{\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right)}(q) = 0$ and since $\left(1, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) \in \mathcal{L}(h_{x_0}(s))$, we also get $\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) \in \mathcal{L}(s)$. This contradicts that assumption that s is simple.

2. Due to part 1, we can assume that each system $S_1, \dots, S_k$ in the THOMAS decomposition is homogeneous. Therefore, it suffices to prove the statement for a single homogeneous simple system s.

   If $(0, \dots, 0) \in \mathcal{L}(s)$, then consider a THOMAS decomposition of

   $$s' = \left(s \cup \{(x_0)_=, \dots, (x_{i-1})_=, (x_i)_{\neq}\} \middle| i = 0, \dots, n \right) .$$

   Each of the systems in s' is homogeneous, therefore, due to part 1., we can choose the decomposition such that each system in it is homogeneous. Since $\mathcal{L}(s') = \mathcal{L}(s) \setminus (0, \dots, 0)$, $c(s') = c(s) - 1$.

   Consider a system s with $(0, \dots, 0) \notin \mathcal{L}(s)$ and let $i \geq 0$ be minimal such that $(0, \dots, 0) \in \mathcal{L}(s_{<x_i})$. If s_{x_i} is an equation or empty, then $(0, \dots, 0) \in \mathcal{L}(s_{\leq x_i})$ which contradicts minimality. Therefore, there is a homogeneous polynomial p with $\mathrm{ld}(p) = x_i$ and $p_{\neq} \in s$. If $i = 0$, then $p = x_0$. If $i > 0$, consider $p_0 := \phi_{<x_i,(0,\dots,0)}(p)$. Since $\mathrm{init}(p)$ is homogeneous, $\mathrm{ld}(\mathrm{init}(p)) > 1$ implies $\deg_{x_i}(p_0) < \mathrm{mdeg}(p)$, therefore $\mathrm{ld}(\mathrm{init}(p)) = 1$ must hold as s is simple. This implies $p_0 = x_i^{\mathrm{mdeg}(p)}$, which must not be a square, therefore $\mathrm{mdeg}(p) = 1$. This proves that the counting polynomial has a factor $u - 1$. □

This proposition gives us the tools to define a counting polynomial for subsets of $\mathbb{P}^n$ that are given as solution sets of homogeneous polynomial systems. The same definition has been given in [Ple09a].

Definition 5.16. Let S be a homogeneous polynomial system over $K[x_0, \dots, x_n]$. We call

$$\mathbb{P}c_n(S) = \frac{c_{n+1}\left(\mathcal{L}(S) \setminus \{(0, \dots, 0)\}\right)}{u - 1} = \begin{cases} \frac{c_{n+1}(S)-1}{u-1} & (0, \dots, 0) \in \mathcal{L}(S) \\ \frac{c_{n+1}(S)}{u-1} & (0, \dots, 0) \notin \mathcal{L}(S) \end{cases} \in \mathbb{Z}[u]$$

the **projective counting polynomial** of S. ◁

Example 5.17. $\mathbb{P}c\left(\mathbb{P}^n\right) = \frac{u^{n+1}-1}{u-1} = \sum_{i=0}^{n} u^i$. ◁

Since $c\left(\mathbb{A}^n\right) = u^n$, this is compatible with our intuitive notion of projective n-space. In particular, projective 1-space is affine 1-space plus a point at infinity, or $\mathbb{P}c(\mathbb{P}^1) = c(\mathbb{A}^1) + 1$. More general, projective n-space is affine n-space plus projective $n-1$-space at infinity, or $\mathbb{P}c(\mathbb{P}^n) = c(\mathbb{A}^n) + \mathbb{P}c(\mathbb{P}^{n-1})$.

This idea and the proof of Proposition (5.15) inspire another approach for computing the projective counting polynomial which is usually faster than computing it directly.

Example 5.18. Consider the system $S = \{(x_0x_3 - x_1x_2)_=\}$ over $\mathbb{Q}[x_0, \dots, x_3]$. Then $\mathcal{L}(S) \subseteq \mathbb{P}^3$ and

$$\begin{aligned} \mathbb{P}c(S) &= c_3\left(S_{|x_0=1}\right) + c_2\left(S_{|x_0=0,x_1=1}\right) + c_1\left(S_{|x_0=0,x_1=0,x_2=1}\right) + c_0\left(S_{|x_0=0,x_1=0,x_2=0,x_3=1}\right) \\ &= c_3\left(\{(x_3 - x_1x_2)_=\}\right) + c_2\left(\{(-x_2)_=\}\right) + c_1\left(\{(0)_=\}\right) + c_0\left(\{(0)_=\}\right) \\ &= u^2 + u + u + 1 = u^2 + 2u + 1 . \end{aligned}$$

◁

Here, c_0 is based on the map $c_0 : \mathrm{Pot}\left(\overline{K}^0\right) \to \mathbb{Z}[u] : M \mapsto |M|$ which can only have the values 0 or 1. In particular, for any $c \in K^*$, $c_0\left(\{0_=\}\right) = c_0\left(\{c_{\neq}\}\right) = 1$ and $c_0\left(\{0_{\neq}\}\right) = c_0\left(\{c_=\}\right) = 0$.

Remark 5.19. If V is the subset of $\mathbb{P}^n$ defined by the homogeneous system S, then $\dim(V) = \deg(\mathbb{P}c(S)) = \deg(c(S)) - 1$. ◁

Finally, for a homogeneous system S over $K[x_0, \dots, x_n]$, we denote the solution set as

$$\begin{aligned} \mathcal{L}^{\mathbb{P}}(S) &= \left(\mathcal{L}(S) \setminus \{(0, \dots, 0)\}\right) / \overline{K}^* \\ &= \{(a_0 : \cdots : a_n) \in \mathbb{P}^n | p(a_0, \dots, a_n) = 0, q(a_0, \dots, a_n) \text{ for all } p_=, q_{\neq} \in S\} \subseteq \mathbb{P}^n . \end{aligned}$$

5.4 Complex Varieties and Euler Characteristic

Consider $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ and set $\overline{K} = \mathbb{C}$, in particular, the algebraic closure of K is contained in $\mathbb{C}$. In this section we will shortly describe a relation between the topological Euler characteristic χ and the counting polynomial of an algebraic variety $V \subseteq \mathbb{C}^n$ or $V \subseteq \mathbb{P}^n(\mathbb{C})$. In [MB12], a method was described to recursively compute the Euler characteristic of an algebraic set. Although the author was unaware of counting polynomials, his arguments prove the following proposition.

Proposition 5.20. *1. Let $V \subseteq \mathbb{C}^n$ be an affine algebraic variety. Then $\chi(V) = c_n(V)_{|u=1}$.*

2. Let $V \subseteq \mathbb{P}^n(\mathbb{C})$ be a projective algebraic variety. Then $\chi(V) = \mathbb{P}c_n(V)_{|u=1}$.

This statement is correct independently of the coordinate system.

For example, the counting polynomial of affine k-space $\mathbb{C}^k$ is u^k and its Euler characteristic is 1. The counting polynomial of projective k-space $\mathbb{P}^k(\mathbb{C})$ is $\frac{u^{k+1}-1}{u-1} = \sum_{i=0}^{k} u^i$ and its Euler characteristic is $k+1$.

5.5 Counting Polynomials of Normal Toric Varieties

In this section, we will compute counting polynomials of certain embeddings of affine and projective normal toric varieties. Instead of using the Decompose algorithm, we will use the combinatorics of the toric variety to construct a Thomas decomposition directly. This is done by means of the orbit-cone-correspondence, which connects the orbits of the action of the torus with certain combinatorial information. We will describe the embedding of each of these orbits separately using a simple system.

The following section introduces some notation and definitions from the topic of toric varieties from [CLS11], which we recommend for a complete introduction into the topic. Readers that are already familiar with the topic may skip to section 5.5.2.

5.5.1 Preliminaries on Toric Varieties

Let $n \in \mathbb{N}$ and $M, N \cong \mathbb{Z}^n$, which we call the the character lattice and the lattice of one-parameter subgroups, respectively, with their associated $\mathbb{R}$-vector spaces $M_{\mathbb{R}} := \mathbb{R} \otimes_{\mathbb{Z}} M$ and $N_{\mathbb{R}} := \mathbb{R} \otimes_{\mathbb{Z}} N$.

A **torus** T is an affine variety T with a map $T \to (\mathbb{C}^*)^n$ that is both an isomorphism of varieties and an isomorphism of groups, where $(\mathbb{C}^*)^n$ is a group under component-wise multiplication. A **character** of T is a morphism $T \to \mathbb{C}^*$ that is a group homomorphism, and each $m \in M$ defines a character χ^m of the torus. A **one-parameter subgroup** of T is a morphism $\mathbb{C}^* \to T$ that is a group homomorphism and each $u \in N$ defines a one-parameter subgroup λ^u. There is a pairing $\langle \cdot, \cdot \rangle : M \times N \to \mathbb{Z}$ given by $(\chi^m \circ \lambda^u)(t) = t^{\langle m,u \rangle}$.

We collect some notation and important definitions and statements from [CLS11, Chap. 1-3].

Remark 5.21. If T is a torus with character lattice M, then $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^*) \cong T$ (cf. [CLS11, pg. 12]). ◁

Definition 5.22. An affine variety V is a **toric variety** if it is the Zariski closure of a torus T such that the action of the torus on itself extends to an action on the variety, where the action homomorphism $T \times V \to V$ is given by a morphism of varieties. ◁

There are classes of toric varieties that are well-understood due to their combinatorial structure. We will now consider affine normal toric varieties, which are characterized by convex rational polyhedral cones.

Definition 5.23. 1. Let $S \subseteq N$ be finite. The set

$$\mathrm{Cone}(S) = \left\{ \sum_{u \in S} \lambda_u u \,\middle|\, \lambda_u \geq 0 \right\} \subseteq N_{\mathbb{R}}$$

is called a **convex rational polyhedral cone** ([CLS11, Def. 1.2.1], [CLS11, Def. 1.2.14]).

2. For a convex rational polyhedral cone σ, the **dual cone** is

$$\sigma^\vee := \{m \in M_\mathbb{R} | \langle m, u\rangle \geq 0 \text{ for all } u \in \sigma\} \ .$$

([CLS11, Def. 1.2.3])

3. For $m \in \sigma^\vee$, let $H_m := \{u \in \mathbb{N}_\mathbb{R} | \langle m, u\rangle = 0\}$. Then $\tau = H_m \cap \sigma$ is a **face** of σ and we write $\tau \preceq \sigma$ ([CLS11, Prop. 1.2.5]). If τ is a **proper face** of σ, i.e. τ is a face of σ and $\tau \neq \sigma$, we write $\tau \prec \sigma$.

4. For every face $\tau \preceq \sigma$, define $\tau^\perp := \{m \in M_\mathbb{R} | \langle m, u\rangle = 0 \text{ for all } u \in \tau\}$ and $\tau^* := \sigma^\vee \cap \tau^\perp$. We call τ^* the **dual face** of τ.

5. A convex rational polyhedral cone σ is **strongly convex** if $\{0\} \preceq \sigma$, or equivalently, if $\dim(\sigma^\vee) = n$ ([CLS11, Prop. 1.2.12]). ◁

Clearly, every cone is a face of itself. In [CLS11, Lem. 1.2.6], it is shown that a face of a polyhedral cone is a cone, that the intersection of two faces of a cone is a face, and that a face of a face is a face of the original cone.

We will now demonstrate how a convex rational polyhedral cones defines an affine toric variety.

Definition 5.24. Let $\sigma \subseteq N_\mathbb{R}$ be a convex rational polyhedral cone. Then the **affine normal toric variety** defined by σ is $U_\sigma := \operatorname{Spec}(\mathbb{C}[\sigma^\vee \cap M])$ ([CLS11, Thm. 1.2.18]). ◁

In the projective case, normal toric varieties are characterized by polytopes as follows.

Definition 5.25.

1. A **lattice polytope** is a set $P \subseteq M_\mathbb{R}$ that is the convex hull of a finite set $S \subseteq M$ ([CLS11, Def. 1.2.2], [CLS11, pg. 66]).

2. Q is a **face** of P, denoted by $Q \preceq P$ if there are $u \in N_\mathbb{R}$ and $b \in \mathbb{R}$ with $\langle m, u\rangle \geq b$ for all $m \in P$ and $Q = \{m \in P | \langle m, u\rangle = b\}$.

3. Let P be a lattice polytope. For a vertex (i.e. zero-dimensional face) m of P, let $P \cap M - m := \{e - m | e \in P \cap M\}$. Define the semigroup $S_{P,m} := \mathbb{Z}_{\geq 0}[P \cap M - m]$. Then P is **very ample** if for every vertex m of P, the semigroup $S_{P,m}$ is saturated, i.e. for all $k \in \mathbb{N}$ and $m \in M$, $km \in S_{P,m}$ implies $m \in S_{P,m}$ ([CLS11, Def. 2.2.17]). ◁

According to [CLS11, Cor. 2.2.19], for every lattice polynomial P there is a $k \in \mathbb{N}$ such that kP is very ample.

Definition 5.26. Let $P \subseteq M_\mathbb{R}$ be a full-dimensional lattice polytope.

1. If P is very ample and $P \cap M = \{m_0, \ldots, m_s\}$, the Zariski closure of the image of the map $(\mathbb{C}^*)^n \to \mathbb{P}^s : t \mapsto (\chi^{m_0}(t) : \cdots : \chi^{m_s}(t)) \in \mathbb{P}^s$ is a projective variety denoted by $X_{P \cap M}$ ([CLS11, pg. 75]).

2. Let $k \in \mathbb{N}$ such that kP is very ample. Then $X_P := X_{kP \cap M}$ is called the toric variety of the polytope P ([CLS11, Def. 2.3.14]). ◁

The variety X_P is a normal toric variety. It only depends on the so-called normal fan of the polytope, i.e. stretching the polytope will not change the variety, but it will change the embedding, as we will see below.

5.5.2 Embeddings of Toric Varieties in Affine and Projective Space

We will now construct embeddings of normal toric varieties into $\mathbb{C}^s$ or $\mathbb{P}^s$ for some $s \in \mathbb{N}$ and compute their counting polynomials.

We start with the affine case. We saw in the last section that a convex rational polyhedral σ cone defines an affine normal toric variety. The intersection $\sigma^\vee \cap M$ of the dual cone with M defines a semi-group. By choosing generators of that semi-group, we define an embedding into affine space. For these embeddings, we can easily compute the counting polynomial.

Lemma 5.27. *Let σ be a strongly convex rational polyhedral cone in $N_{\mathbb{R}}$ and $X \in M^s$ such that $\mathbb{Z}_{\geq 0}X = \sigma^\vee \cap M$. Define*

$$\Psi^X : \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^*) \to \mathbb{C}^s : \chi \mapsto (\chi(X_i) | i = 1, \ldots, s)$$

Then $\mathrm{im}\left(\Psi^X\right) \cong (\mathbb{C}^*)^n$ and $Y_X = \overline{\mathrm{im}\left(\Psi^X\right)} \cong U_\sigma$, i.e. Ψ^X defines an embedding of the torus and the toric variety into affine s-space.

Proof. Since σ is strongly convex, $\sigma^\vee$ is full-dimensional and it follows from the proof of [CLS11, Thm. 1.2.18] that $\langle X \rangle_{\mathbb{Z}} = M$. Therefore, each element of $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^*)$ is uniquely determined by its image on the elements of X, implying injectivity of Ψ^X. As $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^*) \cong (\mathbb{C}^*)^n$, this proves our claim.

Let $U_\sigma := \mathrm{Spec}(\mathbb{C}[\sigma^\vee \cap M])$ as defined in [CLS11, 1.2.18]. As $\sigma^\vee \cap M = \mathbb{Z}_{\geq 0}X$, it follows from [CLS11, 1.1.14] that $\mathrm{Spec}(\mathbb{C}[\sigma^\vee \cap M]) = Y_X$ where Y_X is defined in [CLS11, 1.1.7] to be the Zariski-closure of the image of the map Ψ^X. □

The Orbit-Cone Correspondence (cf. [CLS11, §3.2]) shows that the orbits of the action of the torus on the affine toric variety U_σ correspond to the faces of the cone σ. The following lemma performs this decomposition on the embedding $\overline{\mathrm{im}\left(\Psi^X\right)}$.

Lemma 5.28. *Let σ be a strongly convex rational polyhedral cone in $N_{\mathbb{R}}$, $X \in M^s$ such that $\mathbb{Z}_{\geq 0}X = \sigma^\vee \cap M$ as in Lemma (5.27). Let $\tau \preceq \sigma$ be a face of σ with dual face $\tau^* := \tau^\perp \cap \sigma^\vee$. The map*

$$\begin{array}{rccl} \Psi^X_{\tau^*} : & \mathrm{Hom}_{\mathbb{Z}}\left(\tau^\perp \cap M, \mathbb{C}^*\right) & \to & \mathbb{C}^s : \\ & \chi & \mapsto & \left(\left\{ \begin{array}{ll} \chi(X_i) & X_i \in \tau^* \\ 0 & X_i \notin \tau^* \end{array} \right. \middle| i = 1, \ldots, s \right) \end{array}$$

defines an embedding of the torus orbit corresponding to τ into affine s-space. In particular, $\Psi^X_{\tau^*}$ is injective and the image of $\Psi^X_{\tau^*}$ is contained in $\overline{\mathrm{im}\left(\Psi^X\right)}$.

Proof. 1. $\Psi^X_{\tau^*}$ is injective:

First show that $\langle \tau^* \cap X \rangle_{\mathbb{Z}} = \tau^\perp \cap M$. Let $m \in \tau^\perp \cap M$. Then, since $m \in M$, there are a_i such that $m = \sum_{i=1}^s a_i X_i$. Since $m \in \tau^\perp$, $0 = \langle m, u \rangle = \sum_{i=1}^s a_i \langle X_i, u \rangle$ for all $u \in \tau$. Define $F := \{i \in \underline{s} | X_i \notin \tau^*\}$. Then

$$0 = \sum_{i \in F} a_i \langle X_i, u \rangle + \sum_{i \in \underline{s} \setminus F} a_i \langle X_i, u \rangle = \sum_{i \in F} a_i \langle X_i, u \rangle \ .$$

As $X_i \in \sigma^\vee$ for all $i = 1, \ldots, s$, it holds that $\langle X_i, u \rangle \geq 0$ for all $u \in \sigma \supseteq \tau$. Since $X_i \notin \tau^*$ for $i \in F$, there is $u \in \tau$ such that $\langle X_i, u \rangle > 0$, implying $a_i = 0$. This shows that $\tau^\perp \cap M \subseteq \langle \tau^* \cap X \rangle_{\mathbb{Z}}$. The other inclusion is obvious.

Therefore, each element of $\mathrm{Hom}_{\mathbb{Z}}\left(\tau^\perp \cap M, \mathbb{C}^*\right)$ is uniquely determined by its image on $\tau^* \cap X$, implying injectivity.

2. $\mathrm{im}\left(\Psi^X_{\tau^*}\right) \subseteq \overline{\mathrm{im}\left(\Psi^X\right)}$:

Let $I = I\left(\overline{\mathrm{im}\left(\Psi^X\right)}\right)$ be the vanishing ideal. According to [CLS11, Prop. 1.1.9], this ideal is given by

$$I = \left\langle b_l \middle| l = (l_1, \ldots, l_s) \in \mathbb{Z}^s : \sum_{i=1}^s l_i X_i = 0 \right\rangle \trianglelefteq \mathbb{C}[x_1, \ldots, x_s]$$

with

$$b_l := \mathbf{x}^{l_+} - \mathbf{x}^{l_-} := \prod_{\substack{i=1,\ldots,s \\ l_i > 0}} x_i^{l_i} - \prod_{\substack{i=1,\ldots,s \\ l_i < 0}} x_i^{-l_i} \ .$$

Let F be as above and l such that $\sum_{i=1}^s l_i X_i = 0$. If $l_i = 0$ for every $i \in F$, then $b_l\left(\Psi^X_{\tau^*}(\chi)\right) = b_l(\Psi^X(\chi)) = 0$ where Ψ^X is defined in Lemma (5.27). If there is an $i \in F$ with $l_i > 0$,

it remains to show that there is also $j \in F, i \neq j$ with $l_j < 0$. Then, $b_l\left(\Psi^X_{\tau^*}(\chi)\right) = (b_l)_{|x_i=0,x_j=0}\left(\Psi^X_{\tau^*}(\chi)\right) = 0$.

Let $i \in F$ such that $l_i > 0$ and assume that $l_j \geq 0$ for all $j \in F$ with $j \neq i$. As above, there is $u \in \tau$ such that $\langle X_i, u\rangle > 0$ and

$$0 = \sum_{j\in F} l_j\langle X_j, u\rangle = \underbrace{l_i}_{>0}\underbrace{\langle X_i, u\rangle}_{>0} + \sum_{\substack{j\in F\\ j\neq i}} \underbrace{l_j}_{\geq 0}\underbrace{\langle X_j, u\rangle}_{\geq 0} > 0 \ ,$$

which is a contradiction. Therefore, at least one l_j must be negative. □

Since σ is strongly convex, $\{0\}$ is a face of σ. Clearly, $\Psi^X = \Psi^X_{\{0\}^*}$.

We will now see that the images of $\Psi^X_{\tau^*}$ give a disjoint decomposition of $\overline{\operatorname{im}\left(\Psi^X\right)}$.

Lemma 5.29. *Let σ be a strongly convex rational polyhedral cone in $N_\mathbb{R}$, $X \in M^s$ such that $\mathbb{Z}_{\geq 0}X = \sigma^\vee \cap M$ as in Lemma (5.27). Then*

$$\overline{\operatorname{im}\left(\Psi^X\right)} = \biguplus_{\tau\preceq\sigma} \operatorname{im}\left(\Psi^X_{\tau^*}\right) \ .$$

Proof.

Disjointness As the X_i generate the dual cone $\sigma^\vee$, the subsets of X that generate a particular face of $\sigma^\vee$ are pairwise distinct. Since the zeroes in the definition of $\Psi^X_{\tau^*}$ are inserted in different components for each face τ, this implies disjointness of the images of the $\Psi^X_{\tau^*}$.

"$\supseteq$" Immediately from (5.28).

"$\subseteq$" Immediately from [CLS11, Lem. 3.2.5] and [CLS11, Thm. 3.2.6 (c)]. □

Theorem 5.30. *Let σ be a strongly convex rational polyhedral cone in $N_\mathbb{R}$, $X \in M^s$ such that $\mathbb{Z}_{\geq 0}X = \sigma^\vee \cap M$ as in Lemma (5.27). For every face $\tau \preceq \sigma$ there is a simple system S over $\mathbb{Q}[x_1, \ldots, x_s]$ such that $\operatorname{im}\left(\Psi^X_{\tau^*}\right) = \mathcal{L}(S)$.*

In particular, the decomposition from Lemma (5.29) is a Thomas *decomposition of the embedding defined by X.*

Proof. As before, let $F := \{i \in \underline{s} | X_i \notin \tau^*\}$. Consider the $\mathbb{Z}$-module

$$L_{\tau^*} := \left\{ l \in \mathbb{Z}^s \middle| (l_i = 0 \,\forall\, i \in F) \wedge \sum_{i=1}^s l_i X_i = 0 \right\} \ .$$

Further consider a generating set $\left\{l^{(1)}, \ldots, l^{(k)}\right\}$ of L_{τ^*} such that for any $r = 1, \ldots, k$ the following holds: If i is such that $l^{(r)}_i \neq 0$ and $l^{(r)}_{i'} = 0$ for all $i' > i$, then $l^{(j')}_i = 0$ for all $j' > j$ and $0 \leq l^{(j')}_i < l^{(r)}_i$ for all $j' < j$. Such a generating set can be obtained by computing the Hermite form of the matrix $\left(l^{(r)}_{s-i+1}\right)_{i=1,\ldots,s,r=1,\ldots,k}$.

Now consider the polynomial system

$$S' := \{(b_{l^{(r)}})_= | r = 1, \ldots, k\} \cup \{(x_i)_= | i \in F\}$$

where b_l is defined as in the proof of Lemma (5.28) and define $S := S' \cup \{(x_i)_{\neq} | x_i \notin \operatorname{ld}(S')\}$. Due to the choice of $l^{(1)}, \ldots, l^{(k)}$, the system S is triangular.

To prove that S is simple, first prove that for every monomial $q \in Q := \left\{\prod_{j\in\underline{s}\setminus F} x_j^{d_j} \middle| d_j \geq 0\right\}$ and every solution $\mathbf{a} \in \mathcal{L}(S)$, $\phi_\mathbf{a}(q) \neq 0$ holds. If $\operatorname{ld}(q) = 1$, then $q = 1$ and the statement holds. Now let $i \notin F$ and assume that $\phi_\mathbf{a}(q) \neq 0$ for every $q \in Q$ with $\operatorname{ld}(q) < x_i$ and every $\mathbf{a} \in \mathcal{L}(S)$. Consider $q \in Q$ with $\operatorname{ld}(q) = i$. There are two possibilities: If $(x_i)_{\neq} \in S$, the coefficient

of $x_i^{\mathrm{mdeg}(q)}$ has a leader smaller than x_i and thus the statement follows by induction. Otherwise, there is $1 \leq r \leq k$ such that $\mathrm{ld}\left(b_{l^{(r)}}\right) = x_i$. There are monomials $t_1, t_2 \in Q$ with $\mathrm{ld}(t_1) < x_i$ and $\mathrm{ld}(t_2) < x_i$ such that $t_1 q + t_2 b_{l^{(r)}} =: q' \in Q$ and $\mathrm{ld}(q') < x_i$. By induction, it follows that $\phi_{\mathbf{a}}(q) = \frac{\phi_{\mathbf{a}}(q') - \phi_{\mathbf{a}}(t_2)\phi_{\mathbf{a}}(b_{l^{(r)}})}{\phi_{\mathbf{a}}(t_1)} = \frac{\phi_{\mathbf{a}}(q')}{\phi_{\mathbf{a}}(t_1)}$ is non-zero, and again the statement holds.

Since the initial or discriminant of any $b_{l^{(r)}}$ is a monomial from Q, the system S is simple.

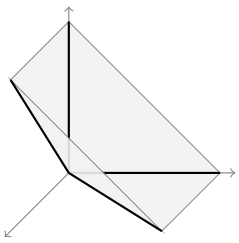
It remains to be shown that $\mathcal{L}(S) = \mathrm{im}\left(\Psi^X_{\tau^*}\right)$. The inclusion $\mathrm{im}\left(\Psi^X_{\tau^*}\right) \subseteq \mathcal{L}(S)$ follows from Lemma (5.28) and its proof. Conversely, let $\mathbf{a} \in \mathcal{L}(S)$ and consider $L := \{l \in \mathbb{Z}^s | \sum_{i=1}^s l_i X_i = 0\}$. For each $l \in L$, either $(b_l)_{|x_i=0, i\in F} = 0$ or $l \in L_{\tau^*}$, which implies $\phi_{\mathbf{a}}(b_l) = 0$ for all $l \in L$. Thus $\mathbf{a} \in V\left(I\left(\mathrm{im}\left(\Psi^X\right)\right)\right) = \overline{\mathrm{im}\left(\Psi^X\right)} = \biguplus_{\tau \preceq \sigma} \mathrm{im}\left(\Psi^X_{\tau^*}\right)$ which implies that there is a $\tau' \preceq \sigma$ with $\mathbf{a} \in \mathrm{im}\left(\Psi^X_{(\tau')^*}\right)$. For every $\mathbf{b} \in \mathrm{im}\left(\Psi^X_{(\tau')^*}\right)$, $\mathbf{b}_i \neq 0$ if and only if $X_i \in \tau'^*$. Moreover, each such τ' is uniquely identified by the set $\{i \in \underline{s} | X_i \in (\tau')^*\}$. Therefore, we get $\tau' = \tau$, which implies $\mathcal{L}(S) \subseteq \mathrm{im}\left(\Psi^X_{\tau^*}\right)$. □

The first two paragraphs of the previous proof give an explicit construction of the simple systems from the relations between the generators X_i. Note that the order of these generators has an influence on the counting polynomial. For example, if $n = 1$, $X_1 = 1$, $X_2 = 2$, we have the relation $(-2, 1)$ which results in the binomial $x_2 - x_1^2$ with main degree 1. On the other hand $X_1 = 2$, $X_2 = 1$ gives the relation $(-1, 2)$ and the binomial $x_2^2 - x_1$ with main degree 2.

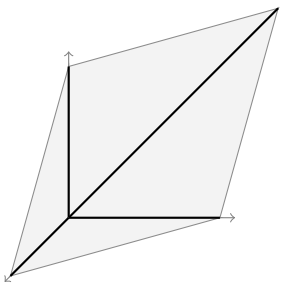
The counting polynomial of the systems constructed in the proof is easily computed. If d is the dimension of the torus orbit, then the corresponding system contains d inequations of the form $(x_i)_{\neq}$, but no other inequations. Its counting polynomial is therefore $n(u-1)^d$ for some $n \in \mathbb{N}$. The number n can be determined from the relations as demonstrated above. If $n > 1$, then the torus orbit is an n-fold cover of the torus. For an affine normal toric variety, we get an expansion $\sum_d n_d (u-1)^d$ of the counting polynomial where n_d is the sum over these numbers for all torus orbits of the same dimension.

The only 0-dimensional torus orbit corresponds to the face $\sigma \preceq \sigma$ and its dual face $\sigma^* = \{0\} \preceq \sigma^\vee$. It always yields a single point and thus the counting polynomial 1. This proves that every affine normal toric variety has Euler characteristic 1.

Example 5.31. Consider the cone $\sigma \subseteq \mathbb{R}^3$ generated by the rays $(1,0,0)$, $(0,1,0)$, $(1,0,1)$ and $(0,1,1)$. The dual cone $\sigma^\vee \subseteq \mathbb{R}^3$ is generated by $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,-1)$.



(a) σ



(b) $\sigma^\vee$

The faces of σ with their dual faces are given as follows:

$$\begin{aligned}
\tau_1^0 &= \{0\} & \left(\tau_1^0\right)^* &= \sigma^\vee \\
\tau_1^1 &= \langle (1,0,0) \rangle_{\mathbb{Z}_{\geq 0}} & \left(\tau_1^1\right)^* &= \langle (0,1,0), (0,0,1) \rangle_{\mathbb{Z}_{\geq 0}} \\
\tau_2^1 &= \langle (0,1,0) \rangle_{\mathbb{Z}_{\geq 0}} & \left(\tau_2^1\right)^* &= \langle (1,0,0), (0,0,1) \rangle_{\mathbb{Z}_{\geq 0}} \\
\tau_3^1 &= \langle (1,0,1) \rangle_{\mathbb{Z}_{\geq 0}} & \left(\tau_3^1\right)^* &= \langle (0,1,0), (1,1,-1) \rangle_{\mathbb{Z}_{\geq 0}} \\
\tau_4^1 &= \langle (0,1,1) \rangle_{\mathbb{Z}_{\geq 0}} & \left(\tau_4^1\right)^* &= \langle (1,0,0), (1,1,-1) \rangle_{\mathbb{Z}_{\geq 0}} \\
\tau_1^2 &= \langle (1,0,0), (1,0,1) \rangle_{\mathbb{Z}_{\geq 0}} & \left(\tau_1^2\right)^* &= \langle (0,1,0) \rangle_{\mathbb{Z}_{\geq 0}}
\end{aligned}$$

$$\begin{aligned}
\tau_2^2 &= \langle (1,0,0),(0,1,0)\rangle_{\mathbb{Z}_{\geq 0}} & \left(\tau_2^2\right)^* &= \langle (0,0,1)\rangle_{\mathbb{Z}_{\geq 0}} \\
\tau_3^2 &= \langle (1,0,1),(0,1,1)\rangle_{\mathbb{Z}_{\geq 0}} & \left(\tau_3^2\right)^* &= \langle (1,1,-1)\rangle_{\mathbb{Z}_{\geq 0}} \\
\tau_4^2 &= \langle (0,1,0),(0,1,1)\rangle_{\mathbb{Z}_{\geq 0}} & \left(\tau_4^2\right)^* &= \langle (1,0,0)\rangle_{\mathbb{Z}_{\geq 0}} \\
\tau_1^3 &= \sigma & \left(\tau_1^3\right)^* &= \{0\}
\end{aligned}$$

Choose $X := ((1,0,0),(0,1,0),(0,0,1),(1,1,-1))$. Then $L_{\left(\tau_1^0\right)} = \langle (-1,-1,1,1)\rangle_{\mathbb{Z}}$, $L_{\tau_i^d} = 0$ for $(d,i) \neq (0,1)$ and the simple systems S_i^d over $\mathbb{C}[x_1,\ldots,x_4]$ with $\mathcal{L}(S_i^d) = \operatorname{im}\left(\Psi^X_{(\tau_i^d)^*}\right)$ are as follows.

$$\begin{aligned}
S_1^0 &= \{(x_1)_{\neq},(x_2)_{\neq},(x_3)_{\neq},(x_3x_4 - x_1x_2)_{=}\} \\
S_1^1 &= \{(x_1)_{=},(x_2)_{\neq},(x_3)_{\neq},(x_4)_{=}\} \\
S_2^1 &= \{(x_1)_{\neq},(x_2)_{=},(x_3)_{\neq},(x_4)_{=}\} \\
S_3^1 &= \{(x_1)_{=},(x_2)_{\neq},(x_3)_{=},(x_4)_{\neq}\} \\
S_4^1 &= \{(x_1)_{\neq},(x_2)_{=},(x_3)_{=},(x_4)_{\neq}\} \\
S_1^2 &= \{(x_1)_{=},(x_2)_{\neq},(x_3)_{=},(x_4)_{=}\} \\
S_2^2 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{\neq},(x_4)_{=}\} \\
S_3^2 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{=},(x_4)_{\neq}\} \\
S_4^2 &= \{(x_1)_{\neq},(x_2)_{=},(x_3)_{=},(x_4)_{=}\} \\
S_1^3 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{=},(x_4)_{=}\}
\end{aligned}$$

The counting polynomial of $\overline{\operatorname{im}(\Psi^X)}$ is $(\infty-1)^3 + 4(\infty-1)^2 + 4(\infty-1) + 1 = u^3 + u^2 - u$.

If we choose $X = ((3,0,2),(1,0,0),(0,1,0),(0,0,1),(1,1,-1))$ instead, we have

$$\begin{aligned}
L_{\left(\tau_1^0\right)^*} &= \langle (0,-1,-1,1,1),(-1,3,0,2,0)\rangle_{\mathbb{Z}} \ , \\
L_{\left(\tau_2^1\right)^*} &= \langle (-1,3,0,2,0)\rangle_{\mathbb{Z}} \ ,
\end{aligned}$$

and $L_{\left(\tau_i^d\right)^*} = 0$ for $(d,i) \notin \{(0,1),(1,2)\}$. The corresponding systems T_i^d over $\mathbb{C}[x_1,\ldots,x_5]$ are then as follows.

$$\begin{aligned}
T_1^0 &= \{(x_1)_{\neq},(x_2)_{\neq},(x_3)_{\neq},(x_2^3x_4^2 - x_1)_{=},(x_4x_5 - x_2x_3)_{=}\} \\
T_1^1 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{\neq},(x_4)_{\neq},(x_5)_{=}\} \\
T_2^1 &= \{(x_1)_{\neq},(x_2)_{\neq},(x_3)_{=},(x_2^3x_4^2 - x_1)_{=},(x_5)_{=}\} \\
T_3^1 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{\neq},(x_4)_{=},(x_5)_{\neq}\} \\
T_4^1 &= \{(x_1)_{=},(x_2)_{\neq},(x_3)_{=},(x_4)_{=},(x_5)_{\neq}\} \\
T_1^2 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{\neq},(x_4)_{=},(x_5)_{=}\} \\
T_2^2 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{=},(x_4)_{\neq},(x_5)_{=}\} \\
T_3^2 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{=},(x_4)_{=},(x_5)_{\neq}\} \\
T_4^2 &= \{(x_1)_{=},(x_2)_{\neq},(x_3)_{=},(x_4)_{=},(x_5)_{=}\} \\
T_1^3 &= \{(x_1)_{=},(x_2)_{=},(x_3)_{=},(x_4)_{=},(x_5)_{=}\}
\end{aligned}$$

For this embedding, the counting polynomial is $2(u-1)^3+(3\cdot 1+1\cdot 2)(u-1)^2+4(u-1)+1 = 2u^3-u^2$. Note that in the last example, the polynomials $x_2^3x_4^2 - x_1$ and $x_4x_5 - x_2x_3$ are not sufficient to generate the vanishing ideal, however, they suffice to describe the toric variety using the above THOMAS decomposition. ◁

Normal projective toric varieties are characterized using lattice polytopes. Note that the variety only depends on the normal vectors of the polytope's $n-1$-dimensional faces, but its embedding into projective space depends on the entire polytope. The following Lemma shows how to construct such an embedding.

Lemma 5.32. *Let $P \subseteq M_{\mathbb{R}}$ be a full-dimensional very ample lattice polytope $P \cap M = \{m_1, \dots m_s\}$. Consider the map*

$$\Phi^{(m_1,\dots,m_s)} : \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^*) \to \mathbb{P}^{s-1} : \chi \mapsto (\chi(m_1) : \cdots : \chi(m_s)) \ .$$

Then $\mathrm{im}(\Phi) \cong (\mathbb{C}^*)^n$ and $\overline{\mathrm{im}(\Phi)} \cong X_P$.

Proof. Since P is full-dimensional, $n > 0$ implies $s > 1$, therefore it holds that $(\chi(m_1) : \cdots : \chi(m_s)) = (1 : \frac{\chi(m_2)}{\chi(m_1)} : \cdots : \frac{\chi(m_2)}{\chi(m_1)}) = (1 : \chi(m_2 - m_1) : \cdots : \chi(m_2 - m_1))$. The lattice points $m_i - m_1$, $i = 2, \dots, s$ generate M, therefore $\Phi^{(m_1,\dots,m_s)}$ is injective and $\mathrm{im}\left(\Phi^{(m_1,\dots,m_s)}\right) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^*) \cong (\mathbb{C}^*)^n$.

Note that since P is very ample, $X_P = X_{P \cap M}$. The second statement then follows directly from [CLS11, Def. 2.1.1]. □

We cannot use this method directly to obtain the simple systems describing the torus orbits. We modify it such that we can reduce the projective case to the affine case.

Remark 5.33. If we denote by ν the canonical epimorphism $\nu : \mathbb{C}^s \setminus \{0\} \to \mathbb{P}^{s-1}$, then $\Phi = \nu \circ \Psi^{(m_1,\dots,m_s)}$. Consider the map

$$(\Psi')^{(m_1,\dots,m_s)} : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z} \oplus M, \mathbb{C}^*) \to \mathbb{C}^s : \chi \mapsto (\chi(1, m_1), \dots, \chi(1, m_s)) \ .$$

Since $\chi(a, m) = \chi((a, 0) + (0, m)) = \chi(a, 0) \cdot \chi(0, m)$ for every $\chi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z} \oplus M, \mathbb{C}^*)$, it holds that $\mathrm{im}(\Psi') = \mathbb{C}^* \,\mathrm{im}(\Psi)$. Therefore $\mathrm{im}(\nu \circ (\Psi')^{(m_1,\dots,m_s)}) = \mathrm{im}(\nu \circ \Psi^{(m_1,\dots,m_s)}) = \mathrm{im}(\Phi^{(m_1,\dots,m_s)})$.

For all $l \in \mathbb{Z}^s$ with $\sum_{i=1}^s l_i(1, m_i) = 0$, we get $\sum_{i=1}^s l_i$. This implies that the binomial $b_l \in \mathbb{C}[x_1, \dots, x_s]$ is homogeneous and therefore, the ideal $I := \langle b_l | \sum_{i=1}^s l_i \cdot (1, m_i) = 0 \rangle$ is a homogeneous ideal. According to [CLS11, Prop. 2.1.4], this implies that I is the vanishing ideal of $X_{P \cap M} = \overline{\mathrm{im}(\Phi)}$ and that $Y_{P \cap M}$ is the affine cone of $X_{P \cap M}$, i.e. $\nu(Y_{P \cap M}) = X_{P \cap M}$. ◁

This remark shows that by simply replacing each element $m \in P \cap M \subseteq M$ with $(1, m) \in \mathbb{Z} \oplus M$, we can treat the the result identically to the affine case. Due to [CLS11, Prop. 2.1.4], we can then interpret the solution set of the resulting homogeneous simple systems as torus orbits of the projective variety X_P.

Theorem 5.34. *For $F \preceq P$, let $\hat{F} := \langle (1, f) | f \in F \rangle_{\mathbb{R}}$ and define $(\Psi')_F^{(m_1,\dots,m_s)}$ as*

$$\begin{array}{rccl} (\Psi')_F^{(m_1,\dots,m_s)} : & \mathrm{Hom}_{\mathbb{Z}}\left(\hat{F} \cap (\mathbb{Z} \oplus M), \mathbb{C}^*\right) & \to & \mathbb{C}^s : \\ & \chi & \mapsto & \left(\left\{ \begin{array}{ll} \chi(1, X_i) & X_i \in F \\ 0 & X_i \notin F \end{array} \right| i = 1, \dots, s \right) \end{array} ,$$

analogously to Lemma (5.28). Then

$$\overline{\mathrm{im}\left(\Phi^{(m_1,\dots,m_s)}\right)} = \biguplus_{F \preceq P} \mathrm{im}\left(\nu \circ (\Psi')_F^{(m_1,\dots,m_s)}\right)$$

and for each $F \preceq P$ there is a simple system S with $\mathcal{L}^{\mathbb{P}}(S) = \mathrm{im}\left(\nu \circ (\Psi')_F^{(m_1,\dots,m_s)}\right)$.

In particular, this yields a Thomas *decomposition of the embedding of X_P defined by the polytope P.*

Proof. Note that $(1, m_1), \ldots, (1, m_s)$ generate a full-dimensional cone in $\mathbb{Z} \oplus M$ and that the faces of this cone that are not equal $\{0\}$ correspond to the faces of P. Therefore, we can apply Lemma (5.28), and get $\overline{\operatorname{im}\left((\Psi')^{(m_1,\ldots,m_s)}\right)} \setminus \{0\} = \biguplus_{F \preceq P} \operatorname{im}\left((\Psi')_F^{(m_1,\ldots,m_s)}\right)$. Since 0 is not contained in this set, we can apply ν to both sides of the equation. As the $\operatorname{im}\left((\Psi')_F^{(m_1,\ldots,m_s)}\right)$ are closed under multiplication with elements of $\mathbb{C}^*$, this leads to

$$\nu\left(\overline{\operatorname{im}\left((\Psi')^{(m_1,\ldots,m_s)}\right)} \setminus \{0\}\right) = \nu\left(\biguplus_{F \preceq P} \operatorname{im}\left((\Psi')_F^{(m_1,\ldots,m_s)}\right)\right) = \biguplus_{F \preceq P} \nu\left(\operatorname{im}\left((\Psi')_F^{(m_1,\ldots,m_s)}\right)\right) .$$

Due to [CLS11, Prop. 2.1.4], this proves the first claim.

The simple systems can now be obtained from Theorem (5.30). □

Just as in the affine case, the projective counting polynomial is easily computed and its interpretation is analogous. The only zero-dimensional torus orbits correspond to the zero-dimensional faces of the polytope, i.e. its vertices. Due to the construction of the simple systems and thus the counting polynomial, this implies that the Euler characteristic of a normal projective toric variety equals the number of the vertices of the polytope that defines it.

Example 5.35. Denote by $\operatorname{Conv}(p_1, \ldots, p_r)$ the convex hull of the points $p_1, \ldots, p_r \in M$. Let $n = 2$ and consider the polytopes

$$P_1 := \operatorname{Conv}((0,0),(1,0),(0,1),(1,1)) ,$$
$$P_2 := \operatorname{Conv}((-1,-1),(1,-1),(-1,1),(1,1)) .$$

Define

$$m^{(1)} := ((0,0),(1,0),(0,1),(1,1)) \in M^4 ,$$
$$m^{(2)} := ((-1,-1),(1,-1),(-1,1),(1,1),(0,0),(1,0),(0,-1),(-1,0),(0,1)) \in M^9 .$$

Then $P_1 \cap M = \left\{m_1^{(1)}, \ldots, m_4^{(1)}\right\}$ and $P_2 \cap M = \left\{m_1^{(2)}, \ldots, m_9^{(2)}\right\}$. The faces of P_1 are as follows:

$$\begin{aligned}
F_1^2 &= P_1 & F_1^2 \cap M &= P_1 \cap M \\
F_1^1 &= \operatorname{Conv}\left(m_1^{(1)}, m_3^{(1)}\right) & F_1^1 \cap M &= \left\{m_1^{(1)}, m_3^{(1)}\right\} \\
F_2^1 &= \operatorname{Conv}\left(m_1^{(1)}, m_2^{(1)}\right) & F_2^1 \cap M &= \left\{m_1^{(1)}, m_2^{(1)}\right\} \\
F_3^1 &= \operatorname{Conv}\left(m_3^{(1)}, m_4^{(1)}\right) & F_3^1 \cap M &= \left\{m_3^{(1)}, m_4^{(1)}\right\} \\
F_4^1 &= \operatorname{Conv}\left(m_2^{(1)}, m_4^{(1)}\right) & F_4^1 \cap M &= \left\{m_2^{(1)}, m_4^{(1)}\right\} \\
F_1^0 &= \operatorname{Conv}\left(m_1^{(1)}\right) & F_1^0 \cap M &= \left\{m_1^{(1)}\right\} \\
F_2^0 &= \operatorname{Conv}\left(m_2^{(1)}\right) & F_2^0 \cap M &= \left\{m_2^{(1)}\right\} \\
F_3^0 &= \operatorname{Conv}\left(m_3^{(1)}\right) & F_3^0 \cap M &= \left\{m_3^{(1)}\right\} \\
F_4^0 &= \operatorname{Conv}\left(m_4^{(1)}\right) & F_4^0 \cap M &= \left\{m_4^{(1)}\right\}
\end{aligned}$$

Let $L_F := \left\{l \in \mathbb{Z}^4 \middle| (m_i \notin F \implies l_i = 0) \wedge \sum_{i=1}^4 l_i \cdot \left(1, m_i^{(1)}\right) = 0\right\}$. Then $L_{F_1^2} = \langle (1,-1,-1,1) \rangle_{\mathbb{Z}}$ and $L_{F_i^d} = 0$ for $(d,i) \neq (2,1)$. We get the following homogeneous simple systems that describe an embedding of X_{P_1} into $\mathbb{P}^3$.

$$S_1^2 = \{(x_1)_{\neq}, (x_2)_{\neq}, (x_3)_{\neq}, (x_1x_4 - x_2x_3)_{=}\}$$

$$
\begin{aligned}
S_1^1 &= \{(x_1)_{\neq}, (x_2)_{=}, (x_3)_{\neq}, (x_4)_{=}\}\\
S_2^1 &= \{(x_1)_{\neq}, (x_2)_{\neq}, (x_3)_{=}, (x_4)_{=}\}\\
S_3^1 &= \{(x_1)_{=}, (x_2)_{=}, (x_3)_{\neq}, (x_4)_{\neq}\}\\
S_4^1 &= \{(x_1)_{\neq}, (x_2)_{=}, (x_3)_{=}, (x_4)_{\neq}\}\\
S_1^2 &= \{(x_1)_{\neq}, (x_2)_{=}, (x_3)_{=}, (x_4)_{=}\}\\
S_2^2 &= \{(x_1)_{=}, (x_2)_{\neq}, (x_3)_{=}, (x_4)_{=}\}\\
S_3^2 &= \{(x_1)_{=}, (x_2)_{=}, (x_3)_{\neq}, (x_4)_{=}\}\\
S_4^2 &= \{(x_1)_{=}, (x_2)_{=}, (x_3)_{=}, (x_4)_{\neq}\}
\end{aligned}
$$

This results in the projective counting polynomial $(u-1)^2 + 4(u-1) + 4 = u^2 + 2u + 1$.

The faces of P_2 are as follows.

$$
\begin{aligned}
G_1^2 &= P_2 & G_1^2 \cap M &= P_2 \cap M\\
G_1^1 &= \mathrm{Conv}\left(m_1^{(2)}, m_3^{(2)}\right) & G_1^1 \cap M &= \left\{m_1^{(2)}, m_3^{(2)}, m_8^{(2)}\right\}\\
G_2^1 &= \mathrm{Conv}\left(m_1^{(2)}, m_2^{(2)}\right) & G_2^1 \cap M &= \left\{m_1^{(2)}, m_2^{(2)}, m_7^{(2)}\right\}\\
G_3^1 &= \mathrm{Conv}\left(m_3^{(2)}, m_4^{(2)}\right) & G_3^1 \cap M &= \left\{m_3^{(2)}, m_4^{(2)}, m_9^{(2)}\right\}\\
G_4^1 &= \mathrm{Conv}\left(m_2^{(2)}, m_4^{(2)}\right) & G_4^1 \cap M &= \left\{m_2^{(2)}, m_4^{(2)}, m_6^{(2)}\right\}\\
G_1^0 &= \mathrm{Conv}\left(m_1^{(2)}\right) & G_1^0 \cap M &= \left\{m_1^{(2)}\right\}\\
G_2^0 &= \mathrm{Conv}\left(m_2^{(2)}\right) & G_2^0 \cap M &= \left\{m_2^{(2)}\right\}\\
G_3^0 &= \mathrm{Conv}\left(m_3^{(2)}\right) & G_3^0 \cap M &= \left\{m_3^{(2)}\right\}\\
G_4^0 &= \mathrm{Conv}\left(m_4^{(2)}\right) & G_4^0 \cap M &= \left\{m_4^{(2)}\right\}
\end{aligned}
$$

The module $L_{G_1^2}$ is generated by the rows of the matrix

$$
\begin{pmatrix}
1 & -2 & -2 & 0 & 1 & 1 & 0 & 0 & 1\\
0 & -1 & -1 & 0 & 0 & 1 & 0 & 1 & 0\\
0 & -2 & -1 & 0 & 1 & 1 & 1 & 0 & 0\\
1 & -2 & -1 & 0 & 0 & 2 & 0 & 0 & 0\\
0 & -1 & -1 & 0 & 2 & 0 & 0 & 0 & 0\\
1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
$$

Furthermore,

$$
\begin{aligned}
L_{G_1^1} &= \langle(-1,0,-1,0,0,0,0,2,0)\rangle_{\mathbb{Z}}\\
L_{G_2^1} &= \langle(-1,-1,0,0,0,0,2,0,0)\rangle_{\mathbb{Z}}\\
L_{G_3^1} &= \langle(0,0,-1,-1,0,0,0,0,2)\rangle_{\mathbb{Z}}\\
L_{G_4^1} &= \langle(0,-1,0,-1,0,2,0,0,0)\rangle_{\mathbb{Z}}
\end{aligned}
$$

and $L_{G_i^d} = 0$ for $d = 0$. The following homogeneous simple systems describe an embedding of X_{P_2} into $\mathbb{P}^8$.

$$
\begin{aligned}
T_1^2 = \{&(x_1)_{\neq}, (x_2)_{\neq}, (x_3)_{\neq}, (x_1x_4 - x_2x_3)_{=}, (x_5^2 - x_2x_3)_{=}, (x_1x_6^2 - x_2^2x_3)_{=},\\
&(x_5x_6x_7 - x_2^2x_3)_{=}, (x_6x_8 - x_2x_3)_{=}, (x_1x_5x_6x_9 - x_2^2x_3^2)_{=}\}\\
T_1^1 = \{&(x_1)_{\neq}, (x_2)_{=}, (x_3)_{\neq}, (x_4)_{=}, (x_5)_{=}, (x_6)_{=}, (x_7)_{=}, (x_8^2 - x_1x_3)_{=}, (x_9)_{=}\}
\end{aligned}
$$

$$T_2^1 = \{(x_1)_{\neq}, (x_2)_{\neq}, (x_3)_{=}, (x_4)_{=}, (x_5)_{=}, (x_6)_{=}, (x_7^2 - x_1x_2)_{=}, (x_8)_{=}, (x_9)_{=}\}$$
$$T_3^1 = \{(x_1)_{=}, (x_2)_{=}, (x_3)_{\neq}, (x_4)_{\neq}, (x_5)_{=}, (x_6)_{=}, (x_7)_{=}, (x_8)_{=}, (x_9^2 - x_3x_4)_{=}\}$$
$$T_4^1 = \{(x_1)_{=}, (x_2)_{\neq}, (x_3)_{=}, (x_4)_{\neq}, (x_5)_{=}, (x_6^2 - x_2x_4)_{=}, (x_7)_{=}, (x_8)_{=}, (x_9)_{=}\}$$
$$T_1^2 = \{(x_1)_{\neq}, (x_2)_{=}, (x_3)_{=}, (x_4)_{=}, (x_5)_{=}, (x_6)_{=}, (x_7)_{=}, (x_8)_{=}, (x_9)_{=}\}$$
$$T_2^2 = \{(x_1)_{=}, (x_2)_{\neq}, (x_3)_{=}, (x_4)_{=}, (x_5)_{=}, (x_6)_{=}, (x_7)_{=}, (x_8)_{=}, (x_9)_{=}\}$$
$$T_3^2 = \{(x_1)_{=}, (x_2)_{=}, (x_3)_{\neq}, (x_4)_{=}, (x_5)_{=}, (x_6)_{=}, (x_7)_{=}, (x_8)_{=}, (x_9)_{=}\}$$
$$T_4^2 = \{(x_1)_{=}, (x_2)_{=}, (x_3)_{=}, (x_4)_{\neq}, (x_5)_{=}, (x_6)_{=}, (x_7)_{=}, (x_8)_{=}, (x_9)_{=}\}$$

This results in the projective counting polynomial $4(u-1)^2 + 8(u-1) + 4 = 4u^2$. ◁

With these methods, we can compute examples that are significantly larger than what the Decompose algorithm can handle. In the affine case, the bottleneck is the computation of a generating set of the semi-group $\sigma^\vee$. For our examples, we used the MAPLE package convex (cf. [Fra09]) to compute a so-called HILBERT basis of the semigroup. This HILBERT basis is the unique minimal generating system of the semigroup and is contained in any generating set. Any tuple from $X \in M^s$ that includes all the members of the HILBERT basis fulfill the conditions of Lemma (5.28).

For the projective case, the bottleneck is determining the lattice points of the polytope. We only used a brute-force algorithm for this purpose, so larger examples may still be hard to compute.

As a final example, we consider a toric variety that is known for being hard to handle.

Example 5.36. Consider $n = 4$ and the rational cone $\sigma \subseteq \mathbb{R}^4$ generated generated by

$$((1,2,3,4), (0,1,0,7), (3,1,0,2), (0,0,1,0)) \in \left(\mathbb{Z}^4\right)^4 .$$

Using the convex package, we can compute the HILBERT basis of the semigroup $\sigma^\vee \cap \mathbb{Z}^4$. It is given by the following 29-tuple in M.

$$\big((0,1,0,0), (1,0,0,0), (0,0,1,0), (0,-2,0,1), (1,-4,1,1), (1,-5,2,1), (2,-6,2,1), (2,-7,3,1),$$
$$(-1,3,0,0), (3,-13,5,2), (-2,8,0,-1), (-1,7,0,-1), (2,-3,0,1), (3,-5,1,1), (4,-7,2,1),$$
$$(5,-14,5,2), (4,-4,0,1), (5,-6,1,1), (6,-21,8,3), (-3,14,0,-2), (5,-21,9,3), (7,-28,11,4),$$
$$(6,-5,0,1), (7,-7,1,1), (-5,21,0,-3), (8,-6,0,1), (10,-7,0,1), (10,-42,17,6),$$
$$(15,-63,25,9)\big)$$

From these, since σ has 16 faces, we obtain 16 simple systems over $\mathbb{Q}[x_1, \ldots, x_{29}]$ and the counting polynomial of the embedding is $(u-1)^4 + 4(u-1)^3 + 6(u-1)^2 + 4(u-1) + 1 = u^4$. Considering the generators reverse order yields the counting polynomial $25(u-1)^4 + 76(u-1)^3 + 54(u-1)^2 + 4(u-1) + 1 = 25u^4 - 24u^3 - 24u^2 + 24u$. In both cases, the overall computation takes less than 2 seconds.

Determining generators of the toric ideal from these systems using Definition (5.1) is infeasible. However, we can use 4ti2 (cf. [tt]) to determine a GROEBNER basis of the toric ideal from the relations of the elements of the HILBERT basis. This way, we can find a generating set of the toric ideal consisting of 341 binomials. From these ideal generators, we can compute the simple systems describing the embedding and the same counting polynomials as before, but the computation now takes more than 8 seconds.

In summary, we can describe the embedding using 16 simple systems, each containing at most four binomials and up to 12 equations or inequations of the form $(x_i)_=$ or $(x_i)_{\neq}$. This is much shorter than describing the embedding using the 341 binomials that generate the toric ideal. ◁

5.6 Constructible Sets

This section describes how sets from the class $\mathcal{P}$ can be interpreted from a geometric point of view. In particular, the solution sets $\mathcal{L}(S)$ and $\mathcal{L}^{\mathbb{P}}(S)$ of a disjoint family of simple systems S are

constructible subsets of affine and projective space, respectively. We demonstrate how to describe these constructible set by means of pairs of ideals.

For any ideal $I \trianglelefteq K[x_1, \ldots, x_n]$, we denote by $V(I) = \mathrm{Spec}(K[x_1, \ldots, x_n]/I)$ the affine subvariety of $\mathbb{A}^n$ defined by I. If $I \trianglelefteq K[x_0, \ldots, x_n]$ is a homogeneous ideal, we denote by $V^{\mathbb{P}}(I) = \mathrm{Proj}(K[x_0, \ldots, x_n]/I)$ the projective subvariety of $\mathbb{P}^n$ defined by I.

If $I, J \trianglelefteq R$ are ideals, then they define the **quasi-affine subset** $V(I) \setminus V(J) \subseteq \overline{K}^n$. We can also write this as $V(I) \cap \mathcal{C}V(J)$ which shows that a quasi-affine subset of $\overline{K}^n$ is open in its closure.

Remark 5.37. Let $G, U \subseteq R$ be finite such that $I = \langle G \rangle$ and $J = \langle U \rangle$. If $U = \{u_1, \ldots, u_s\}$, then define the systems V_i, $i = 1, \ldots, s$ as

$$V_i = \{g_= | g \in G\} \cup \left\{(u_1)_=, \ldots, (u_{i-1})_=, (u_i)_{\neq}\right\} .$$

Then $V(I) \setminus V(J) = \bigcup_{i=1}^{s} \mathcal{L}(V_i)$ and we represent $V(I) \setminus V(J)$ using a Thomas decomposition of the V_i which we denote by $S_{I,J}$. ◁

Notation 5.38. Denote by $\overline{S}$ a Thomas decomposition of $I(S)$, such that $\mathcal{L}\left(\overline{S}\right) = \overline{\mathcal{L}(S)}$. Further denote $S^c := \mathsf{Complement}(S)$ and $J(S) := I\left(\mathsf{Intersect}\left(S^c, \overline{S}\right)\right)$ ◁

Proposition 5.39. *Let S be a disjoint family of simple systems representing a quasi-affine subset of $\overline{K}^n$, $I = I(S)$ and $J = J(S)$. Then $\mathcal{L}(S) = V(I) \setminus V(J)$.*

Proof. Let $\mathbf{a} \in \mathcal{L}(S)$. Then $\mathbf{a} \in V(I) = \overline{\mathcal{L}(S)}$. Since $\mathbf{a} \notin \mathcal{L}(S^c)$ by definition, it follows that $\mathbf{a} \notin \mathcal{L}\left(\mathsf{Intersect}\left(S^c, \overline{S}\right)\right)$. As $\mathcal{L}(S)$ is open in its closure, its complement $\mathcal{L}(S^c) \cap \overline{\mathcal{L}(S)}$ is closed and thus $\mathbf{a} \notin \overline{\mathcal{L}\left(\mathsf{Intersect}\left(S^c, \overline{S}\right)\right)} = V(J)$.

Conversely, let $\mathbf{a} \notin \mathcal{L}(S)$. If $\mathbf{a} \in V(I)$, then clearly $\mathbf{a} \in V(I) \setminus \mathcal{L}(S) = \overline{\mathcal{L}(S)} \setminus \mathcal{L}(S)$. Thus, $\mathbf{a} \in V(J)$ by definition and therefore $\mathbf{a} \notin V(I) \setminus V(J)$. □

The second part of this proof does not depend on the solution set being quasi-affine, which results in the following corollary.

Corollary 5.40. *Let S be a disjoint family of simple systems and $I = I(S)$, $J = J(S)$. Then $V(I) \setminus V(J) \subseteq \mathcal{L}(S)$.*

Example 5.41. Let $K = \mathbb{Q}$, $\overline{K} = \mathbb{C}$ and consider the disjoint family of simple systems given by

$$S = \left(\{x_{\neq}, \}, \{x_=, (y^2 + 1)_=\}\right) .$$

This family does not represent a quasi-affine set. The closure of $\mathcal{L}(S)$ is $\mathbb{C}^2$. Since $J := J(S) = \langle x \rangle$, we get

$$V\left(\langle 0 \rangle\right) \setminus V\left(\langle x \rangle\right) = \mathcal{L}\left(\{x_{\neq}, \}\right) \subsetneq \mathcal{L}\left(S\right) .$$

In fact, there is no ideal J' such that $\mathcal{L}(S) = V\left(\langle 0 \rangle\right) \setminus V\left(J'\right)$. If such an ideal existed, then $V\left(J'\right) = \left\{(0, b) \in \mathbb{C}^2 \middle| b \notin \{i, -i\}\right\}$, which is not a Zariski-closed subset of $\mathbb{C}^2$. ◁

Unions and complements of quasi-affine subsets of $\overline{K}^n$ are not necessarily quasi-affine. A set is called **constructible set** if it is the union of finitely many quasi-affine sets and finitely many complements of quasi-affine sets. Every constructible set can be represented via a family of simple systems and vice versa.

Definition 5.42. Let S be a disjoint family of simple systems, $I = I(S)$ and $J = J(S)$. Furthermore, let Q, Q' be disjoint families of simple systems such that $\mathcal{L}(Q) = V(I) \setminus V(J)$ and $\mathcal{L}(Q') = \mathcal{L}(S) \setminus \mathcal{L}(Q)$.

Define the **quasi-affine decomposition** of S as (Q) if $\mathcal{L}(Q') = \emptyset$ and as the concatenation of (Q) with the quasi-affine decomposition of Q' otherwise. ◁

Note that in a quasi-affine decomposition $(Q_1, \ldots, Q_r)$, each $\mathcal{L}(Q_i)$ is by definition a quasi-affine set and $\mathcal{L}(S) = \biguplus_{i=1}^{r} \mathcal{L}(Q_i)$ as per Corollary (5.40). As a consequence, $\mathcal{L}(S)$ is quasi-affine if and only if its quasi-affine decomposition has at most one element.

As an alternative notation, we can describe the quasi-affine decomposition as a sequence of pairs of ideals $((I_1, J_1), \ldots, (I_r, J_r))$ such that $\mathcal{L}(Q_i) = V(I_i) \setminus V(J_i)$. We can compute both descriptions of the quasi-affine decomposition using the methods described in sections 3.4 and 5.1.

To demonstrate this, we reconsider Example (5.41).

Example 5.43. As before, let $K = \mathbb{Q}$, $\overline{K} = \mathbb{C}$ and consider $S = \left(\{x_{\neq},\}, \{x_{=}, (y^2+1)_{=}\}\right)$. We compute the quasi-affine decomposition in MAPLE.

```
> restart;
> with(AlgebraicThomas):
> L := [[x<>0],[x,y^2+1]]:
> S := AlgebraicThomasDecompositionMany(L,[x,y],quiet=true);
```

$$S := [[x \neq 0], [x = 0, y^2 + 1 = 0]]$$

This procedure computes the ideal $J(S)$.

```
> J := S->Closure(SolIntersect(Complement(S),Closure(S))):
```

We compute Q_1 and Q_1' as described in the previous Definition.

```
> Q1 := SolDifference(Closure(S),J(S)):
> Q1p := SolDifference(S,Q1):
> countingPolynomial(Q1p);
```

$$2$$

Since Q_1' is not empty, we continue computing Q_2 and Q_2'.

```
> Q2 := SolDifference(Closure(Q1p),J(Q1p)):
> Q2p := SolDifference(Q1p,Q2):
> countingPolynomial(Q2p);
```

$$0$$

Since Q_2' is empty, we conclude that Q_1'=Q_2 is quasi-affine and we are done.

```
> [Q1, Q2];
```

$$[[[x \neq 0]], [[x = 0, y^2 + 1 = 0]]]$$

Finally, we represent this quasi-affine decompositions using ideals.

```
> Ideals := S->[Ideal(S),Ideal(J(S))]:
> map(Ideals, [Q1, Q2]);
```

$$[[[0], [x]], [[x, y^2 + 1], [1]]]$$

This means that $\mathcal{L}(S) = (V(\langle 0\rangle) \setminus V(\langle x\rangle)) \uplus \left(V\left(\langle x, y^2+1\rangle\right) \setminus V(\langle 1\rangle)\right)$. ◁

Proposition 5.44. *If $(Q_1, \ldots, Q_r)$ and $(P_1, \ldots, P_s)$ are two quasi-affine decompositions of S, then $s = r$ and $\mathcal{L}(Q_i) = \mathcal{L}(P_i)$ for $i = 1, \ldots, r$.*

Proof. The closure of $\mathcal{L}(S)$ only depends on the set $\mathcal{L}(S) \subseteq \overline{K}^n$. Therefore, so do the ideals I and J from Definition (5.42) and thus Q_1 is equivalent to P_1. Since $\mathcal{L}(S) \setminus \mathcal{L}(Q_1) = \mathcal{L}(S) \setminus \mathcal{L}(P_1)$, the statement follows. □

Proposition 5.45. *If $(Q_1, \ldots, Q_r)$ is a quasi-affine decomposition of S, then*

$$\dim(Q_i) - \dim(Q_{i-1}) \geq 2$$

for $i = 2, \ldots, r$.

Proof. If $X = \mathcal{L}(S)$, $I = V(S)$ and $J(S)$ then

$$\begin{aligned} X \setminus (V(I) \setminus V(J)) &= (X \setminus V(I)) \cup (X \cap V(J)) \\ &= X \cap V(J) \end{aligned}$$

Since $V(J) = \overline{\overline{X} \setminus X}$ and $\dim\left(\overline{X} \setminus X\right) < \dim(X)$, we get $\dim\left(V\left(J\right)\right) \leq \dim\left(X\right) - 1$. Furthermore,

$$\begin{aligned} X \cap V(J) &= (X \cap V(J)) \cup \underbrace{\left(\mathcal{C}\overline{X} \cap V(J)\right)}_{=\emptyset} \\ &= V(J) \cap \left(X \cup \mathcal{C}\overline{X}\right) \\ &= V(J) \setminus \left(\mathcal{C}X \cap \overline{X}\right) \end{aligned}$$

Since $V(J) = \overline{\left(\mathcal{C}X \cap \overline{X}\right)}$, this implies $\dim(X \cap V(J)) < \dim(V(J))$ and therefore

$$\dim\left(X \cap V(J)\right) \leq \dim(X) - 2\ . \qquad \square$$

The quasi-affine decomposition is a useful tool to represent a constructible set, especially since it shows if a set is quasi-affine. The following example demonstrates a disadvantage which is apparent from the previous proposition.

Example 5.46. Let $R = \mathbb{Q}[x, y, z]$ and define the ideals $I_1 = \langle z \rangle$, $I_2 = \langle y \rangle$ and $I_3 = \langle z - y, z - x \rangle$. The constructible set $X = (V(I_1) \setminus V(I_2)) \cup (V(I_2) \setminus V(I_1)) \cup V(I_3)$ has dimension 2. However, the quasi-affine decomposition

$$\underbrace{V\left(\langle zy(z-y), zy(x-y)\rangle\right) \setminus V\left(\langle y, z\rangle\right)}_{\dim(\cdot)=2} \biguplus \underbrace{V\left(\langle x, y, z\rangle\right)}_{\dim(\cdot)=0}$$

contains no indication that X is actually the union of surfaces and lines.

On the other hand, the set X may be decomposed as the disjoint union of the quasi-affine sets

$$\underbrace{V\left(\langle yz\rangle\right) \setminus V\left(\langle y, z\rangle\right)}_{\dim(\cdot)=2} \biguplus \underbrace{V\left(\langle y - x, z - x\rangle\right)}_{\dim(\cdot)=1}$$

which separates the line from the two surfaces. $\triangleleft$

The following algorithm computes a different decomposition into quasi-affine sets that takes the dimension into account.

Algorithm 5.47 (EquidimensionalQuasiAffineDecomposition)**.** *Input: A disjoint family of simple systems S over $K[x_1, \ldots, x_n]$.*
Output: A tuple $(D_1, \ldots, D_k)$ of disjoint families of simple systems, where

(a) $\dim(D_i) > \dim(D_{i+1})$,

(b) $I(D_i)$ *is equidimensional with dimension* $\dim(D_i)$,

(c) $\mathcal{L}(D_i)$ *is a quasi-affine subset of* $\overline{K}^n$ *and*

(d) $\mathcal{L}(S) = \biguplus_{i=1}^{k} \mathcal{L}(D_i)$, $i = 1, \ldots, k-1$.

Algorithm:

1: $D \leftarrow ()$
2: ***while*** $\mathcal{L}(S) \neq \emptyset$ ***do***
3: $\quad S_{\max} \leftarrow (s \in S | \dim(s) = \dim(S))$
4: $\quad I_{\max} \leftarrow I(S_{\max})$
5: $\quad T \leftarrow (s \in S | \mathsf{Reduce}(s, p) = 0$ *for all* $p \in I_{\max})$

6: $J \leftarrow I\left(\mathsf{Intersect}\left(\mathsf{Complement}(T), \overline{T}\right)\right)$
7: $Q \leftarrow \mathcal{S}_{I_{\max},J}$
8: $D \leftarrow (D,(Q))$
9: $S \leftarrow \mathsf{Difference}(S,Q)$
10: ***end while***
11: ***return*** D

Proof of Correctness. Let $d = \dim(S)$. The ideal $I_{\max}$ is given by $I_{\max} = \bigcap_{s \in S_{\max}} I(s)$. Therefore, it is the intersection of equidimensional ideals of dimension d, and thus itself equidimensional of dimension d. By construction, we have $I(T) = I_{\max} = I(Q)$, which proves (b).

The set $\mathcal{L}(Q)$ is a quasi-affine subset of $\overline{K}^n$ by construction, proving (c). Condition (d) is also true by construction.

For condition (a), it suffices to show that $\dim(\mathsf{Difference}(S,Q)) < \dim(S)$. It holds that $\mathcal{L}(Q) \subseteq \mathcal{L}(T) \subseteq \mathcal{L}(S)$. Therefore $\mathcal{L}(S) \setminus \mathcal{L}(Q) = (\mathcal{L}(S) \setminus \mathcal{L}(T)) \cup (\mathcal{L}(T) \setminus \mathcal{L}(Q))$. By construction $T \subseteq S$, i.e. every system in T also occurs in S, therefore $\mathcal{L}(S) \setminus \mathcal{L}(T) = \mathcal{L}(S \setminus T)$, and every system in $S \setminus T$ has dimension smaller than d. Finally, $\mathcal{L}(Q) = V(I(T)) \setminus V(J(T))$, and by the proof of Proposition (5.45), this implies $\dim(\mathcal{L}(T) \setminus \mathcal{L}(Q)) < \dim(\mathcal{L}(T)) = d$. □

This decomposition cannot test whether a set is quasi-affine, but it gives another representation of a set from the class $\mathcal{P}$. As before, we can express the quasi-affine sets using pairs of ideals.

Example 5.48. We compute Example (5.46) in MAPLE.

```
> restart;
> with(AlgebraicThomas):
> v := [x,y,z]:
> I1 := [z];
```

$$I1 := [z]$$

```
> I2 := [y];
```

$$I2 := [y]$$

```
> I3 := [z-y,z-x];
```

$$I3 := [z-y, z-x]$$

This defines the set from Example (5.46).

```
> S := SolUnion(
>    SolDifference(
>     AlgebraicThomasDecomposition(I1,v),
>     AlgebraicThomasDecomposition(I2,v)
>    ),
>    SolDifference(
>     AlgebraicThomasDecomposition(I2,v),
>     AlgebraicThomasDecomposition(I1,v)
>    ),
>    AlgebraicThomasDecomposition(I3,v)
> ):
> Dimension(S);
```

$$2$$

We follow the algorithm and find the quasi-affine set of dimension two.

```
> M := select(s->Dimension(s)=2, S):
> IM := Ideal(M):
> T := select(s->`and`(op(map(p->evalb(reduce(p,s)=0),IM))), S):
> J := Closure(SolIntersect(Complement(T),Closure(T))):
> D1 := [IM,Ideal(J)]:
```

```
> S1 := SolDifference(
>    S,
>    SolDifference(AlgebraicThomasDecomposition(IM,v),Closure(J))
> ):
> Dimension(S1);
```

$$1$$

We continue with dimension 1.

```
> M := select(s->Dimension(s)=1, S1):
> IM := Ideal(M):
> T := select(s->`and`(op(map(p->evalb(reduce(p,s)=0),IM))), S1):
> J := Closure(SolIntersect(Complement(T),Closure(T))):
> D2 := [IM,Ideal(J)]:
> S2 := SolDifference(
>    S1,
>    SolDifference(AlgebraicThomasDecomposition(IM,v),Closure(J))
> ):
> Dimension(S2);
```

$$-\infty$$

After removing the components of dimension 1, the set is empty. The equidimensional quasi-affine decomposition is represented by the following pairs of ideals:

```
> [D1,D2];
```

$$[[[zy],[y,z]],[[x-z,y-z],[1]]]$$

◁

5.7 Images of Rational Maps

This section will focus on applying the THOMAS decomposition and counting polynomial to the study of rational maps. In particular, we will give examples of such maps and use the AlgebraicThomas software to compute their image and determine whether they are surjective.

Let K be a field, $m, n \in \mathbb{N}$ and consider two sets $M \in \mathcal{P}_K^m$, $N \in \mathcal{P}_K^n$. We will use the THOMAS decomposition for analyzing rational maps

$$f : M \to N : (a_1, \ldots, a_m) \mapsto (p_1(a_1, \ldots, a_m), \ldots, p_n(a_1, \ldots, a_m))$$

where $p_i = \frac{n_i}{d_i} \in K(x_1, \ldots, x_m)$ and $n_i, d_i \in K[x_1, \ldots, x_m]$ for $i = 1, \ldots, n$. For simplicity, assume that both M and N are given by a single polynomial system.

Remark 5.49. We can use THOMAS decomposition to check whether the p_i induce a well-defined map $M \to N$. Consider systems T_1 over $K[x_1, \ldots, x_m]$ and T_2 over $K[y_1, \ldots, y_n]$ with $\mathcal{L}(T_1) = M$ and $\mathcal{L}(T_2) = N$. Define the system

$$S := T_1 \cup T_2 \cup \left\{ (d_i y_i - n_i)_= , (d_i)_{\neq} \middle| i = 1, \ldots, n \right\}$$

over $K[x_1, \ldots, x_m, y_1, \ldots, y_n]$. Then the p_i induce a well-defined map $M \to N$ if and only if $\mathcal{L}(\mathsf{Project}(S, m)) = \mathcal{L}(M)$. Since $M \subseteq \mathsf{Project}(S, m)$ we only need to test equality of $c(M)$ and $c(\mathsf{Project}(S, m))$.

If we interpret S as a system over $K[y_1, \ldots, y_n, x_1, \ldots, x_m]$, then $\mathcal{L}(\mathsf{Project}(S, n)) \subseteq N$ is the image of f. We can determine whether the map is surjective by comparing the counting polynomials $c(\mathcal{L}(\mathsf{Project}(S, n)))$ and $c(N)$. ◁

As a first example, we will show how the THOMAS decomposition can be used to discover the determinant, Cramer's rule and the counting polynomial computed in Proposition (4.6). In this case, we do not know have explicit formulas for the p_i in advance, but define them implicitly by means of the equation $AB - 1 = 0$.

Example 5.50. Let

$$A = (a_{i,j})_{i,j=1,\dots,n}, B = (b_{i,j})_{i,j=1,\dots,n} \in \mathbb{Q}\left[a_{i,j}, b_{i,j} | i,j = 1,\dots,n\right]^{n\times n}$$

and consider the equation $AB - 1 = 0$. This matrix multiplication yields n^2 polynomial equations. By performing a THOMAS decomposition with a ranking $<$ such that $a_{i,j} < b_{i,j}$ we can analyze the map $A \mapsto \frac{1}{A}$. We consider the case $n = 3$.

```
> restart:
> with(AlgebraicThomas):
> (A,B):=Matrix(3,symbol=a),Matrix(3,symbol=b);
```

$$A,\, B := \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}, \begin{bmatrix} b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}$$

```
> v := [op(indets(B)),op(indets(A))];
```

$$v := [b_{1,1}, b_{1,2}, b_{1,3}, b_{2,1}, b_{2,2}, b_{2,3}, b_{3,1}, b_{3,2}, b_{3,3}, a_{1,1}, a_{1,2}, a_{1,3}, a_{2,1}, a_{2,2}, a_{2,3}, a_{3,1}, a_{3,2}, a_{3,3}]$$

```
> S:=AlgebraicThomasDecomposition(convert(A.B-1,list),v):
```

From this decomposition, we first determine that our implicit description yields a map.

```
> G:=groupCounting(Comprehensive(S,9)):
> nops(G);
```

$$1$$

```
> G[1][2];
```

$$1$$

This means that for every matrix A there is exactly one matrix B such that our implicit equations hold, thus proving that they define a map. We consider the largest subset of $\mathbb{Q}\left[a_{i,j} | i,j = 1,\dots,3\right]$ such that this map is well-defined.

```
> Sp := Project(S,9):
> countingPolynomial(Sp);
```

$$u^9 - u^8 - u^7 + u^5 + u^4 - u^3$$

This is the counting polynomial we computed in Proposition (4.6). We want to determine the defining equations and inequations to see if it is the same set. For that, we consider the complement.

```
> Spc := Complement(Sp):
> evalb(countingPolynomial(Spc) = countingPolynomial(Closure(Spc)));
```

$$\mathit{true}$$

This shows that the complement is closed, i.e. defined by equations only. Those equations can be computed by determining the ideal of the set.

```
> Ideal(Spc);
```

$$[a_{1,1}a_{2,2}a_{3,3} - a_{1,1}a_{2,3}a_{3,2} - a_{1,2}a_{2,1}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,3}a_{2,2}a_{3,1}]$$

This is the determinant of A. What remains is to determine an explicit description of the map. We look for a system that only restricts the $a_{i,j}$ with inequations, i.e. a system that contains no equations in the $a_{i,j}$ only. In this case, such a system must have maximal dimension.

```
> map(Dimension, S);
```

$$[9, 8, 8, 7, 8, 7, 6, 8, 7, 7, 6, 8, 7, 7, 6, 7, 6, 7, 6, 6]$$

By looking at the first system, we can now determine our formula.

```
> isolate(getTermForVariable(S[1], b[1,1]),b[1,1]);
```

$$b_{1,1} = \frac{a_{2,2}a_{3,3} - a_{2,3}a_{3,2}}{a_{1,1}a_{2,2}a_{3,3} - a_{1,1}a_{2,3}a_{3,2} - a_{1,2}a_{2,1}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,3}a_{2,2}a_{3,1}}$$

```
> isolate(getTermForVariable(S[1], b[1,2]),b[1,2]);
```

$$b_{1,2} = \frac{-a_{1,2}a_{3,3} + a_{1,3}a_{3,2}}{a_{1,1}a_{2,2}a_{3,3} - a_{1,1}a_{2,3}a_{3,2} - a_{1,2}a_{2,1}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,3}a_{2,2}a_{3,1}}$$

Similar formulas hold for all $b_{i,j}$ and we have in fact recovered Cramer's rule. ◁

We now want to study maps of the form $K^{n\times n} \to K^{n\times n} : A \mapsto p(A)$ where $p \in K[x]$ is a polynomial. In particular, we want to determine the image and some interesting fibers of the map. Since all matrices are conjugates of upper triangular matrices and conjugation of matrices commutes with polynomial maps, we can simplify the computation by restricting ourselves to upper triangular matrices, in particular, we study maps of the form

$$K_{\mathrm{u}}^{n\times n} \to K_{\mathrm{u}}^{n\times n} : A \mapsto p(A)$$

where $K_{\mathrm{u}}^{n\times n}$ denotes the set of all upper triangular $n \times n$ matrices.

Example 5.51. Let $s, t \in \mathbb{C}$ and $f_{s,t} : \mathbb{C}^{2\times 2} \to \mathbb{C}^{2\times 2} : A \mapsto A^2 + sA + t$.

```
> restart:
> with(AlgebraicThomas):
> A := Matrix(2,symbol=a,shape=triangular[upper]);
```

$$A := \begin{bmatrix} a_{1,1} & a_{1,2} \\ 0 & a_{2,2} \end{bmatrix}$$

```
> B := Matrix(2,symbol=b,shape=triangular[upper]);
```

$$B := \begin{bmatrix} b_{1,1} & b_{1,2} \\ 0 & b_{2,2} \end{bmatrix}$$

```
> p := A->A^2+s*A+<<t,0>|<0,t>>:
> pA := p(A):
> L := convert(B-pA,list):
> v := [op(indets(A)),op(indets(B)),t,s];
```

$$v := [a_{1,1}, a_{1,2}, a_{2,2}, b_{1,1}, b_{1,2}, b_{2,2}, t, s]$$

```
> S := AlgebraicThomasDecomposition(L,v):
```

We are only interested in the image of $f_{s,t}$, therefore we can remove the highest three components.

```
> Sp := Project(S, 5):
```

We want to analyze this image depending on s, t, thus we need to make the decomposition (s, t)-comprehensive.

```
> Spc := Comprehensive(Sp, 2, group=false):
```

We now group together all systems where $\mathcal{L}\left(S_{<b_{2,2}}\right)$ is the same in order to analyze the different cases.

```
> Sg0 := [ListTools[Categorize](
>              (a,b)->equalSystem(Project(a,2),Project(b,2)),
>              Spc
>          )]:
> nops(Sg0);
```

1

There is only one case. We determine the complement of the image.

```
> Complement(Sg0[1],parameters=2);
> systemSolutions(%[1]);
```

$$[[s^2 + 4\,b_{1,1} - 4\,t = 0, b_{1,2} \neq 0, s^2 + 4\,b_{2,2} - 4\,t = 0]]$$

$$[[b_{1,1} = -\frac{1}{4}\,s^2 + t, b_{2,2} = -\frac{1}{4}\,s^2 + t]]$$

This shows that the matrix

```
> Z := subs(%[1], B);
```

$$Z := \begin{bmatrix} -\frac{1}{4}\,s^2 + t & b_{1,2} \\ 0 & -\frac{1}{4}\,s^2 + t \end{bmatrix}$$

with $b_{1,2} \neq 0$ is not in the image of $f_{s,t}$. The reason is as follows. If we compute a solution for $a_{1,1}$ and $a_{2,2}$, we get the following.

```
> solve(pA[1,1]-Z[1,1],a[1,1]);
> solve(pA[2,2]-Z[2,2],a[2,2]);
```

$$-\frac{1}{2}\,s, -\frac{1}{2}\,s$$

$$-\frac{1}{2}\,s, -\frac{1}{2}\,s$$

Inserting this solution into the upper right entry of the result always yields zero.

```
> subs([a[1,1]=-s/2, a[2,2]=-s/2], pA[1,2]);
```

$$0$$

If we had more than one solution for either $a_{1,1}$ or $a_{2,2}$, then we could always choose $a_{1,1}$ and $a_{2,2}$ such that finding a suitable $a_{1,2}$ is possible.

```
> pA[1,2]=b[1,2];
> isolate(%,a[1,2]);
```

$$s a_{1,2} + a_{1,1} a_{1,2} + a_{1,2} a_{2,2} = b_{1,2}$$

$$a_{1,2} = \frac{b_{1,2}}{a_{1,1} + a_{2,2} + s}$$

Therefore, candidates for the matrices with an empty fiber are the ones where the discriminant of

```
> x^2+s*x+t-b[1,1];
> x^2+s*x+t-b[2,2];
```

$$sx + x^2 + t - b_{1,1}$$

$$sx + x^2 + t - b_{2,2}$$

is identically zero. This is the case if

```
> isolate(discrim(x^2+s*x+t-b[1,1],x),b[1,1]);
> isolate(discrim(x^2+s*x+t-b[2,2],x),b[2,2]);
```

$$b_{1,1} = -\frac{1}{4}\,s^2 + t$$

$$b_{2,2} = -\frac{1}{4}\,s^2 + t$$

All other matrices are in the image of $f_{s,t}$. We analyze their fibers.

```
> Sc := Comprehensive(S, 5):
> fib := map(a->[SmallerDecomposition(a[1]),a[2]], groupCounting(Sc)):
> nops(fib);
```

$$4$$

The first case is the generic case, where each fiber has 4 elements.

```
> fib[1];
```

$$[[[4\,{b_{1,1}}^2 + \left(s^2 - 4\,t - 4\,b_{2,2}\right) b_{1,1} + \left(-s^2 + 4\,t\right) b_{2,2} \neq 0, s^2 + 4\,b_{2,2} - 4\,t \neq 0]], 4]$$

In the second case, the fiber has 2 elements.

```
> printSystem(fib[2][1],pretty=true);
> fib[2][2];
```

$$[s^2 + 4\,b_{1,1} - 4\,t = 0, s^2 + 4\,b_{2,2} - 4\,t \neq 0]$$

$$[b_{1,1} - b_{2,2} = 0, b_{1,2} \neq 0, s^2 + 4\,b_{2,2} - 4\,t \neq 0]$$

$$[s^2 + 4\,b_{1,1} - 4\,t \neq 0, s^2 + 4\,b_{2,2} - 4\,t = 0]$$

$$2$$

This is the case if exactly one of the following three conditions holds:
1. The discriminant

```
> discrim(x^2+s*x+t-b[1,1],x);
```

$$s^2 + 4\,b_{1,1} - 4\,t$$

is identically zero.
2. The discriminant

```
> discrim(x^2+s*x+t-b[2,2],x);
```

$$s^2 + 4\,b_{2,2} - 4\,t$$

is identically zero.
3. Both diagonal entries are identical.

In the third case, the fiber is infinite.

```
> fib[3];
```

$$[[[b_{1,1} - b_{2,2} = 0, b_{1,2} = 0, s^2 + 4\,b_{2,2} - 4\,t \neq 0]], 2\,u + 2]$$

We analyze such a fiber.

```
> map(op@(a->a[2]), select(s->equalSystem(s[1],fib[3][1][1]), Sc)):
> mat3 := map(subs, map(op@systemSolutions, %), A):
> printSystem(%%, pretty=true);
```

$$[a_{1,1} + a_{2,2} + s = 0, a_{1,2} \neq 0, {a_{2,2}}^2 + s a_{2,2} - b_{2,2} + t = 0]$$

$$[{a_{1,1}}^2 + s a_{1,1} - b_{2,2} + t = 0, a_{1,2} = 0, {a_{2,2}}^2 + s a_{2,2} - b_{2,2} + t = 0]$$

```
> nops(mat3);
```

$$6$$

We get the 4 obvious diagonal matrices.

```
> for M in mat3[3..6] do
> print(M, simplify(p(M)));
> od;
```

$$\left[\begin{array}{cc} -\frac{1}{2}\,s + \frac{1}{2}\,\sqrt{s^2 + 4\,b_{2,2} - 4\,t} & 0 \\ 0 & -\frac{1}{2}\,s + \frac{1}{2}\,\sqrt{s^2 + 4\,b_{2,2} - 4\,t} \end{array}\right], \left[\begin{array}{cc} b_{2,2} & 0 \\ 0 & b_{2,2} \end{array}\right]$$

$$\left[\begin{array}{cc} -\frac{1}{2}\,s - \frac{1}{2}\,\sqrt{s^2 + 4\,b_{2,2} - 4\,t} & 0 \\ 0 & -\frac{1}{2}\,s + \frac{1}{2}\,\sqrt{s^2 + 4\,b_{2,2} - 4\,t} \end{array}\right], \left[\begin{array}{cc} b_{2,2} & 0 \\ 0 & b_{2,2} \end{array}\right]$$

$$\left[\begin{array}{cc} -\frac{1}{2}\,s + \frac{1}{2}\,\sqrt{s^2 + 4\,b_{2,2} - 4\,t} & 0 \\ 0 & -\frac{1}{2}\,s - \frac{1}{2}\,\sqrt{s^2 + 4\,b_{2,2} - 4\,t} \end{array}\right], \left[\begin{array}{cc} b_{2,2} & 0 \\ 0 & b_{2,2} \end{array}\right]$$

$$\left[\begin{array}{cc} -\frac{1}{2}\,s - \frac{1}{2}\,\sqrt{s^2 + 4\,b_{2,2} - 4\,t} & 0 \\ 0 & -\frac{1}{2}\,s - \frac{1}{2}\,\sqrt{s^2 + 4\,b_{2,2} - 4\,t} \end{array}\right], \left[\begin{array}{cc} b_{2,2} & 0 \\ 0 & b_{2,2} \end{array}\right]$$

For each arbitrary $b_{1,2} \neq 0$ we get two more matrices.

```
> for M in mat3[1..2] do
> print(M, simplify(p(M)));
> od;
```

$$\left[\begin{array}{cc} -\frac{1}{2}\,s-\frac{1}{2}\,\sqrt{s^2+4\,b_{2,2}-4\,t} & a_{1,2} \\ 0 & -\frac{1}{2}\,s+\frac{1}{2}\,\sqrt{s^2+4\,b_{2,2}-4\,t} \end{array}\right], \left[\begin{array}{cc} b_{2,2} & 0 \\ 0 & b_{2,2} \end{array}\right]$$
$$\left[\begin{array}{cc} -\frac{1}{2}\,s+\frac{1}{2}\,\sqrt{s^2+4\,b_{2,2}-4\,t} & a_{1,2} \\ 0 & -\frac{1}{2}\,s-\frac{1}{2}\,\sqrt{s^2+4\,b_{2,2}-4\,t} \end{array}\right], \left[\begin{array}{cc} b_{2,2} & 0 \\ 0 & b_{2,2} \end{array}\right]$$

In the fourth case, the fiber is again infinite.

```
> fib[4];
```

$$[[[s^2+4\,b_{1,1}-4\,t=0, b_{1,2}=0, s^2+4\,b_{2,2}-4\,t=0]], u]$$

```
> map(op@(a->a[2]), select(s->equalSystem(s[1],fib[4][1][1]), Sc));
> mat4 := map(subs, map(op@systemSolutions, %), A):
```

$$[[2\,a_{1,1}+s=0, a_{1,2}\neq 0, 2\,a_{2,2}+s=0], [2\,a_{1,1}+s=0, a_{1,2}=0, 2\,a_{2,2}+s=0]]$$

For arbitrary $a_{1,2}$, the following matrix is in the fiber.

```
> mat4[1], simplify(p(mat4[1]));
```

$$\left[\begin{array}{cc} -\frac{1}{2}\,s & a_{1,2} \\ 0 & -\frac{1}{2}\,s \end{array}\right], \left[\begin{array}{cc} -\frac{1}{4}\,s^2+t & 0 \\ 0 & -\frac{1}{4}\,s^2+t \end{array}\right]$$

◁

The special cases in the previous example all occur when the discriminant of $x^2+sx+t-e$ is identically zero where e is an Eigenvalue of the result matrix. We consider the same problem with a polynomial of degree 3 where a similar phenomenon occurs.

Example 5.52. We want to determine for which $r, s, t \in \mathbb{C}$ the map

$$f_{r,s,t} : \mathbb{C}_{\mathrm{u}}^{2\times 2} \to \mathbb{C}_{\mathrm{u}}^{2\times 2} : A \mapsto A^3 + rA^2 + sA + t$$

is surjective. In case it is not, we want to determine the image of $f_{r,s,t}$.

```
> restart:
> with(AlgebraicThomas):
> A := Matrix(2,symbol=a,shape=triangular[upper]);
```

$$A := \left[\begin{array}{cc} a_{1,1} & a_{1,2} \\ 0 & a_{2,2} \end{array}\right]$$

```
> B := Matrix(2,symbol=b,shape=triangular[upper]);
```

$$B := \left[\begin{array}{cc} b_{1,1} & b_{1,2} \\ 0 & b_{2,2} \end{array}\right]$$

```
> p := A->A^3+r*A^2+s*A+<<t,0>|<0,t>>:
> pA := p(A):
> L := convert(B-pA,list):
> v := [op(indets(A)),op(indets(B)),t,s,r];
```

$$v := [a_{1,1}, a_{1,2}, a_{2,2}, b_{1,1}, b_{1,2}, b_{2,2}, t, s, r]$$

```
> S := AlgebraicThomasDecomposition(L,v):
```

As in the previous example, we are only interested in the image of $f_{r,s,t}$, therefore we can remove the highest three components.

```
> Sp := Project(S, 6):
```

We make the decomposition (r, s, t)-comprehensive.

```
> Spc := Comprehensive(Sp,3, group=false):
```

We now group together all systems where $\mathcal{L}\left(S_{<b_{2,2}}\right)$ is the same in order to analyze the different cases.

```
> Sg0 := [ListTools[Categorize](
>              (a,b)->equalSystem(Project(a,3),Project(b,3)),
>              Spc)
>           ]:
```

For each such case, we now determine the complement of the image.

```
> Sg := map(a->[Project(a[1],3),Complement(a,parameters=3)], Sg0):
```

```
> nops(Sg);
```

$$2$$

For almost all r, s, t, the map $f_{r,s,t}$ is surjective.

```
> Sg[1];
```

$$[[-r^2+3\,s\neq 0],[]]$$

For certain r, s, t, the following matrix is not in the image of $f_{r,s,t}$, where $b_{1,2}\neq 0$.

```
> Sg[2];
```

$$[[-r^2+3\,s=0],[[27\,b_{1,1}+r^3-27\,t=0, b_{1,2}\neq 0, 27\,b_{2,2}+r^3-27\,t=0, -r^2+3\,s=0]]]$$

```
> systemSolutions(Sg[2][2]);
> map(subs, %, B);
```

$$[[b_{1,1}=-\frac{1}{27}\,r^3+t, b_{2,2}=-\frac{1}{27}\,r^3+t, s=\frac{1}{3}\,r^2]]$$

$$[\begin{bmatrix} -\frac{1}{27}\,r^3+t & b_{1,2} \\ 0 & -\frac{1}{27}\,r^3+t \end{bmatrix}]$$

The reason is similar to the previous example. The polynomial

```
> subs(s=r^2/3, x^3+r*x^2+s*x+t - (-1/27*r^3+t));
```

$$x^3+rx^2+\frac{1}{3}\,r^2x+\frac{1}{27}\,r^3$$

has discriminant zero.

```
> simplify(discrim(%,x));
```

$$0$$

In fact, it has only one distinct root.

```
> factor(%%);
```

$$\frac{1}{27}\,(r+3\,x)^3$$

The previous example explains how this results in an empty fiber.

We analyze the cardinalities of the fibers.

```
> Comprehensive(S, [6,3]):
> fib := map(a->[a[1], groupCounting(a[2])], %):
```

```
> nops(fib);
```

$$2$$

We start with the generic case.

```
> fib[1][1];
```

$$[-r^2+3\,s\neq 0]$$

```
> map(a->[countingPolynomial(a[1]),a[2]], fib[1][2]);
> add(p[1], p=%);
```

$$[[u^3 - 5\,u^2 + 6\,u, 9], [4\,u^2 - 8\,u, 6], [u^2 - 3\,u + 2, 3], [u - 2, 6\,u + 3], [2\,u, 4], [2\,u - 2, 1], [2, 3\,u + 1]]$$

$$u^3$$

We see that generically, the fiber is finite with 9 elements. In some cases, the fiber may be smaller. In two cases however, the fiber is infinite.

```
> fib[1][2][4][1];
```

$$[[b_{1,1} - b_{2,2} = 0, b_{1,2} = 0, 27\,{b_{2,2}}^2 + \left(-4\,r^3 + 18\,rs - 54\,t\right) b_{2,2} + 4\,r^3 t - r^2 s^2 - 18\,rst + 4\,s^3 + 27\,t^2 \neq 0]]$$

```
> fib[1][2][7][1];
```

$$[[b_{1,1} - b_{2,2} = 0, b_{1,2} = 0, 27\,{b_{2,2}}^2 + \left(-4\,r^3 + 18\,rs - 54\,t\right) b_{2,2} + 4\,r^3 t - r^2 s^2 - 18\,rst + 4\,s^3 + 27\,t^2 = 0]]$$

This shows that all scalar matrices have an infinite fiber. Now consider the special case.

```
> fib[2][1];
```

$$[-r^2 + 3\,s = 0]$$

```
> map(a->[countingPolynomial(a[1]),a[2]], fib[2][2]);
> add(p[1], p=%);
```

$$[[u^3 - 3\,u^2 + 2\,u, 9], [3\,u^2 - 4\,u + 1, 3], [u - 1, 6\,u + 3], [1, u]]$$

$$u^3 - u + 1$$

Again, the fiber has 9 elements generically, but is smaller in some cases. From the last counting polynomial, we see again that some fibers are empty. As above, there are two cases where the fiber is infinite.

```
> fib[2][2][3][1];
```

$$[[b_{1,1} - b_{2,2} = 0, b_{1,2} = 0, 27\,b_{2,2} + r^3 - 27\,t \neq 0]]$$

```
> fib[2][2][4][1];
```

$$[[27\,b_{1,1} + r^3 - 27\,t = 0, b_{1,2} = 0, 27\,b_{2,2} + r^3 - 27\,t = 0]]$$

As before, these are all scalar matrices. This is plausible since the upper right entry of $f_{r,s,t}\mathrm{A}$ is

```
> collect(pA[1,2], [a[1,2],s,r], expand);
```

$$\left(s + r\left(a_{1,1} + a_{2,2}\right) + {a_{1,1}}^2 + a_{2,2}a_{1,1} + {a_{2,2}}^2\right) a_{1,2}$$

The result of the computation implies that for given $b_{1,1}$, $b_{2,2}$, there are $a_{1,1}$, $a_{2,2}$ that solve the system and ensure that the coefficient of $a_{1,2}$ in the above polynomial is identically zero. Therefore, there is no equation to restrict $a_{1,2}$ in these cases and the counting polynomial has degree 1. ◁

To conclude this discussion, we will now consider the previous examples in positive characteristic and compare the results.

Example 5.53. We analyze the image of the map $g_{s,t} : \left(\overline{\mathbb{F}_2}\right)_{\mathrm{u}}^{2\times 2} \to \left(\overline{\mathbb{F}_2}\right)_{\mathrm{u}}^{2\times 2} : A \mapsto A^2 + sA + t$. The steps to compute this in MAPLE are almost identical to the ones in Example (5.51).

```
> restart:
> with(AlgebraicThomas):
```

We set the characteristic to 2 and perform the same steps as before.

```
> AlgebraicThomasOptions("characteristic", 2);
> A := Matrix(2,symbol=a,shape=triangular[upper]):
> B := Matrix(2,symbol=b,shape=triangular[upper]):
> p := A->A^2+s*A+<<t,0>|<0,t>>:
> pA := p(A):
> L := convert(B-pA,list):
> v := [op(indets(A)),op(indets(B)),t,s]:
> S := AlgebraicThomasDecomposition(L,v):
> Sp := Project(S, 5):
```

```
> Spc := Comprehensive(Sp,2, group=false):
> Sg0 := [ListTools[Categorize](
>              (a,b)->equalSystem(Project(a,2),Project(b,2)),
>              Spc)
>            ]:
> Sg := map(a->[Project(a[1],2),Complement(a,parameters=2)], Sg0);
```

$$Sg := [[[s \neq 0], []], [[s = 0], [[b_{1,1} + b_{2,2} = 0, b_{1,2} \neq 0, s = 0]]]]$$

This behaviour is different from characteristic 0. In fact, the map is surjective if $s \neq 0$. If $s = 0$, all non-diagonal matrices with two identical Eigenvalues have an empty fiber. This is because after choosing values for s, t, the discriminant of

```
> x^2+s*x+t-e;
```

$$sx + x^2 - e + t$$

is always s, in particular, it does not depend on e.

Finally, we consider $g_{r,s,t} : \left(\overline{\mathbb{F}_3}\right)_{\mathrm{u}}^{2\times 2} \to \left(\overline{\mathbb{F}_3}\right)_{\mathrm{u}}^{2\times 2} : A \mapsto A^3 + rA^2 + sA + t$ and compare with Example (5.52).

```
> restart:
> with(AlgebraicThomas):
```

We perform the same steps as before for characteristic 3 and a polynomial of degree 3.

```
> AlgebraicThomasOptions("characteristic", 3);
> A := Matrix(2,symbol=a,shape=triangular[upper]):
> B := Matrix(2,symbol=b,shape=triangular[upper]):
> pA := A^3+r*A^2+s*A+<<t,0>|<0,t>>:
> L := convert(B-pA,list):
> v := [op(indets(A)),op(indets(B)),t,s,r]:
> S := AlgebraicThomasDecomposition(L,v):
> Sp := Project(S, 6):
> Spc := Comprehensive(Sp, 3, group=false):
> Sg0 := [ListTools[Categorize](
>              (a,b)->equalSystem(Project(a,3),Project(b,3)),
>              Spc)
>            ]:
> Sg := map(a->[Project(a[1],3),Complement(a,parameters=3)], Sg0):
> select(p->p[2]<>[], Sg);
```

$$[[[s = 0, r = 0], [[b_{1,1} + 2\,b_{2,2} = 0, b_{1,2} \neq 0, s = 0, r = 0]]]]$$

Similarly to characteristic 0, there are cases where the map is not surjective. However, in characteristic 3, the complement of the image consists of all non-diagonal matrices with identical Eigenvalues, while in characteristic 0, only matrices with a specific Eigenvalue were affected.

We analyze why that is the case. As we saw earlier, to ensure that the fiber is empty, the polynomial

```
> q := x^3+r*x^2+s*x+t-e;
```

$$q := rx^2 + x^3 + sx - e + t$$

must only have one solution for every Eigenvalue e. This is the case is and only if

```
> lcoeff(diff(q,x) mod 3,x) = 0;
```

$$2\,r = 0$$

and

```
> Prem(q,diff(q,x) mod 3,x) mod 3 = 0;
```

$$er^3 + 2\,r^3t + r^2s^2 + 2\,s^3 = 0$$

which is the case if and only if $r = s = 0$. This condition is independent of e. ◁

Chapter 6

Faithful Counting Polynomials

The definition of the counting polynomial in chapter 2 only applies to subsets of K^n where K is an infinite set. In chapter 3, we only consider counting polynomials of solution sets of polynomial systems over algebraically closed fields, which are again infinite. In this chapter, we introduce faithful counting polynomials in order to compute actual cardinalities of finite sets. If K is a field and $V \subseteq \overline{K}^n$ has the faithful counting polynomial $c(V)$, then for a finite field L with $K \subseteq L \subseteq \overline{K}$, the number of elements of $V \cap L^n$ is $c(V)_{u=|L|}$. Of course, such a faithful counting polynomial does not always exist.

We will introduce conditions that ensure the existence of a faithful counting polynomial and demonstrate how it can be computed in these cases.

6.1 Changing the Characteristic

In this section, we introduce a technique for computing a Thomas decomposition in characteristic 0 and interpreting it as a Thomas decomposition in positive characteristic. We observe that during the Decompose algorithm (3.47), we never use division. In particular, new polynomials are only produced by either taking coefficients of existing polynomials, or by taking a weighted sum $ap + bq$ of two existing polynomials p, q from the system, where the weights a, b are arbitrary polynomials from the base ring. Even the leading coefficients of the subresultants, where our definition includes a division, can be constructed as polynomials in the coefficients of the original polynomials. Taking the remainder modulo a natural number commutes with all these operations in the sense of the following remark.

Remark 6.1. Let A be a principal ideal domain with quotient field $Q := \mathrm{Quot}(A)$ and residue class fields $F_p := A/\langle p \rangle$ for any prime element $p \in A$. We have a ring monomorphism

$$\iota : A \to Q : a \mapsto \frac{a}{1}$$

and ring epimorphisms

$$\nu_p : A \to F_p : a \mapsto a + \langle p \rangle \ .$$

Since these are homomorphisms, it holds that $\nu_p(a \cdot b) = \nu_p(a) \cdot \nu_p(b)$ and $\nu_p(a+b) = \nu_p(a) + \nu_p(b)$ for all $a, b \in A$. Furthermore, if $da = n$ for $d, n \in A$, $a \in Q$ and $\nu_p(d) \neq 0$, then $a \mapsto \frac{\nu_p(n)}{\nu_p(d)}$ induces a ring epimorphism $\nu_p : A_{\langle p \rangle} \to F_p : \frac{a}{b} \mapsto \frac{\nu_p(a)}{\nu_p(b)}$ where $A_{\langle p \rangle} := (A \setminus \langle p \rangle)^{-1} A \subseteq Q$.

Now consider the basic operations of the Decompose algorithm. Let A, Q be as above and consider $R = Q[x_1, \ldots, x_n]$ and let $S = (S_T, S_Q)$ be a system over R as described in section 3.2.2. Assume further that all polynomials in S are elements of $A[x_1, \ldots, x_n]$. If $\nu_p(\mathrm{init}((S_T)_{x_i})) \neq 0$ for $i = 1, \ldots, n$, then for all $q \in A[x_1, \ldots, x_n]$

$$\nu_p(\mathsf{Reduce}(S, q)) = \mathsf{Reduce}(\nu_p(S), \nu_q) \ ,$$

where we consider $\nu_p(S)$ as a system over F_p.

If $q_1, q_2 \in A[x_1, \ldots, x_n]$ with $\mathrm{ld}(q_1) = \mathrm{ld}(q_2) = x_i$ and $\nu_p(\mathrm{init}(q_1)) \neq 0$, then

$$\nu_p(\mathrm{res}_j(q_1, q_2, x_i)) = \mathrm{res}_j(\nu_p(q_1), \nu_p(q_2), x_i)$$

for all $j \geq 0$ and similarly

$$\nu_p(\mathrm{RRes}_j(q_1, q_2, x_i)) = \mathrm{RRes}_j(\nu_p(q_1), \nu_p(q_2), x_i) \ . \qquad \triangleleft$$

There are two steps in Decompose that change when applying ν_p. The first one is testing whether an element $q \in A$ is zero. The second one relates to square-freeness.

Remark 6.2. Let $q \in A[x_1, \ldots, x_n]$ with $\mathrm{ld}(q) = x_i$, $\mathrm{mdeg}(q) =: d$ and $\mathrm{init}(q) =: c$. In the Decompose algorithm, we split the system $\{q_=\}$ into $S_1 := \{q_=, c_{\neq}\}$ and $S_2 := \{(q - cx_i^d)_=, c_=\}$. If $\mathrm{ld}(\nu_p(q)) \neq \mathrm{ld}(q)$ or $\mathrm{mdeg}(\nu_p(q)) \neq \mathrm{mdeg}(q)$, then $\nu_p(S_1)$ is inconsistent since $\nu_p(c)_{\neq} = 0_{\neq}$ is a contradiction.

If $\mathrm{ld}(c) > 1$, a similar split is applied to c. This recursion continues until $\mathrm{ld}(c) = 1$. Therefore, we can detect the situation where either the leader or main degree of any equation or inequation changes when ν_p is applied by only looking at the constants that we add to the system. $\triangleleft$

Our general strategy is to perform all computations in Q and ensure that the actual polynomials are in a polynomial ring over A. Whenever we add a non-zero constant a to a system, we record the primes p such that $\nu_p(a) = 0$.

Example 6.3. Let $A = \mathbb{Z}$, $Q = \mathbb{Q}$ and apply the Decompose algorithm to $S := \{((2y-1)x-1)_=\}$ with $y < x$. We first split the system into

$$(\{((2y-1)x-1)_=, (2y-1)_{\neq}\}, \{(-1)_=, (2y-1)_=\}) \ .$$

The second system contains $(-1)_=$ and is therefore inconsistent. Also note that $\nu_p(-1) \neq 0$ for all primes $p \in \mathbb{Z}$. The first system splits further into

$$(\{((2y-1)x-1)_=, (2y-1)_{\neq}, 2_{\neq}\}, \{((2y-1)x-1)_=, (-1)_{\neq}, 2_=\})$$

In both system, the constant 2 appears. It holds that $\nu_p(2) \neq 0$ for all primes $p \neq 2$ and $\nu_2(2) = 0$. We remember this and continue the computation. The second system is inconsistent and in the first system, the inequation $2_{\neq}$ is redundant. We conclude that $(\{((2y-1)x-1)_=, (2y-1)_{\neq}\})$ is a Thomas decomposition of S when we interpret S as a system over $\mathbb{Q}$ or over $\mathbb{F}_p$ with $p \neq 2$. In any of these cases, the counting polynomial is $(u-1)$.

Over $\mathbb{F}_2$, a Thomas decomposition of S is given by $(\{(x+1)_=\})$ and the counting polynomial is u. $\triangleleft$

In this example, we computed a Thomas decomposition for the given system in all characteristics by invoking the Decompose algorithm only twice.

There is a second problem which only occurs when there are $n \in \mathbb{N}$ and $p \in A$ such that $\nu_p(n) = 0$, i.e. if the characteristic of Q is zero and $\mathbb{Q} \subsetneq A$.

Remark 6.4. During the Decompose algorithm, when we compute the square-free part $\hat{q}$ of a polynomial q, then $\nu_p(\hat{q})$ is not necessarily the square-free part of $\nu_p(q)$ if $p \in \{2, \ldots, \mathrm{mdeg}(q)\}$. $\triangleleft$

We can apply the ideas from Remarks (6.1), (6.2) and (6.4) to the following cases:

1. $A = \mathbb{Z}, Q = \mathbb{Q}$
2. $A = K[y], Q = K(y)$ for any field K.

In the latter case, Remark (6.4) can be ignored. Our implementation in the AlgebraicThomas package only handles the former case and it is the only case that interests us in the next section. We demonstrate such a computation in Maple.

Example 6.5. We compute a THOMAS decomposition of $\{(x^3 + ax^2 + bx + c)_=\}$ over $\mathbb{Q}[a, b, c, x]$ and interpret the result over $\mathbb{F}_p[a, b, c, x]$ for different primes $p \in \mathbb{N}$.

```
> restart;
> with(AlgebraicThomas):
> L := [ x^3 + a*x^2 + b*x + c ];
```

$$L := [x^3 + x^2 a + xb + c]$$

```
> v := [x,c,b,a];
```

$$v := [x, c, b, a]$$

```
> AlgebraicThomasOptions("save zero sets", true);
> S := AlgebraicThomasDecomposition(L, v):
> countingPolynomial(S);
```

$$3\,u^3 - 2\,u^2$$

```
> map(
>    n->op(map(f->f[1],ifactors(n)[2])),
>    map(numer,AlgebraicThomasZeroSets())
> );
```

$$\{2, 3\}$$

We need to separately compute the decomposition and counting polynomial for characteristics 2 and 3.

```
> AlgebraicThomasOptions("characteristic", 2);
> S2 := AlgebraicThomasDecomposition(L,v):
> countingPolynomial(S2);
```

$$3\,u^3 - u^2 - u$$

```
> AlgebraicThomasOptions("characteristic", 3);
> S3 := AlgebraicThomasDecomposition(L,v):
> countingPolynomial(S3);
```

$$3\,u^3 - u^2 - u$$

The counting polynomials for characteristic 2 and 3 are the same, but we can see a difference in the counting trees.

```
> evalb(CountingTree(S2)=CountingTree(S3));
```

false

Both decompositions even contain systems that contain roots of variables. Therefore, they cannot be obtained by taking the remainder of a system over characteristic 0 modulo 2 or 3.

```
> S2[3];
```

$$[x + \sqrt{b} = 0, ba + c = 0, a^2 + b \neq 0]$$

```
> S3[5];
```

$$[x + \sqrt[3]{c} = 0, b = 0, a = 0]$$

For any characteristic other than 2 and 3, the result is the same as in characteristic 0.

```
> AlgebraicThomasOptions("characteristic", 5);
> S5 := AlgebraicThomasDecomposition(L,v):
> evalb(CountingTree(S)=CountingTree(S5));
```

true

We even get the same systems, up to multiplication with non-zero constants.

```
> nops(S),nops(S5);
```

4, 4

```
> printSystem(S[1]) mod 5;
```

$$[x^3 + x^2a + xb + c = 0, 4\,b^2a^2 + 4\,b^3 + 2\,c^2 + \left(4\,a^3 + 2\,ba\right)c \neq 0, 4\,a^2 + 3\,b \neq 0]$$

```
> S5[1];
```

$$[x^3 + x^2a + xb + c = 0, 2\,b^2a^2 + 2\,b^3 + c^2 + \left(2\,a^3 + ba\right)c \neq 0, 3\,a^2 + b \neq 0]$$

This result is not surprising. Since the degree of the original polynomial is 3, it is expected that we need to take special care of characteristics 2 and 3. As all coefficients are 1, one would expect that all characteristics larger than 3 do not need special treatment, although this is no guarantee. ◁

6.2 Faithful Counting Polynomials and Split Systems

If a set is finite, its counting polynomial¡¡¡¡¡ equals its cardinality. Now let L be an algebraically closed field and $V \in \mathcal{P}_L^n$ be an infinite set. For any finite subfield $K \subset L$, we want to determine the cardinality of the intersection $V \cap K^n$. Moreover, if $p = \mathrm{char}(L)$, we want to determine $V \cap \mathbb{F}_{p^d}^n$ for all $d > 0$.

Remark 6.6. Let K be a field of characteristic p and S be a polynomial system over $K[x_1, \ldots, x_n]$. Consider the system $S^{(d)} := S \cup \left\{ \left(x_i^{p^d} - x_i \right)_= \middle| i = 1, \ldots, n \right\}$. Then $c\left(S^{(d)}\right) = \left| \mathcal{L}(S) \cap \mathbb{F}_{p^d}^n \right| \in \mathbb{Z}_{\geq 0}$. ◁

This is apparent from the fact that the solution set of $x^{p^d} - x$ over $\overline{\mathbb{F}_p}$ is exactly $\mathbb{F}_{p^d}$. However, this method has two major drawbacks: Since the degree of $x^{p^d} - x$ is rather large, the computation becomes very expensive when d increases. Furthermore, this method only computes the number of solutions over a single field.

Definition 6.7. Let K be a field of characteristic p and $V \in \mathcal{P}_K^n$. A polynomial $f \in \mathbb{Z}[u]$ is called **p^d-faithful counting polynomial** of V if $f(|L|) = |V \cap L^n|$ for every finite field extension $L \supseteq \mathbb{F}_{p^d}$.

If S is a family of polynomial systems over $\mathbb{Z}[x_1, \ldots, x_n]$, then $f \in \mathbb{Z}[u]$ is called **faithful counting polynomial** of S if for any prime number $p \in \mathbb{N}$, f is a p-faithful counting polynomial of $\mathcal{L}(\nu_p(S))$, with ν_p as in Remark (6.1). ◁

We already saw an example of a faithful counting polynomial in Proposition (4.6). There, for an arbitrary field K and all $k, n \in \mathbb{N}$ with $k \leq n$, the set $\mathcal{M}_{k,n}$ of all $k \times n$ matrices of rank k was described using $\binom{n}{k}$ polynomial systems. We also computed the counting polynomial

$$c(\mathcal{M}_{k,n}) = \prod_{i=0}^{k-1} u^n - u^i \ .$$

Since for a finite field K, the number of such matrices is known to be

$$|\mathcal{M}_{k,n}| = \prod_{i=0}^{k-1} |K|^n - |K|^i \ ,$$

we can conclude that $c(\mathcal{M}_{k,n})$ is a faithful counting polynomial.

Clearly, a faithful counting polynomial does not always exist. For example, if we consider $\{(x^2 + 1)_=\}$ in characteristic 3, then $f = 2$ is 9-faithful, but not 3-faithful. There is one important case where the counting polynomial yields the faithful counting polynomial, which has been introduced [Ple09b, Sect. 3].

Definition 6.8. A simple system S over $K[x_1, \ldots, x_n]$ is called **split** if for every equation $p_= \in S$ or inequation $p_\neq \in S$, the polynomial p can be factorized into linear factors in $K[x_1, \ldots, x_n]$, i.e. $p = \prod_{i=1}^{\mathrm{mdeg}(p)} q_i$ where $\mathrm{ld}(q_i) = \mathrm{ld}(p)$ and $\mathrm{mdeg}(q_i) = 1$. ◁

Obviously, all linear systems in the sense of section 2.3 can be decomposed into split simple systems. Below we will consider examples of non-linear systems where all polynomials have main degree 1 and thus are linear with respect to each variable. These systems can often be decomposed into split simple systems. We continue by showing that decompositions into split simple systems yield faithful counting polynomials.

Proposition 6.9. *1. Let K be a finite field. If a set $V \in \mathcal{P}_K^n$ is the solution set of a disjoint family of split simple systems over $K[x_1, \ldots, x_n]$, then $c(V)$ is a $|K|$-faithful counting polynomial of V.*

2. Let S, T be a families of polynomial systems over $\mathbb{Z}[x_1, \ldots, x_n]$ such that T is a Thomas *decomposition of S into split simple systems over $\mathbb{Q}[x_1, \ldots, x_n]$. Assume further that for all prime numbers $p \in \mathbb{N}$, $\nu_p(T)$ is a* Thomas *decomposition of $\nu_p(S)$ into split simple systems over $\mathbb{F}_p[x_1, \ldots, x_n]$ and that $c(S) = c(\nu_p(S))$. Then $c(S)$ is a faithful counting polynomial of S.*

Proof. It suffices to show that the counting polynomial of a split simple systems s is faithful. Let $L \supseteq K$ be a finite field extension.

If s_{x_1} is empty, then $|\mathcal{L}(s_{\leq x_1}) \cap L| = |L| = c(s_{\leq x_1})(|L|)$. Otherwise, there is a polynomial $p \in K[x_1]$ with $s_{x_1} = p_=$ or $s_{x_1} = p_{\neq}$. This polynomial p is of the form $p = \prod_{j=1}^{d}(x_1 - a_j)$ with $a_j \in K$, $j = 1, \ldots, d$. Since the system is simple, the a_j are pairwise different and p has d distinct roots, which all lie in K since s is split.

Therefore, in case $s_{x_1} = p_=$,

$$|\mathcal{L}(s_{\leq x_1}) \cap L| = |\{a_1, \ldots, a_d\}| = d = c(s_{\leq x_1})(|L|) \ .$$

In case $s_{x_1} = p_{\neq}$,

$$|\mathcal{L}(s_{\leq x_1}) \cap L| = |L \setminus \{a_1, \ldots, a_d\}| = |L| - |\{a_1, \ldots, a_d\} \cap L| = |L| - d = c(s_{\leq x_1})(|L|) \ .$$

Let $1 \leq i \leq n$ and $\mathbf{a} \in \mathcal{L}(s_{<x_i}) \cap L^{i-1}$. Assume by induction that $|\mathcal{L}(s_{<x_i}) \cap L^{i-1}| = c(s_{<x_i})(|L|)$. With the same arguments we applied for s_{x_1}, we can conclude that $|\mathcal{L}(\phi_{<x_i,\mathbf{a}}(s_{\leq x_i})) \cap L| = c(\phi_{<x_i,\mathbf{a}}(s_{\leq x_i}))(|L|)$, implying

$$\begin{aligned} |\mathcal{L}(s_{\leq x_i}) \cap L^i| &= |\mathcal{L}(s_{<x_i}) \cap L^{i-1}| \cdot |\mathcal{L}(\phi_{<x_i,\mathbf{a}}(s_{\leq x_i})) \cap L| \\ &= c(s_{<x_i})(|L|) \cdot c(\phi_{<x_i,\mathbf{a}}(s_{\leq x_i}))(|L|) \\ &= c(s_{\leq x_i})(|L|) \end{aligned}$$

since s is simple. □

Using this proposition, we can now compute the size of the solution set for a number of systems. We start with the set of all 4×4 matrices of rank 4, 3, 2 and 1. This example allows us to demonstrate how to compute such examples with the AlgebraicThomas package.

Example 6.10.

```
> restart:
> with(AlgebraicThomas):
> with(LinearAlgebra):
> AlgebraicThomasOptions("warnings", false);
> AlgebraicThomasOptions("save zero sets", true);
> A := Matrix(4,symbol=a);
```

$$A := \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}$$

```
> v := [op(indets(A))];
```

$$v := [a_{1,1}, a_{1,2}, a_{1,3}, a_{1,4}, a_{2,1}, a_{2,2}, a_{2,3}, a_{2,4}, a_{3,1}, a_{3,2}, a_{3,3}, a_{3,4}, a_{4,1}, a_{4,2}, a_{4,3}, a_{4,4}]$$

First compute the system defined by giving the determinant as an inequation. We already know this result, but it is easily reproduced by the package.

```
> L4 := [Determinant(A)<>0]:
> S4 := AlgebraicThomasDecomposition(L4, v):
> countingPolynomial(S4);
```

$$u^{16} - u^{15} - u^{14} + 2\,u^{11} - u^8 - u^7 + u^6$$

```
> IsSplit(S4);
```

true

All systems are split. The next line tells us that the result is valid for all characteristics, implying that the counting polynomial is faithful.

```
> AlgebraicThomasZeroSets();
```

{ }

In order to characterize the matrices of rank 3, we need to compute the determinants of all 3×3 submatrices.

```
> threebythree := map(
>    s->op(map(
>       t->Determinant(SubMatrix(A,s,t)),
>       combinat[choose](4,3))),
>    combinat[choose](4,3)):
> L3 := ineqOr([Determinant(A)=0], threebythree):
> AlgebraicThomasZeroSetsReset();
> S3 := AlgebraicThomasDecompositionMany(L3, v):
> countingPolynomial(S3);
```

$$u^{15} + u^{14} - u^{12} - 3\,u^{11} - 2\,u^{10} + 2\,u^8 + 3\,u^7 + u^6 - u^4 - u^3$$

```
> IsSplit(S3);
```

true

```
> AlgebraicThomasZeroSets();
```

{0}

Due to an implementation detail, this set may sometimes contain 0, 1, -1 or fractions. We can ignore these safely. Therefore, as before, we have a faithful counting polynomial.

```
> twobytwo := map(
>    s->op(map(
>       t->Determinant(SubMatrix(A,s,t)),
>       combinat[choose](4,2))),
>    combinat[choose](4,2)):
> L2 := ineqOr(threebythree, twobytwo):
> AlgebraicThomasZeroSetsReset();
> S2 := AlgebraicThomasDecompositionMany(L2, v):
> countingPolynomial(S2);
```

$$u^{12} + u^{11} + 2\,u^{10} - u^8 - 3\,u^7 - 3\,u^6 - u^5 + 2\,u^3 + u^2 + u$$

```
> IsSplit(S2);
```

$$\mathit{true}$$

```
> AlgebraicThomasZeroSets();
```

$$\{0, 2\}$$

This result indicates that the counting polynomial for the 2×2 matrices may not be 2-faithful. We will compute the number of 1×1 matrices first and then reconsider this problem.

```
> onebyone := map(
>    s->op(map(
>       t->Determinant(SubMatrix(A,s,t)),
>       combinat[choose](4,1))),
>    combinat[choose](4,1)):
> AlgebraicThomasZeroSetsReset();
> S1 := AlgebraicThomasDecompositionMany(ineqOr(twobytwo, onebyone), v):
> countingPolynomial(S1);
```

$$u^7 + u^6 + u^5 + u^4 - u^3 - u^2 - u - 1$$

```
> IsSplit(S1);
```

$$\mathit{true}$$

```
> AlgebraicThomasZeroSets();
```

$$\{\quad\}$$

Again, we have a faithful counting polynomial. Adding up these counting polynomials and adding 1 for the zero matrix should yield the number of all 4×4 matrices.

```
> add(countingPolynomial(s), s=[S1,S2,S3,S4])+1;
```

$$u^{16}$$

Since only one result indicated a potential problem in characteristic 2, but the sum of the counting polynomials is correct, we can conclude that the counting polynomial in the 2×2 case was also 2-faithful. Therefore, we do not need to repeat the computation in characteristic 2. It is now easy to determine the number of 4×4 matrices of rank 1, 2, 3 or 4 over any finite field.

```
> subs(u=2, map(countingPolynomial, [S1,S2,S3,S4]));
```

$$[225, 7350, 37800, 20160]$$

```
> subs(u=25, map(countingPolynomial, [S1,S2,S3,S4]));
```

$$[6357796224, 62179393789094400, 968508529986816000000, 22314493656000000000000]$$

```
> subs(u=27, map(countingPolynomial, [S1,S2,S3,S4]));
```

$$[10862633600, 156065163140577600, 3063564512679712204800, 76702722499018794447360]$$

Since the number of all matrices is known, it would have been possible to omit one of the above computations, preferably the most expensive one, and subtract the other results from the number all matrices to determine the missing result.

The inclusion-exclusion principle gives a different method for computing these polynomials which is more efficient since it only uses equations. We now compute the number of matrices with rank smaller than a fixed number and use the results to construct the correct faithful counting polynomials.

```
> AlgebraicThomasZeroSetsReset();
> Ss4 := AlgebraicThomasDecomposition([Determinant(A)], v):
> Ss3 := AlgebraicThomasDecomposition(threebythree, v):
> Ss2 := AlgebraicThomasDecomposition(twobytwo, v):
> Ss1 := AlgebraicThomasDecomposition(onebyone, v):
```

```
> AlgebraicThomasZeroSets();
```

$$\{\quad\}$$

```
> c := map(countingPolynomial, [Ss1,Ss2,Ss3,Ss4]):
> u^(4^2) - c[4];
```

$$u^{16} - u^{15} - u^{14} + 2\,u^{11} - u^8 - u^7 + u^6$$

```
> c[4] - c[3];
```

$$u^{15} + u^{14} - u^{12} - 3\,u^{11} - 2\,u^{10} + 2\,u^8 + 3\,u^7 + u^6 - u^4 - u^3$$

```
> c[3] - c[2];
```

$$u^{12} + u^{11} + 2\,u^{10} - u^8 - 3\,u^7 - 3\,u^6 - u^5 + 2\,u^3 + u^2 + u$$

```
> c[2] - c[1];
```

$$u^7 + u^6 + u^5 + u^4 - u^3 - u^2 - u - 1$$

```
> c[1];
```

$$1$$

There are the same faithful counting polynomials as above. ◁

In [Ple82], Plesken produces polynomials that count the number of pairs of 3×3 matrices of specific rank such that the sum of these matrices is a fixed matrix. He also proves that such polynomials are independent of the characteristic. Therefore, if we can decompose a polynomial system describing this problem into split simple systems in characteristic 0, we get a faithful counting polynomial. We show results for the case of 4×4 matrices.

Example 6.11. Let $c_{i,j,k} : \mathbb{Z} \to \mathbb{Z}$ be a function such that for any finite field K, $c_{i,j,k}(|K|)$ is the number of pairs of matrices $A, B \in K^{4\times4}$ with $\mathrm{rk}(A) = i$ and $\mathrm{rk}(A) = j$ such that $A + B = C$ for a fixed matrix $C \in K^{4\times4}$ of rank k. Then, according to [Ple82], $c_{i,j,k}$ is a polynomial function.

Because of the symmetry, we assume $i \geq j$. If $i \neq j$, then $c_{i,j,0} = 0$ and if $i = j$, then $c_{i,j,0}$ is the number of matrices of rank i, which we computed already in Example (6.10). If $j = 0$, then $c_{k,0,k} = 1$ and $c_{i,0,k} = 0$ for $i \neq k$. It only remains to consider $i, j, k > 0$. If $k < |i - j|$ or $k > |i + j|$, then $c_{i,j,k} = 0$

For the remaining cases, we use the inclusion-exclusion principle as we did in Example (6.10) to compute the counting polynomials. The results are as follows:

$$
\begin{aligned}
&c_{1,1,1} = 2u^4 - u - 2,\\
&c_{2,1,1} = u^7 + u^6 + u^5 - u^4 - u^3 - u^2,\\
&c_{2,2,1} = 2u^{10} + 2u^9 + u^8 - 4u^7 - 5u^6 - 3u^5 + u^4 + 3u^3 + 2u^2 + u,\\
&c_{3,2,1} = u^{12} + u^{11} - 2u^9 - 2u^8 + u^6 + u^5,\\
&c_{3,3,1} = 2u^{14} + u^{13} - 2u^{12} - 5u^{11} - 3u^{10} + 3u^9 + 4u^8 + 3u^7 - u^5 - u^4 - u^3,\\
&c_{4,3,1} = u^{15} - u^{14} - u^{13} + u^{11} + u^{10} - u^9,\\
&c_{4,4,1} = u^{16} - 2u^{15} + u^{13} + u^{11} - u^{10} + u^9 - u^8 - u^7 + u^6,\\
&c_{1,1,2} = u^2 + u, c_{2,1,2} = 2u^5 + 2u^4 - u^3 - 2u^2 - 2u - 1,\\
&c_{2,2,2} = u^9 + 5u^8 + u^7 - 4u^6 - 7u^5 - 4u^4 + 3u^3 + 3u^2 + 3u,\\
&c_{3,1,2} = u^7 + u^6 - u^5 - u^4,\\
&c_{3,2,2} = 2u^{11} + 3u^{10} - 2u^9 - 6u^8 - 4u^7 + u^6 + 4u^5 + 2u^4,\\
&c_{3,3,2} = u^{14} + 3u^{13} - 8u^{11} - 7u^{10} + 3u^9 + 9u^8 + 6u^7 - u^6 - 3u^5 - 2u^4 - u^3,\\
&c_{4,2,2} = u^{12} - u^{11} - u^{10} + u^9,\\
&c_{4,3,2} = u^{15} - 3u^{13} - u^{12} + 3u^{11} + 2u^{10} - u^9 - u^8,\\
&c_{4,4,2} = u^{16} - 2u^{15} - u^{14} + 3u^{13} - u^{10} - u^7 + u^6,
\end{aligned}
$$

$$
\begin{aligned}
c_{2,1,3} &= u^4 + u^3 + u^2,\\
c_{2,2,3} &= 2u^8 + 3u^7 + 2u^6 - 2u^5 - 5u^4 - 4u^3 - 2u^2,\\
c_{3,1,3} &= 2u^6 + u^5 - 2u^3 - 2u^2 - u - 1,\\
c_{3,2,3} &= u^{11} + 3u^{10} + 2u^9 - 3u^8 - 7u^7 - 6u^6 + u^5 + 4u^4 + 5u^3 + 2u^2 + u,\\
c_{3,3,3} &= u^{14} + 2u^{13} + 2u^{12} - 5u^{11} - 10u^{10} - 4u^9 + 6u^8 + 13u^7 + 5u^6 - 2u^5 - 5u^4 - 4u^3,\\
c_{4,1,3} &= u^7 - u^6,\\
c_{4,2,3} &= u^{12} - u^{10} - 2u^9 + u^7 + u^6,\\
c_{4,3,3} &= u^{15} - 2u^{13} - 3u^{12} + u^{11} + 5u^{10} + 2u^9 - u^8 - 3u^7,\\
c_{4,4,3} &= u^{16} - 2u^{15} - u^{14} + 2u^{13} + 2u^{12} + u^{11} - 4u^{10} + u^6,\\
c_{2,2,4} &= u^8 + u^7 + 2u^6 + u^5 + u^4,\\
c_{3,1,4} &= u^6 + u^5 + u^4 + u^3,\\
c_{3,2,4} &= u^{11} + 2u^{10} + 2u^9 - 3u^7 - 5u^6 - 5u^5 - 3u^4 - u^3,\\
c_{3,3,4} &= u^{14} + 2u^{13} + u^{12} - 3u^{11} - 7u^{10} - 6u^9 - u^8 + 6u^7 + 9u^6 + 7u^5 + 3u^4,\\
c_{4,1,4} &= u^7 - 2u^3 - u^2 - u - 1,\\
c_{4,2,4} &= u^{12} - 2u^9 - 2u^8 - u^7 + 3u^5 + 2u^4 + 3u^3 + u^2 + u,\\
c_{4,3,4} &= u^{15} - 2u^{13} - 2u^{12} - u^{11} + 3u^{10} + 4u^9 + 3u^8 - 4u^6 - 3u^5 - 2u^4 - u^3,\\
c_{4,4,4} &= u^{16} - 2u^{15} - u^{14} + 2u^{13} + u^{12} + 3u^{11} - 3u^{10} - 2u^9 - 2u^8 - u^7 + 5u^6
\end{aligned}
$$

None of these polynomials has a positive integer root larger than 1, so these pairs of matrices exist for every finite field. ◁

Relying on a decomposition into split simple system is often insufficient to obtain a faithful counting polynomial. In [PB14], which was joint work with W. Plesken, we used the Thomas decomposition to count the number of matrices that represent a particular matroid over a specific field. However, not all systems occurring in these computations were split.

Definition 6.12 ([PB14, Def. 2.2])**.** Let K be a field and $V \in \mathcal{P}_K^n$.

1. V is called **uniformly f-enumerable** if there is a disjoint family S of split simple systems with $V = \mathcal{L}(S)$.
2. V is called **f-enumerable** if there is a disjoint family S of simple systems with $V = \mathcal{L}(S)$ and for every $i = 1, \ldots, |S|$, there is a split simple system T_i and a bijection $\mathcal{L}(S_i) \to \mathcal{L}(T_i)$ defined by a rational function over K.
3. V is called **polynomially countable** if $V = \bigcup_{i=1}^{k} V_i$ such that for each subset $J \subseteq \{1, \ldots, k\}$, either $\bigcap_{i\in J} V_i$ or its complement $\overline{K}^n \setminus \bigcap_{i\in J} V_i$ is enumerable. ◁

In either of these cases, we can obtain a faithful counting polynomial. In the last case, we can do so using the inclusion-exclusion principle.

In [PB14, Ex. 5.8], we listed the faithful counting polynomials for the number of matrix representations of simple matroids of rank 3 on 7 points. We will now demonstrate with two examples how these polynomials were computed.

Example 6.13.

```
> restart:
> with(LinearAlgebra):
> with(AlgebraicThomas):
> AlgebraicThomasOptions("save zero sets", true):
```

We count the number of matrices that represent the matroid on 7 points

```
> E := { $1..7 };
```

$$E := \{1, 2, 3, 4, 5, 6, 7\}$$

with only one non-trivial hyperplane, namely

```
> H := [ [1,2,4] ];
```

$$H := [[1, 2, 4]]$$

These matrices are characterized by determinants. In particular, we want to count set of matrices

```
> M := Matrix(3,7,symbol=x);
```

$$M := \begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} & x_{1,5} & x_{1,6} & x_{1,7} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} & x_{2,5} & x_{2,6} & x_{2,7} \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} & x_{3,5} & x_{3,6} & x_{3,7} \end{bmatrix}$$

such that the determinant of $M_{|\{1,2,3\}\times\{a,b,c\}}$ is zero for $(a, b, c) \in H$ and non-zero for $(a, b, c) \in \mathrm{Pot}_3(\underline{7}) \setminus H$.

```
> cH := select(l->not l in H, combinat[choose](7,3)):
```

As demonstrated in [PB14, Cor. 3.8], we can restrict ourselves to the number of matrices

```
> M2 := subs([
>            x[1,1]=1, x[2,1]=0, x[3,1]=0,
>            x[1,2]=0, x[2,2]=1, x[3,2]=0,
>            x[1,3]=0, x[2,3]=0, x[3,3]=1,
>            x[1,4]=1, x[2,4]=1, x[3,4]=0,
>            x[1,5]=1, x[3,5]=1,
>            x[1,6]=1,
>            x[1,7]=1
>          ], M);
```

$$M2 := \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & x_{2,5} & x_{2,6} & x_{2,7} \\ 0 & 0 & 1 & 0 & 1 & x_{3,6} & x_{3,7} \end{bmatrix}$$

with this property and multiply the result by

```
> factor((u^3-u^2)*(u^3-u)*(u^3-1)*(u-1)^6);
```

$$u^3 (u-1)^9 (u+1) \left(u^2+u+1\right)$$

Computing the counting polynomial directly is infeasible. However, we can use the inclusion-exclusion principle: We define $V_i := \mathcal{L}\left(\left\{\left(\prod_{\{a,b,c\}\in N_i} \det\left(M_{|\{1,2,3\}\times\{a,b,c\}}\right)\right)_{=}\right\}\right)$, $i = 1, \ldots, k$ for certain $N_i \subseteq \mathrm{Pot}_3(\underline{7}) \setminus H$ with $\biguplus_{i=1}^{k} N_i = \mathrm{Pot}_3(\underline{7}) \setminus H$. We then compute $\bigcap_{i\in J} V_i$ for every $J \subseteq \{1, \ldots, k\}$. From there, we can compute the counting polynomial.

```
> v := [x[2,7], x[3,7], x[2,6], x[3,6], x[2,5]];
```

$$v := [x_{2,7}, x_{3,7}, x_{2,6}, x_{3,6}, x_{2,5}]$$

```
> G := map[3](Determinant@SubMatrix, M2, 1..-1, [op(H)]);
```

$$G := [0]$$

We now define the V_i:

```
> U:=map[3](Determinant@SubMatrix, M2, 1..-1, [op(cH)]):
> nops(U);
```

$$34$$

```
> U := select(p->p=0 or degree(p)>0, U):
> nops(U);
```

$$25$$

```
> [[$1..4],[$5..8],[9,10],[$11..15],[$16..19],[$20..23],[24,25]]:
> V:=map(l->mul(U[i],i=l),%):
> AlgebraicThomasZeroSetsReset();
```

The following procedure automatically performs the computation we described above.

```
> S:=InclExclCount(G,V,v,quiet=true):
> S[3];
```

$$[]$$

The previous command lists all results from the computation that were not split. Since there are none, the set is polynomially countable with the following p -faithful counting polynomial for almost all prime numbers p.

```
> factor(S[1]);
```

$$(u-5)\,(u-3)\left(u^3-13\,u^2+54\,u-66\right)$$

```
> AlgebraicThomasZeroSets();
```

$$\left\{0,2,3,4,\frac{1}{2}\right\}$$

For characteristics 2 and 3, the result may be incorrect. In fact, the counting polynomial cannot be correct for $p=2$ since

```
> subs(u=2, S[1]);
```

$$-6$$

is a negative number. We repeat the computation for the two critical cases.

```
> AlgebraicThomasOptions("characteristic",2);
> S2:=InclExclCount(G,V,v,quiet=true):
> S2[3];
```

$$[]$$

```
> evalb(S[1]=S2[1]);
```

$$\mathit{false}$$

```
> factor(S2[1]);
> S2[1]-S[1];
```

$$(u-4)\,(u-2)\left(u^3-15\,u^2+75\,u-123\right)$$

$$6$$

As predicted, in characteristic 2, we get a different result. This result implies that the given matroid has no matrix representation over a field of 2 or 4 elements.

```
> AlgebraicThomasOptions("characteristic",3);
> S3:=InclExclCount(G,V,v,quiet=true):
> S3[3];
```

$$[]$$

```
> evalb(S3[1]=S[1]);
```

$$\mathit{true}$$

For characteristic 3, we get the same result as for characteristic 0. This result implies that the given matroid has no matrix representation over a field of 3 or 5 elements. The overall number of matrices representing the matroid is

```
> factor(S2[1]*(u^3-u^2)*(u^3-u^2)*(u^3-1)*(u-1)^6);
```

$$(u-4)\,(u-2)\left(u^3-15\,u^2+75\,u-123\right)u^4\,(u-1)^9\,\left(u^2+u+1\right)$$

over a field of characteristic 2 and

```
> factor(S[1]*(u^3-u^2)*(u^3-u^2)*(u^3-1)*(u-1)^6);
```

$$(u-5)\,(u-3)\left(u^3-13\,u^2+54\,u-66\right)u^4\,(u-1)^9\,\left(u^2+u+1\right)$$

otherwise.

The isomorphism type of this matroid is listed in [PB14, Tbl. 2] as $\emptyset_3$. ◁

This example demonstrated how we can compute a faithful counting polynomial of a set that is polynomially countable, but not necessarily f-enumerable in the sense of Definition (6.12). We will now present such a computation for a polynomially countable set where some of the $\bigcap_i V_i$ are not uniformly f-enumerable.

Example 6.14. Consider the uniform matroid of rank 3 on 7 points. We perform the same computation as in the previous example.

```
> restart:
> with(LinearAlgebra):
> with(AlgebraicThomas):
> AlgebraicThomasOptions("save zero sets", true):
> AlgebraicThomasOptions("warnings", false);
> E := { $1..7 };
```

$$E := \{1, 2, 3, 4, 5, 6, 7\}$$

```
> cH := combinat[choose](7,3):
```

As demonstrated in [PB14, Cor. 3.8], we consider matrices of the form

```
> M := subs([
>            x[1,1]=1, x[2,1]=0, x[3,1]=0,
>            x[1,2]=0, x[2,2]=1, x[3,2]=0,
>            x[1,3]=0, x[2,3]=0, x[3,3]=1,
>            x[1,4]=1, x[2,4]=1, x[3,4]=1,
>            x[1,5]=1, x[1,6]=1, x[1,7]=1
>          ], Matrix(3,7,symbol=x));
```

$$M := \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & x_{2,5} & x_{2,6} & x_{2,7} \\ 0 & 0 & 1 & 1 & x_{3,5} & x_{3,6} & x_{3,7} \end{bmatrix}$$

and multiply the resulting counting polynomial by

```
> factor((u^3-u^2)*(u^3-u)*(u^3-1)*(u-1)^6);
```

$$u^3 (u-1)^9 (u+1) \left(u^2+u+1\right)$$

```
> v := [x[2,7],x[3,7],x[2,6],x[3,6],x[2,5],x[3,5]];
```

$$v := [x_{2,7}, x_{3,7}, x_{2,6}, x_{3,6}, x_{2,5}, x_{3,5}]$$

As before, define the V_i:

```
> U:=map[3](Determinant@SubMatrix, M, 1..-1, [op(cH)]):
> nops(U);
```

35

```
> U := select(p->p=0 or degree(p)>0, U):
> nops(U);
```

28

```
> [[$1..5],[$6..9],[10,11],[$12..14],[$15..19],[$20..24],[25,26],[27,28]]:
> V:=map(l->mul(U[i],i=l),%):
> AlgebraicThomasZeroSetsReset();
```

Compute the counting polynomial using inclusion-exclusion.

```
> S:=InclExclCount([],V,v,quiet=true):
> nops(S[3]);
```

6

We now have 6 cases where not all systems are split and thus the systems are not necessarily uniformly enumerable.

```
> S[3][1][1];
```

$$\{2, 6, 7\}$$

For the first case, the systems belonged to the intersection $V_2 \cap V_6 \cap V_7$. In the inclusion-exclusion computation, this system's counting polynomial was thus added with a negative sign.

```
> X1 := remove(IsSplit, S[3][1][2]):
> nops(X1);
```

$$3$$

Only three of the systems were not split. We recompute them with a different ranking and hope to obtain a faithful counting polynomial this time. There is no guarantee that such a ranking exists.

```
> v1 := v[[1,2,3,4,6,5]];
```

$$v1 := [x_{2,7}, x_{3,7}, x_{2,6}, x_{3,6}, x_{3,5}, x_{2,5}]$$

```
> Y1 := AlgebraicThomasDecompositionMany(map(printSystem, X1),v1):
> IsSplit(Y1);
```

$$true$$

Since these systems are now split, we can correct the counting polynomial.

```
> C1 := +countingPolynomial(X1)-countingPolynomial(Y1);
```

$$C1 := 0$$

No correction was necessary in this case. We repeat the same steps for the other 5 cases.

```
> S[3][2][1];
```

$$\{2, 3, 5, 6\}$$

```
> X2 := remove(IsSplit, S[3][2][2]):
> nops(X2);
```

$$2$$

```
> Y2 := AlgebraicThomasDecompositionMany(map(printSystem, X2),v1):
> IsSplit(Y2);
```

$$true$$

```
> C2 := -countingPolynomial(X2)+countingPolynomial(Y2);
```

$$C2 := 2\,u - 2$$

```
> S[3][3][1];
```

$$\{2, 5, 6, 7\}$$

```
> X3 := remove(IsSplit, S[3][3][2]):
> nops(X3);
```

$$1$$

```
> Y3 := AlgebraicThomasDecompositionMany(map(printSystem, X3),v1):
> IsSplit(Y3);
```

$$true$$

```
> C3 := -countingPolynomial(X3)+countingPolynomial(Y3);
```

$$C3 := u - 1$$

```
> S[3][4][1];
```

$$\{1, 2, 5, 6, 7\}$$

```
> X4 := remove(IsSplit, S[3][4][2]):
> nops(X4);
```

$$1$$

```
> Y4 := AlgebraicThomasDecompositionMany(map(printSystem, X4),v1):
> IsSplit(Y4);
```

$$true$$

```
> C4 := +countingPolynomial(X4)-countingPolynomial(Y4);
```

$$C4 := u - 1$$

```
> S[3][5][1];
```

$$\{1, 3, 5, 6, 7\}$$

```
> X5 := remove(IsSplit, S[3][5][2]):
> nops(X5);
```

$$1$$

```
> Y5 := AlgebraicThomasDecompositionMany(map(printSystem, X5),v1):
> IsSplit(Y5);
```

$$true$$

```
> C5 := +countingPolynomial(X5)-countingPolynomial(Y5);
```

$$C5 := u - 1$$

```
> S[3][6][1];
```

$$\{2, 3, 5, 6, 7\}$$

```
> X6 := remove(IsSplit, S[3][6][2]):
> nops(X6);
```

$$1$$

```
> Y6 := AlgebraicThomasDecompositionMany(map(printSystem, X6),v1):
> IsSplit(Y6);
```

$$true$$

```
> C6 := +countingPolynomial(X6)-countingPolynomial(Y6);
```

$$C6 := u - 1$$

The overall correction is given by

```
> C1+C2+C3+C4+C5+C6;
```

$$-6 + 6\,u$$

and the faithful counting polynomial is

```
> F := factor(S[1]+C1+C2+C3+C4+C5+C6);
```

$$F := (u-5)\,(u-3)\left(u^4 - 20\,u^3 + 148\,u^2 - 468\,u + 498\right)$$

```
> AlgebraicThomasZeroSets();
```

$$\left\{0, 1, 2, 3, 4, 6, 8, 24, \frac{1}{2}, \frac{1}{3}\right\}$$

This entire computation must be repeated separately for characteristics 2 and 3. We will omit this here and simply state the result. For characteristic 2, the result is

```
> factor(F - 30);
```

$$(u-2)\,(u-4)\left(u^4 - 22\,u^3 + 183\,u^2 - 678\,u + 930\right)$$

and for characteristic 3, the result is the same as in characteristic 0. ◁

The previous examples show how all computations from [PB14] can be reproduced using the AlgebraicThomas package. They also show that even if a (p-)faithful counting polynomial exists, its computation is not always straightforward due to the complexity of the problem.

Bibliography

[ALMM99] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symbolic Comput.*, 28(1-2):105–124, 1999. Polynomial elimination—algorithms and applications. 40

[Bäc08] Thomas Bächler. Enumerating solutions of algebraic systems using thomas' decomposition algorithm. Diplomarbeit, Lehrstuhl B für Mathematik, RWTH Aachen University, December 2008. 6

[BGLHR12] T. Bächler, V. P. Gerdt, M. Lange-Hegermann, and D. Robertz. Algorithmic Thomas decomposition of algebraic and differential systems. *J. Symbolic Comput.*, 47(10):1233–1266, 2012. (`arXiv:1108.0817`). 6, 35

[BLH14] Thomas Bächler and Markus Lange-Hegermann. *AlgebraicThomas and DifferentialThomas: Thomas Decomposition for algebraic and differential systems*, 2008-2014. (`http://wwwb.math.rwth-aachen.de/thomasdecomposition/`). 6, 69

[CGL+07] C. Chen, O. Golubitsky, F. Lemaire, M. Moreno Maza, and W. Pan. Comprehensive triangular decomposition. In Victor G. Ganzha, Ernst W. Mayr, and Evgenii V. Vorozhtsov, editors, *CASC*, volume 4770 of *Lecture Notes in Computer Science*, pages 73–101. Springer, 2007. 65

[CLS11] David A. Cox, John B. Little, and Henry K. Schenck. *Toric varieties*, volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011. 93, 94, 95, 96, 99, 100

[Fra09] Matthias Franz. *Convex - a Maple package for convex geometry*, 1999–2009. (`http://www.math.uwo.ca/~mfranz/convex/`). 102

[Hub03a] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. I. Polynomial systems. In *Symbolic and numerical scientific computation (Hagenberg, 2001)*, volume 2630 of *Lecture Notes in Comput. Sci.*, pages 1–39. Springer, Berlin, 2003. 6, 85, 87

[Hub03b] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. II. Differential systems. In *Symbolic and numerical scientific computation (Hagenberg, 2001)*, volume 2630 of *Lecture Notes in Comput. Sci.*, pages 40–87. Springer, Berlin, 2003. 6

[Kal93] Michael Kalkbrener. A generalized euclidean algorithm for computing triangular representations of algebraic varieties. *Journal of Symbolic Computation*, 15(2):143 – 167, 1993. 5

[Laz91] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Applied Mathematics*, 33(1–3):147 – 160, 1991. 6

[LH14] M. Lange-Hegermann. *Counting Solutions of Differential Equations*. PhD thesis, RWTH Aachen, Germany, 2014. Available at `http://darwin.bth.rwth-aachen.de/opus3/frontdoor.php?source_opus=4993`. 5

[LMMX05] F. Lemaire, M. Moreno Maza, and Y. Xie. The RegularChains library in MAPLE. *SIGSAM Bull.*, 39(3):96–97, 2005. 6

[LMW10] X. Li, C. Mou, and D. Wang. Decomposing polynomial sets into simple sets over finite fields: the zero-dimensional case. *Comput. Math. Appl.*, 60(11):2983–2997, 2010. 55, 57, 59

[LW99] Z. Li and D. Wang. Coherent, regular and simple systems in zero decompositions of partial differential systems. *System Science and Mathematical Sciences*, 12:43–60, 1999. 6

[MB12] Miguel A. Marco-Buzunáriz. A polynomial generalization of the Euler characteristic for algebraic sets. *J. Singul.*, 4:114–130, 2012. With an appendix by J. V. Rennemo. 93

[Mis93] B. Mishra. *Algorithmic algebra*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993. 44, 45, 47, 49, 52

[MM99] M. Moreno Maza. On triangular decompositions of algebraic varieties. Technical report, presented at the MEGA-2000 Conference, 1999. 6, 37

[MWL13] C. Mou, D. Wang, and X. Li. Decomposing polynomial sets into simple sets over finite fields: The positive-dimensional case. *Theoret. Comput. Sci.*, 468:102–113, 2013. 55

[OT92] Peter Orlik and Hiroaki Terao. *Arrangements of hyperplanes*, volume 300 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1992. 17, 20

[PB14] W. Plesken and T. Bächler. Counting polynomials for linear codes, hyperplane arrangements, and matroids. *Documenta Math.*, 19(9):247–284, 2014. 125, 126, 127, 128, 130

[Ple82] Wilhelm Plesken. Counting with groups and rings. *J. Reine Angew. Math.*, 334:40–68, 1982. 124

[Ple09a] W. Plesken. Counting solutions of polynomial systems via iterated fibrations. *Arch. Math. (Basel)*, 92(1):44–56, 2009. 6, 11, 91, 92

[Ple09b] W. Plesken. Gauss-Bruhat decomposition as an example of Thomas decomposition. *Arch. Math. (Basel)*, 92(2):111–118, 2009. 6, 80, 81, 120

[Rit50] J. F. Ritt. *Differential Algebra*. American Mathematical Society Colloquium Publications, Vol. XXXIII. American Mathematical Society, New York, N. Y., 1950. 5

[Rob12] D. Robertz. Formal Algorithmic Elimination for PDEs. June 2012. Habilitationsschrift, accepted by the Faculty of Mathematics, Computer Science and Natural Sciences, RWTH Aachen University, 2012. 87

[Tho37] J. M. Thomas. *Differential Systems*. AMS Colloquium Publications vol XXI, 1937. 5, 35, 37, 43

[Tho62] J. M. Thomas. *Systems and Roots*. The William Byrd Press, INC, Richmond Virginia, 1962. 5

[tt] 4ti2 team. 4ti2—a software package for algebraic, geometric and combinatorial problems on linear spaces. Available at www.4ti2.de. 102

[Wan98] D. Wang. Decomposing polynomial systems into simple systems. *J. Symbolic Comput.*, 25(3):295–314, 1998. 6, 37, 39

[Wan01] Dongming Wang. *Elimination methods*. Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 2001. 6

[Wan03] D. Wang. *ϵpsilon: description, help pages and examples of use*, 2003. (`http://www-spiral.lip6.fr/~wang/epsilon/`). 6

[Wan04] D. Wang. *Elimination practice*. Imperial College Press, London, 2004. Software tools and applications, With 1 CD-ROM (UNIX/LINUX, Windows). 6

[Wu00] Wen-Tsun Wu. *Mathematics mechanization*, volume 489 of *Mathematics and its Applications*. Kluwer Academic Publishers Group, Dordrecht, 2000. Mechanical geometry theorem-proving, mechanical geometry problem-solving and polynomial equations-solving. 5

[Yap00] C. K. Yap. *Fundamental problems of algorithmic algebra*. Oxford University Press, New York, 2000. 45

Index