SYMMETRIC IDEALS AND NUMERICAL PRIMARY DECOMPOSITION

A Thesis
Presented to
The Academic Faculty

by

Robert C. Krone

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Mathematics

Georgia Institute of Technology
August 2015

SYMMETRIC IDEALS AND NUMERICAL PRIMARY DECOMPOSITION

Approved by:

Professor Anton Leykin, Advisor
School of Mathematics
Georgia Institute of Technology

Professor Stavros Garoufalidis
School of Mathematics
Georgia Institute of Technology

Professor Josephine Yu
School of Mathematics
Georgia Institute of Technology

Professor Santosh Vempala
College of Computing
Georgia Institute of Technology

Professor Greg Blekherman
School of Mathematics
Georgia Institute of Technology

Date Approved: 26 May 2015

ACKNOWLEDGEMENTS

There are many people who deserve recognition for their parts in my completion of the Ph.D. thesis. First I thank my advisor Anton Leykin for his guidance and support, for supplying interesting and fruitful research problems, for pushing me to go to conferences, give talks and meet potential collaborators, and for putting up with my procrastination and habitual tardiness.

I would also like to acknowledge the other research collaborators who contributed to the work that appears in this thesis. These are Jan Draisma, Rob Eggermont, Jon Hauenstein, Chris Hillar and Thomas Kahle. Thanks to Jan Draisma for giving the me the opportunity to work with him and his group at TU Eindhoven during the spring of 2013.

Thanks to my thesis committee members Greg Blekherman, Stavros Garoufalidis, Anton Leykin, Santosh Vempala and Josephine Yu, for taking the time to be a part of this process.

Gratitude goes to all of my friends at Georgia Tech who worked very hard to make my graduate school experience interesting, both mathematically and otherwise. This includes Albert Bush, Peter Whalen, Krista Whalen, Steven Ehrlich, Geehoon Hong and many others.

Finally, special thanks to my parents and brother for their unconditional love, support and encouragement. I also recognize here my parents' integral role in my being, without which this thesis would not be possible.

TABLE OF CONTENTS

LIST OF FIGURES

SUMMARY

The thesis explores two distinct strategies for algebraic computation with polynomial systems in high dimension. Chapters 1-4 address symmetric ideals, while the topic of Chapters 5-7 is numerical algebraic geometry.

The first topic is the use of symmetry to describe and compute with high dimensional or infinite dimensional polynomial ideals and varieties in many variables. Chapter 1 introduces the topic of $\mathfrak{S}_\infty$-invariant ideals: ideals which are closed under an action of the infinite symmetric group $\mathfrak{S}_\infty$. These objects can be used to study families of increasingly large ideals with $\mathfrak{S}_n$ symmetry, and often provide finite descriptions which allow for computations. This chapter also summarizes some of the previous work in the area, much of which has focused on $\mathfrak{S}_\infty$-invariant toric ideals. This interest has been driven by their applications to algebraic statistics, and this connection is explained. Chapter 2 presents a result which is joint work with Jan Draisma, Rob Eggermont and Anton Leykin, showing that a broad class of $\mathfrak{S}_\infty$-invariant toric ideals are generated by the $\mathfrak{S}_\infty$-orbits of only a finite number of binomials. This result generalizes several past finite generation results, and settles some open questions. Chapter 3 begins to tackle the problem of explicitly computing generating sets for the class of $\mathfrak{S}_\infty$-invariant toric ideals considered in the previous chapter. This chapter is joint with work Thomas Kahle and Anton Leykin, and we find success on some simple cases suggesting a way forward on the more general problem. Chapter 4 describes equivariant Gröbner bases and algorithms to compute them. We address some questions of when invariant ideals have finite equivariant Gröbner bases, and when these algorithms will terminate, in particular for the toric ideals of Chapter 3.

The second topic covers an assortment of problems in numerical algebraic geometry. Numerical algebraic geometry offers strategies to approximately solve polynomial systems efficiently that would be infeasible for symbolic algorithms. These algorithms can compute all roots of a zero dimensional system, or even categorize the irreducible components of a positive dimensional variety. However, a weakness of numerical algorithms has been dealing with singular solutions and describing multiplicity structure of an ideals components. We develop algorithmic solutions to some of these problems in the paradigm of numerical algebraic geometry. Chapter 5 introduces the topic Macaulay dual spaces and how it can be used as a tool for computing local multiplicity information about an ideal at an approximate zero. Chapter 6 describes the relationship between the dual space of an ideal at a point and the local Hilbert function there. This relationship is used to give an algorithm for computing the local Hilbert polynomial and regularity of an ideal from the dual space. This also leads to an algorithm to test if a given polynomial is in the ideal, even if the point of interest has been computed numerically. Finally Chapter 7 applies these tools to solve a critical problem in numerical primary decomposition: determining if a given point in the zero set (computed numerically) lies on an embedded prime of an ideal. This work in this chapter is joint work with Anton Leykin.

CHAPTER I

INVARIANT IDEALS

The focus of the first part of the thesis is on ideals with an action of the infinite symmetric group. Such objects have been rediscovered multiple times, arising in several different areas. Cohen first proved finite generation results for certain polynomial ideals with symmetry in 1967 in studying metabelain groups [10]. These ideas later resurfaced in the 2007 work of Aschenbrenner and Hillar [3] with a focus on algebraic computational for questions coming from chemistry and other applications. Invariant toric ideals meanwhile were implicitly being utilized as a tool in problems concerning integer lattices from both algebraic statistics [18] and optimization [13]. Simultaneously a more categorical approach to studying families of modules with symmetry has been developed recently to study problems of representation stability in algebraic topology [9], as well as other problems in representation theory, and the study of tensor rank [54][20]. Problems from other diverse areas readily admit descriptions in the language of invariant ideals, such as the Hadwiger-Nelson problem [25] from graph theory, and the cap-set problem [22] coming from additive combinatorics.

1.1 Invariant ideal preliminaries

Let R be a commutative K-algebra where K is a Noetherian ring (typically a field), and let Π be a monoid. Suppose that Π acts on R by K-algebra homomorphisms, $\Pi \to \mathrm{End}(R)$. In other words R is a Π-algebra: a functor from the category Π to the category of K-algebras.

Definition 1.1.1. A Π-invariant ideal $I \subseteq R$ is an ideal that is closed under the

action of Π.

$$\sigma I \subseteq I \text{ for all } \sigma \in \Pi.$$

Morphisms of Π-algebras are called Π-*equivariant* maps. A K-algebra homomorphism $\phi : R \to S$ is Π-equivariant if it commutes with the action of Π, $\sigma\phi(f) = \phi(\sigma f)$. Note that if ϕ is a Π-equivariant map then $\ker \phi$ is a Π-invariant ideal of R and $\operatorname{im} \phi$ a Π-subalgebra of S.

We focus on the case where $\Pi = \mathfrak{S}_\infty$ with $\mathfrak{S}_\infty$ defined here to be the group of all permutations of $\mathbb{N}$ that fix all but a finite number of elements, $\mathfrak{S}_\infty = \bigcup_n \mathfrak{S}_n$. We also will typically have R a polynomial algebra over K, or a sub- or quotient-algebra.

The framework of Π-invariant ideals was developed to study the limiting behavior of families of ideals with symmetry in increasingly many (but finite) variables [3][7].

Example 1.1.2. Let I_n be the ideal of equations on the entries of $n \times n$ matrices $A = (a_{ij})$ that vanish when $\operatorname{rank} A \leq 1$. Note that I_n is invariant under the $\mathfrak{S}_n$ action which simultaneously permutes rows and columns. This ideal is generated by the two-by-two minors,

$$a_{ij}a_{kl} - a_{il}a_{kj} \quad \text{for } i, j, k, l \in [n].$$

Although the number of minors grows in n they are all in the $\mathfrak{S}_n$-orbits of a fixed set of polynomials,

$$F = \{a_{12}a_{34} - a_{14}a_{32},\ a_{11}a_{23} - a_{13}a_{21},\ a_{11}a_{22} - a_{12}a_{21}\}.$$

where $\mathfrak{S}_n$ acts by simultaneously permuting rows and columns. There are natural containments $I_n \subseteq I_{n+1}$, so one can define the ideal $I = \bigcup_{n\in\mathbb{N}} I_n$, which is $\mathfrak{S}_\infty$-invariant and is generated by the $\mathfrak{S}_\infty$-orbits of F.

$$\begin{array}{ccccccc} \cdots & \hookrightarrow & \mathfrak{S}_n & \hookrightarrow & \mathfrak{S}_{n+1} & \hookrightarrow & \cdots \\ & & \circlearrowright & & \circlearrowright & & \\ \cdots & \hookrightarrow & I_n & \hookrightarrow & I_{n+1} & \hookrightarrow & \cdots \end{array} \qquad \begin{array}{c} \mathfrak{S}_\infty = \bigcup_n \mathfrak{S}_n \\ \circlearrowright \\ I = \bigcup_n I_n \end{array}$$

This description of I captures the structure of the entire family $\{I_n\}_{n\in\mathbb{N}}$ of truncations.

In general we will denote a Π-invariant ideal I that is generated by the Π-orbits of a set F as $\langle F\rangle_\Pi$. In the above example,

$$I = \langle a_{12}a_{34} - a_{14}a_{32},\ a_{11}a_{23} - a_{13}a_{21},\ a_{11}a_{22} - a_{12}a_{21}\rangle_{\mathfrak{S}_\infty}.$$

If X is a set of variables, then $[X]$ will denote the free commutative monoid generated by X, and $K[X]$ the polynomial ring with variables from X. Note that the monomials in $K[X]$ form a monoid under multiplication which is exactly $[X]$. More generally for an commutative monoid M, we can consider the monoid ring of M with coefficients in K, which will be denoted $K\,\mathrm{M}$ to maintain consistency with the previous notation. We will primarily consider the case the Π action on R is through a Π action on M by monoid endomorphisms.

Ring R has right action of both R and Π, which can together be considered as the action a single ring $R*\Pi$ referred to as the *twisted monoid ring* of Π with coefficients in R. The additive structure of $R*\Pi$ is that of the monoid ring, with elements of the form $\sum_{\sigma\in\Pi} r_\sigma\sigma$ with only a finite number of non-zero terms. Multiplication is defined term-wise by

$$(r\sigma)\cdot(s\tau) = r\sigma(s)\ \sigma\tau$$

where $\sigma(s)$ denotes the element of R obtained by applying σ to s. R is then a $R*\Pi$-module and a Π-invariant ideal I is exactly an ideal which is an $R*\Pi$-submodule of R.

In the case where $R = K\,\mathrm{M}$ and Π acts through an action on M, it is also useful to define the monoid $\mathrm{M}*\Pi$. This is a semi-direct product of M and Π, although we will represent pair (m,σ) as $m\sigma$. The monoid operation is defined by

$$(m\sigma)\cdot(n\tau) = m\sigma(n)\ \sigma\tau.$$

Then M is a $\mathrm{M}*\Pi$-module.

Definition 1.1.3. A Π-invariant ideal I is Π-*finitely generated* (or "finitely generated up to symmetry") if $I = \langle F \rangle_\Pi$ for a finite set F. Equivalently I is finitely generated as an $R * \Pi$-module.

This is the situation that we hope for, since it allows a finite description of the ideal, which can be used in computation.

1.2 Truncations and FI*-modules*

A $\mathfrak{S}_\infty$-invariant ideal I is often used to study the limiting behavior of a sequence of "truncated" ideals $I_0, I_1, I_2, \ldots$, each I_n being $\mathfrak{S}_n$-invariant (such as in Example 1.1.2). We can formalize this notion through the language of **FI**-modules introduced in [8]. Define **FI** as the category with objects the sets $[0], [1], [2], \ldots$ where $[n] := \{1, \ldots, n\}$ and morphisms being all injective maps. In [8] **FI** is defined to include all finite sets, but restricting to these representatives will be more convenient for us.

Definition 1.2.1. An **FI**-module (or **FI**-algebra) is a functor $\mathbf{R}$ from **FI** to the category of K-modules (resp. K-algebras).

Each K-module $\mathbf{R}([n])$ is a $\mathfrak{S}_n$-representation by applying $\mathbf{R}$ to the automorphisms of $[n]$. There are also maps from $\mathbf{R}([n])$ to $\mathbf{R}([m])$ for $n \leq m$ given by the injections $[n] \to [m]$, which respect these symmetric group actions. Given an **FI**-algebra $\mathbf{R}$, an **FI**-ideal is defined as an **FI**-module $\mathbf{I}$ with each $\mathbf{I}([n])$ an ideal of $\mathbf{R}([n])$.

Given an **FI**-algebra $\mathbf{R}$, applying $\mathbf{R}$ to the sequence of natural inclusions

$$[0] \hookrightarrow [1] \hookrightarrow [2] \hookrightarrow \cdots$$

and then taking the colimit produces a $\mathfrak{S}_\infty$-algebra R. This process defines a functor $\mathcal{F}$ from **FI**-modules (or algebras) to $\mathfrak{S}_\infty$-modules (resp. algebras). An **FI**-ideal $\mathbf{I}$ of $\mathbf{R}$ corresponds to a $\mathfrak{S}_\infty$-invariant ideal $\mathcal{F}\mathbf{I}$ of $R = \mathcal{F}\mathbf{R}$. We can similarly move in the

other direction, starting with a $\mathfrak{S}_\infty$-object, and producing its truncations, which will define an **FI**-object.

Definition 1.2.2. For $f \in R$, the *index support* of f is the minimal set $M \subseteq \mathbb{N}$ such that all permutations σ that fix M also fix f. The *width* of f, denoted $w(f)$ is the smallest integer n such that $M \subseteq [n]$. If no such integer exists, $w(f) = \infty$.

The multiplicative identity always has $w(1) = 0$ because $\mathfrak{S}_\infty$ acts trivially on it. The following example demonstrates a ring with elements that have infinite width.

Example 1.2.3. Let R be the polynomial ring with variables indexed by the elements of $\mathfrak{S}_\infty$, $K[y_\sigma \mid \sigma \in \mathfrak{S}_\infty]$, with $\mathfrak{S}_\infty$ acting on variables by $\tau y_\sigma = y_{\tau\sigma}$. Each variable y_σ (and each non-constant polynomial) has index support $\mathbb{N}$, and so infinite width.

Definition 1.2.4. For $M \subseteq \mathbb{N}$, the *truncation* of R corresponding to M is

$$R_M := \{f \in R \mid \text{index support of } f \subseteq M\}.$$

We will denote $R_{[n]}$ as R_n, the *nth truncation* of R, which consists of the elements with width bounded by n.

We will apply the term width to other objects besides algebra elements. The width of a $\mathfrak{S}_\infty$-algebra or module R is the smallest n such that $R = \mathfrak{S}_\infty R_n$. The width of a $\mathfrak{S}_\infty$-equivariant map is the width of its domain.

Proposition 1.2.5. *R_M is a subalgebra of R. Moreover R_M is closed under the action of $\mathfrak{S}_M$, the permutations of M considered as a subgroup of $\mathfrak{S}_\infty$.*

Proof. Any $\sigma \in \mathfrak{S}_\infty$ that fixes M also fixes any $f, g \in R_M$. Because σ acts on R by K-algebra homomorphism, it also fixes $f + g$, fg and sf for any $s \in S$, so R_M is a K-algebra.

For $\tau \in \mathfrak{S}_M$, τ fixes $\mathbb{N} \setminus M$, and so τ commutes with any σ that fixes M. For $f \in R_M$,

$$\sigma(\tau f) = \tau\sigma f = \tau f,$$

which implies $\tau f \in R_M$. $\square$

For I a $\mathfrak{S}_\infty$-invariant ideal, $I_M := I \cap R_M$ is a $\mathfrak{S}_M$-invariant ideal of R_M. We will primarily consider the sequence of truncations $I_1, I_2, \ldots$ since I_M is isomorphic to I_n for $n = |M|$.

Proposition 1.2.6. *The truncations of a $\mathfrak{S}_\infty$-invariant ideal I define an* **FI***-module F by $F([n]) = I_n$.*

Proof. Any injective map $\alpha : [n] \to [m]$ can be factored into $\alpha = \sigma \circ \iota$ where $\iota : [n] \hookrightarrow [m]$ is the natural inclusion, and σ is a permutation of $[m]$. Then $F(\alpha)$ is the composition of the inclusion $I_n \hookrightarrow I_m$ and the map on I_m induced by σ. It can be checked that $F(\beta\alpha) = F(\beta)F(\alpha)$. $\square$

This gives a functor $\mathcal{G}$ from $\mathfrak{S}_\infty$-modules (or algebras) to **FI**-modules (resp. algebras). This $\mathcal{G}$ is right adjoint to $\mathcal{F}$ defined earlier. Note that any element of R with infinite width will not appear in any of the truncations of R. As a result $\mathcal{F}\mathcal{G}R$ is the subalgebra of R consisting of only the finite width elements.

For the remainder of the work we will require R to have finite width, which implies that every $f \in R$ has finite width. In other words $R = \mathcal{F}\mathbf{R}$ for some **FI**-algebra $\mathbf{R}$, or equivalently $R = \mathcal{F}\mathcal{G}R$.

Remark 1.2.7. Let $\tilde{\mathfrak{S}}_\infty$ denote the group of *all* permutations of $\mathbb{N}$, which contains $\mathfrak{S}_\infty$ as a subgroup. Suppose that R is a $\tilde{\mathfrak{S}}_\infty$-algebra. For any polynomial $f \in R$ of finite width, the orbits of f under $\tilde{\mathfrak{S}}_\infty$ and $\mathfrak{S}_\infty$ are identical. Therefore in the case where all elements of R have finite width, $\tilde{\mathfrak{S}}_\infty$ and $\mathfrak{S}_\infty$ are interchangeable.

If I is finitely generated up to symmetry, then I has a generating set F in bounded degree, $F \subset R_n$. In this case the truncations of I stabilize in the sense that $I_m = \mathfrak{S}_m I_n$ for all $m \geq n$. If R has the property that each R_n is a Noetherian ring (which is the case in most examples we will consider), then the converse is also true: if the truncations of I stabilize in this sense, then I is finitely generation up to symmetry.

1.3 Π*-Noetherianity*

Definition 1.3.1. Π-algebra R is Π-*Noetherian* if every Π-invariant ideal is Π-finitely generated.

The property of Π-Noetherianity is closed under taking quotients, but not necessarily under taking subalgebras.

When computing with $\mathfrak{S}_\infty$-invariant ideals, it will be useful to introduce a related monoid $\mathrm{Inc}(\mathbb{N})$ which we will define as the set of all strictly increasing functions $\mathbb{N} \to \mathbb{N}$ with cofinite image. (Note that as in the case of $\mathfrak{S}_\infty$ versus $\tilde{\mathfrak{S}}_\infty$, the cofinite image condition will turn out not to matter for our purposes.)

Although the elements of $\mathrm{Inc}(\mathbb{N})$ are not permutations, a $\mathfrak{S}_\infty$-algebra R is also an $\mathrm{Inc}(\mathbb{N})$-algebra in a natural way. Given $f \in R$ with width k and $\rho \in \mathrm{Inc}(\mathbb{N})$, there exists $\sigma \in \mathfrak{S}_\infty$ such that ρ and σ agree on $[k]$. Define $\rho f := \sigma f$. It can be checked that this gives a well-defined action of $\mathrm{Inc}(\mathbb{N})$ on R.

It also follows that $\mathrm{Inc}(\mathbb{N})f \subseteq \mathfrak{S}_\infty f$, so any $\mathfrak{S}_\infty$-invariant ideal is also $\mathrm{Inc}(\mathbb{N})$-invariant. While the orbit $\mathfrak{S}_\infty f$ is generally larger than $\mathrm{Inc}(\mathbb{N})f$, $\mathfrak{S}_\infty f$ can be expressed as the union of a finite number of $\mathrm{Inc}(\mathbb{N})$ orbits, specifically

$$\mathfrak{S}_\infty f = \bigcup_{\sigma \in \mathfrak{S}_k} \mathrm{Inc}(\mathbb{N})(\sigma f).$$

Proposition 1.3.2. *A $\mathfrak{S}_\infty$-invariant ideal I is $\mathfrak{S}_\infty$-finitely generated if and only it is* $\mathrm{Inc}(\mathbb{N})$*-finitely generated. If $\mathfrak{S}_\infty$-algebra R is* $\mathrm{Inc}(\mathbb{N})$*-Noetherian, then it is $\mathfrak{S}_\infty$-Noetherian.*

Theorem 1.3.3 (Cohen [11]; Aschenbrenner-Hillar-Sullivant [4][35])**.** *Let $R = K[x_{i,j} | i \in [k], j \in \mathbb{N}]$ with* $\mathrm{Inc}(\mathbb{N})$ *action on the set of variables by acting on the second index, $\sigma x_{i,j} = x_{i,\sigma(j)}$. Then R is* $\mathrm{Inc}(\mathbb{N})$*-Noetherian.*

The proof of this theorem is recounted later in the section, as the ideas will be used later.

However for $R = K[x_{i,j}|i,j \in \mathbb{N}]$ with $\mathrm{Inc}(\mathbb{N})$ acting simultaneously on both indices $\sigma x_{i,j} = x_{\sigma(i),\sigma(j)}$, R is not $\mathfrak{S}_\infty$-Noetherian. This is demonstrated by the following example.

Example 1.3.4 (Aschenbrenner-Hillar [4])**.**

$$C = \langle y_{11},\ y_{12}y_{21},\ y_{12}y_{23}y_{31},\ y_{12}y_{23}y_{34}y_{41}, \ldots \rangle_{\mathfrak{S}_\infty}.$$

Note each monomials in this ring corresponds to a finite directed (multi-)graph on vertex set $\mathbb{N}$, by taking each variable $y_{i,j}$ to represent an edge (i,j). With that interpretation in mind, C is the ideal containing the monomials corresponding to graphs with a directed cycle. Because a cycle of length k does not have any shorter cycles as subgraphs, no finite set of the family of generators listed above suffices to generate C.

To prove Theorem 1.3.3, we first need some basic results from order theory.

Definition 1.3.5. A partial order $\preceq$ on a set P is a *well-partial-order* (or *wpo*) if for every infinite sequence $p_1, p_2, \ldots$ in P, there is some $i < j$ such that $p_i \preceq p_j$; see [42] for alternative characterisations.

For instance, the natural numbers with the usual total order $\leq$ is a well-partial-order. The product of a finite collection of partially ordered sets is also a well-partial-order. This yields Dickson's Lemma.

Lemma 1.3.6 (Dickson's Lemma)**.** $\mathbb{N}_0^k$ *with the entry-wise partial order given by*

$$(a_1, \ldots, a_k) \leq (b_1, \ldots, b_k) \quad \Leftrightarrow \quad a_i \leq b_i \text{ for all } i \in [k],$$

is a well-partial order.

Remark 1.3.7. Dickson's Lemma implies Hilbert's basis theorem: that $R = K[x_1, \ldots, x_k]$ is Noetherian. Note that the monoid of monomials in R ordered by divisibility is isomorphic to $(\mathbb{N}_0^k, \leq)$ as a partially ordered set. Dickson's Lemma implies then that

every monomial ideal of R is finitely generated. To extend this result to any ideal I, fix a monomial order on R. The initial ideal $\text{in}_{\geq} I$ is finitely generated by monomials $\{m_1, \ldots, m_s\}$. For each m_i, choose polynomial $g_i \in I$ with $\text{in}_{\geq} g_i = m_i$. The set $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of I so I is finitely generated.

It is this relationship between Noetherianity and well-partial orders that we will exploit. Let R be the monoid ring $K\,\mathrm{M}$ of commutative monoid M, and suppose Π acts on M by monoid endomorphisms. We will refer to the elements of M as the monomials of R.

Definition 1.3.8. A Π *respecting monomial order* $\leq$ on $R = K\,\mathrm{M}$ is a total well-order on M such that for any pair $a < b$,

$$\gamma a < \gamma b \quad \text{for all } \gamma \in \mathrm{M} * \Pi.$$

In general, Π respecting monomial orders on R are not guaranteed to exist.

Proposition 1.3.9. *If* Π *is a group and acts non-trivially on* M*, then* $R = K\,\mathrm{M}$ *has no* Π *respecting monomial orders.*

Proof. Assume the contrary and choose $m \in \mathrm{M}$ and $\alpha \in \Pi$ such that $\alpha m \neq m$. Either $\alpha m < m$ or $\alpha^{-1} m < m$, and assume the former without loss of generality. Then $m > \alpha m > \alpha^2 m > \cdots$ is an infinite descending chain, contradicting the fact that $\leq$ is a well-order. □

This immediately excludes the possibility of $\mathfrak{S}_\infty$ respecting orders (unless $\mathfrak{S}_\infty$ acts trivially). Another consequence of the proof is that if $\leq$ is a Π respecting order then $m \leq \alpha m$ for all $m \in \mathrm{M}$ and $\alpha \in \Pi$.

The divisibility relation $|$ defined by $a|b$ if there exists a $c \in \mathrm{M}$ with $ac = b$ is another partial order on M. Define a third order (which may only be a quasi order), the Π-*divisibility order*, $\preceq$ on M by $a \preceq b$ if there exists a $\gamma \in \mathrm{M} * \Pi$ such that $\gamma a = b$. In the case that R admits a Π respecting monomial order $\leq$ then $\preceq$ is, indeed, a

partial order because $\leq$ refines $\preceq$. To see that, if $a \preceq b$ then $b = c\sigma a$ for $c \in \mathrm{M}$ and $\sigma \in \Pi$, so then $a \leq \sigma a \leq c\sigma a$.

Proposition 1.3.10. *If $R = K\,\mathrm{M}$ admits a Π respecting monomial order, and the Π-divisibility order $\preceq$ is a well-partial-order, then R is Π-Noetherian.*

Proof. This statement was proved in [35] for the case where K is a field.

It is essentially the same as the argument for Hilbert's Basis Theorem from Dickson's Lemma. For any Π-invariant ideal I, the initial ideal $\mathrm{in}_{\geq} I$ is also Π-invariant. Because $\preceq$ is wpo, $\mathrm{in}_{\geq} I$ is Π-finitely generated. For each generator of $\mathrm{in}_{\geq} I$, choose an element of I with the same lead term. The resulting set is a finite Π-equivariant Gröbner basis of I and therefore generates I. (See Chapter 4 for definition and details on equivariant Gröbner bases.)

The more general case of K a Noetherian ring can be proved with the same argument by incorporating work done in [4]. □

To work with $\preceq$ we will need Higman's Lemma [32] which can be seen as a generalization of Dickson's Lemma. For a nice proof of Higman's Lemma we refer to the paper of Nash-Williams [50].

Lemma 1.3.11 (Higman's Lemma)**.** *Let $(P, \preceq)$ be a well-partial-order and let $P^* := \bigcup_{l=0}^{\infty} P^l$, the set of all finite sequences of elements of P. Define the partial order $\preceq'$ on P^* by $(a_1, \ldots, a_l) \preceq' (b_1, \ldots, b_m)$ if and only if there exists a strictly increasing function $\rho : [l] \to [m]$ such that $a_j \preceq b_{\rho(j)}$ for all $j \in [l]$. Then $\preceq'$ is a well-partial-order.*

Proof of Theorem 1.3.3. For $R = K[X]$ with $X = \{x_{i,j} \mid i \in [k], j \in \mathbb{N}\}$, the monoid of monomials is isomorphic to $\bigoplus_{i=1}^{\infty} \mathbb{N}_0^k$. For $a \in [X]$ let $\tilde{a}$ denote the element of $(\mathbb{N}_0^k)^{w(a)}$ obtained by cutting off the trailing zero vectors. By Dickson's Lemma $(\mathbb{N}_0^k, \leq)$ is a wpo, and by Higman's Lemma $((\mathbb{N}_0^k)^*, \leq')$ is then a wpo. Suppose that $\tilde{a} \leq' \tilde{b}$ and

strictly increasing function $\rho : [w(a)] \to [w(b)]$ witnesses this relationship. Extend ρ to a function $\sigma : \mathbb{N} \to \mathbb{N}$ in $\mathrm{Inc}(\mathbb{N})$. Then $\sigma a | b$ implying $a \preceq b$. Therefore the $\mathrm{Inc}(\mathbb{N})$-divisibility order $\preceq$ is also a wpo, and by Proposition 2.4, R is $\mathrm{Inc}(\mathbb{N})$-Noetherian. $\square$

1.4 Toric ideals in algebraic statistics

A major driver of the study of $\mathfrak{S}_\infty$-invariant toric ideals is applications to statistics. Toric ideals naturally arise in the study of log-linear statistical models. We briefly describe this connection below, and a more detailed account can be found in [21].

We can consider a discrete random variable P with k possible outcomes with probabilities $p_1, \ldots, p_k$ as a point in $\mathbb{R}^k$. A log-linear model M is the set of such random variables where the probabilities are parameterized by variables $\theta_1, \ldots, \theta_d$ according to fixed log-linear relations,

$$\log p_i = a_{i1} \log \theta_1 + \cdots + a_{id} \log \theta_d \quad \text{for } i = 1, \ldots, k.$$

When all coefficients a_{ij} are non-negative integers, this relationship describes a monomial map

$$\phi_A : \mathbb{C}[p_1, \ldots, p_k] \to \mathbb{C}[\theta_1, \ldots, \theta_d]$$

$$p^v \mapsto \theta^{Av}$$

where A is the $d \times k$ matrix (a_{ij}). Let $\Delta \subseteq \mathbb{R}^k$ denote the "probability simplex" defined by $p_i \geq 0$ for all i and $\sum_i p_i = 1$. Then $M = \mathbb{V}(\ker \phi_A) \cap \Delta$.

The defining ideal $\ker \phi_A$ is a toric ideal, generated by binomials in the following way

$$\ker \phi_A = \langle p^v - p^w \mid Av = Aw \rangle.$$

Example 1.4.1. Suppose $P = (X, Y)$ is a joint distribution of two random variables each of which has possible outcomes from the set $[n]$. Let $p_{ij} = \Pr(P = (i, j))$, $x_i = \Pr(X = i)$ and $y_i = \Pr(Y = i)$. The "independence model" is the set of such

random variables P where X and Y are independent, in which case $p_{ij} = x_i y_j$. This is a log-linear model with parameters $x_1, \ldots, x_n, y_1, \ldots, y_n$.

Let $\phi : R \to S$ be the map $p_{ij} \mapsto x_i y_j$ where $R = \mathbb{C}[p_{ij} \mid i, j \in [n]]$ and $S = \mathbb{C}[x_i, y_i \mid i \in [n]]$. There is an action of $\mathfrak{S}_n$ on R and S by permuting indices of the variables, and ϕ is $\mathfrak{S}_n$-equivariant. Therefore the toric ideal $I_n = \ker \phi$ is $\mathfrak{S}_n$-invariant. In fact, I_n is exactly the ideal defining rank 1 $n \times n$ matrices given in Example 1.1.2.

Suppose one wishes to test if a random variable P belongs to log-linear model M specified by a $d \times k$ matrix A with non-negative integer entries. One might perform a statistical trial taking N independent samples from P arriving at a data set $u = (u_1, \ldots, u_k)$ of the number of occurrences of each outcome. The vector $b = Au$ is called the "sufficient statistic" of u and determines the point in the model that was most likely to produce sample data u. The fiber of b, $\mathcal{F}(b) := A^{-1}(b) \cap \mathbb{N}_0^k$ is the set of all points with the same sufficient statistic. To test the likelihood of the model producing u a Monte Carlo Markov chain (MCMC) process called the Metropolis-Hastings algorithm is used to randomly sample points of $\mathcal{F}(b)$. To perform this algorithm we require a set of vectors in $\ker A$ that can be used to walk from point to point in the fiber. A set of vectors $B \subset \ker A$ that connects the fiber of *any* point $b \in \mathbb{N}_0^d$ is called a *Markov basis* of A.

The lattice $\mathbb{N}_0^k$ can be related to the monomials of $K[y_1, \ldots, y_k]$, and a binomial $y^v - y^w \in \ker \phi_A$ corresponds to a vector $v - w \in \ker A$.

Theorem 1.4.2 (Diaconis–Sturmfels [18])**.** *A set of binomials* $\{y^{v_1} - y^{w_1}, \ldots, y^{v_s} - y^{w_s}\}$ *with* $\gcd(v_i, w_i) = 1$ *generates* $\ker \phi_A$ *if and only if* $\{v_1 - w_1, \ldots, v_s - w_s\}$ *is a Markov basis for* A.

According to this theorem, if we can compute a generating set for the toric ideal of a log-linear model, we have a Markov basis with which to use the Metropolis-Hastings algorithm to perform statistical tests.

Example 1.4.3. Continuing from Example 1.4.1, two $n \times n$ matrices have the same sufficient statistic in the independence model if all corresponding row and column sums are equal. By Theorem 1.4.2, a Markov basis for the independence model for two random variables is the set of vectors of the form $e_{ij} + e_{kl} - e_{il} - e_{kj}$ with $i, j, k, l \in [n]$ where e_{ij} is the unit vector for the (i, j)th entry of an $n \times n$ matrix. (This is the vector corresponding to binomial $y_{ij}y_{kl} - y_{il}y_{kj}$.) These are matrices with four non-zero entries in the following pattern:

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

So for any two matrices with non-negative integer entries that have the same row and column sums b, there is a path from one to the other in $\mathcal{F}(b)$ by adding and subtracting vectors of the above form.

Many useful families of log-linear models have natural $\mathfrak{S}_n$-invariance. If we can compute a generating set up to symmetry for the corresponding $\mathfrak{S}_\infty$-invariant toric ideal, then we obtain a Markov basis for all of the truncations.

Definition 1.4.4. For matrix A that defines a $\mathfrak{S}_\infty$-equivariant toric map ϕ_A, a $\mathfrak{S}_\infty$-equivariant Markov basis of A is a set of vectors B such that the $\mathfrak{S}_\infty$-orbits of B form a Markov basis of A.

Even when n is so large that the full Markov basis becomes intractably large, we can still efficiently sample Markov moves from a $\mathfrak{S}_\infty$-equivariant Markov basis. For example this technique was used in [2], with the toric ideal family in Theorem 1.4.9, to analyze how chromosomes are arranged in the cell nucleus.

$\mathfrak{S}_\infty$-invariant toric ideals in $\mathfrak{S}_\infty$-Noetherian rings (such as in Theorem 1.3.3) necessarily have finite $\mathfrak{S}_\infty$-equivariant Markov bases. However many toric ideals in $\mathfrak{S}_\infty$-algebras that are not $\mathfrak{S}_\infty$-Noetherian still prove to have finite $\mathfrak{S}_\infty$-equivariant Markov

bases. In Example 1.1.2 it was shown that the toric ideal corresponding to the independence model of two random variables is finitely generated up to symmetry. This generalizes to any k random variables.

Theorem 1.4.5 (Independence model)**.**

$$\phi : K[y_{(\alpha_1,\ldots,\alpha_k)} \mid \alpha_1,\ldots,\alpha_k \in \mathbb{N}] \to K[z_{i,j} \mid i \in [k], j \in \mathbb{N}]$$

$$y_{(\alpha_1,\ldots,\alpha_k)} \mapsto z_{1,\alpha_1} \cdots z_{k,\alpha_k}.$$

$\ker \phi$ *is generated by binomials of degree 2 (corresponding to* 2×2 *minors of an order* k *tensor). A consequence is that* $\ker \phi$ *is finitely generated up to symmetry.*

The following fact is useful for understanding when $\mathfrak{S}_\infty$-invariant toric ideals are $\mathfrak{S}_\infty$-finitely generated.

Proposition 1.4.6. *Let* $R = K[Y]$ *with* $\mathfrak{S}_\infty$ *acting on* Y*, and* Y *having a finite number of* $\mathfrak{S}_\infty$ *orbits. For* $\mathfrak{S}_\infty$*-invariant binomial ideal* $I \subseteq R$*, the following statements are equivalent.*

1. *I is $\mathfrak{S}_\infty$-finitely generated.*
2. *I has a binomial generating set of bounded degree.*
3. *For some $d \geq 0$ every truncation I_n has a binomial generating set of degree $\leq d$.*

Proof. It is clear that (1) implies (2). Also (2) and (3) are equivalent since a union over $n \in \mathbb{N}$ of the generators of the truncations I_n forms a generating set of I. To show that (2) implies (1), let $k = \max_{y \in Y} |\text{index support of } y|$, which is finite since Y has a finite number of orbits. A degree d binomial f contains at most $2d$ distinct variables, so the index support of f has size at most $2kd$. Therefore $\sigma f \in I_{2kd}$ for some $\sigma \in \mathfrak{S}_\infty$. Note that R_{2kd} is a Noetherian ring, so I_{2kd} is finitely generated by binomials. The $\mathfrak{S}_\infty$ orbits of such a generating set of I_{2kd} generate I. □

A family of models generalizing independence models are *hierarchical models*. Let $V = (V_1, \ldots, V_m)$ be a finite collection of random variables with each V_i taking values from the set C_i and let $C = C_1 \times \cdots \times C_m$ be the set of outcomes of V. Let Γ be a collection of subsets of $[m]$ (i.e. a hypergraph on vertex set $[m]$) representing dependence relations among the variables. For $F \in \Gamma$ let C_F denote the set of outcomes of the variables in F and for $c \in C$ let $c|_F \in C_F$ be the vector of entries of c indexed by F. The hierarchical model of Γ is defined by the relation

$$p_c = \prod_{F \in \Gamma} q_{F, c|_F}$$

with parameters $q_{F,d}$ for each $F \in \Gamma$ and $d \in C_F$. This gives rise to monomial map

$$\phi_\Gamma : \mathbb{C}[y_c \mid c \in C] \to \mathbb{C}[z_{F,d} \mid F \in \Gamma, d \in C_F]$$

$$y_c \mapsto \prod_{F \in \Gamma} z_{F, c|_F}.$$

If Γ consists of only the singleton sets $\{1\}, \ldots, \{m\}$ then the hierarchical model is exactly the independence model of $V_1, \ldots, V_m$.

Theorem 1.4.7 (Independent Set Theorem; Hillar–Sullivant [35])**.** *Suppose $T \subseteq V$ is an independent set of hypergraph Γ (every edge of Γ contains at most one vertex in T). Suppose that for each $i \in T$, $C_i = \mathbb{N}$, while for $i \notin T$, C_i is a finite set. Let $\mathfrak{S}_\infty$ act on $\mathbb{C}[p_c \mid c \in C]$ by permuting each C_i for $i \in T$. Then $\ker \phi_\Gamma$ is finitely generated up to symmetry.*

Conversely, when the graph Γ has an edge containing more than one vertex with an infinite number of outcomes, the corresponding ideal is typically not $\mathfrak{S}_\infty$-finitely generated. This is illustrated in the following "no hope" theorem of de Loera and Onn, where the underlying graph Γ is the triangle $\{1,2\}, \{2,3\}, \{1,3\}$.

Theorem 1.4.8 (de Loera–Onn [14])**.** *Let ϕ be the following $\mathfrak{S}_\infty$-equivariant monomial map, with $\mathfrak{S}_\infty$ acting on indices i and j,*

$$\phi : K[y_{i,j,k} \mid i, j \in \mathbb{N}, k \in [3]] \to K[w_{i,j}, x_{j,k}, z_{i,k} \mid i, j \in \mathbb{N}, k \in [3]]$$

$$y_{i,j,k} \mapsto w_{i,j}, x_{j,k}, z_{i,k}.$$

The $\mathfrak{S}_\infty$-invariant toric ideal $\ker \phi$ *is not $\mathfrak{S}_\infty$-finitely generated.*

Some other examples of $\mathfrak{S}_\infty$-finite generation results are given below.

Theorem 1.4.9 (de Loera–Sturmfels–Thomas [15]). *Let ϕ be the following $\mathfrak{S}_\infty$-equivariant monomial map, with $\mathfrak{S}_\infty$ acting on indices i and j.*

$$\phi : K[y_{\{i,j\}} \mid i, j \in \mathbb{N} \text{ distinct}] \to K[z_i \mid i \in \mathbb{N}]$$

$$y_{\{i,j\}} \mapsto z_i z_j.$$

Then $\ker \phi = \langle y_{\{1,2\}} y_{\{3,4\}} - y_{\{1,4\}} y_{\{2,3\}} \rangle_{\mathfrak{S}_\infty}$.

Theorem 1.4.10 (Aoki–Takemura [1]). *Let ϕ be the following $\mathfrak{S}_\infty$-equivariant monomial map, with $\mathfrak{S}_\infty$ acting on indices i and j.*

$$\phi : K[y_{i,j} \mid i, j \in \mathbb{N} \text{ distinct}] \to K[z_i, w_i \mid i \in \mathbb{N}]$$

$$y_{(i,j)} \mapsto z_i w_j.$$

Then $\ker \phi = \langle y_{1,2} y_{2,3} y_{3,1} - y_{2,1} y_{3,2} y_{1,3},\ y_{1,2} y_{3,4} - y_{1,4} y_{3,2} \rangle_{\mathfrak{S}_\infty}$.

A proof of the above theorem is given after Corollary 2.3.3. The statement was recently generalized to allow the variables of the domain ring to have an arbitrary number of indices, stated below. These two theorems will be very useful to us later on, as many more general $\mathfrak{S}_\infty$-equivariant toric maps factor through maps of this form.

Theorem 1.4.11 (Ogawa–Takemura–Yamaguchi [59]). *Let ϕ be the following $\mathfrak{S}_\infty$-equivariant monomial map, with $\mathfrak{S}_\infty$ acting on indices $\alpha_1, \ldots, \alpha_k$ in the domain ring and on j in the codomain ring,*

$$\phi : K[y_{(\alpha_1,\ldots,\alpha_k)} \mid \alpha_1, \ldots, \alpha_k \in \mathbb{N} \text{ distinct}] \to K[z_{i,j} \mid i \in [k], j \in \mathbb{N}]$$

$$y_{(\alpha_1,\ldots,\alpha_k)} \mapsto z_{1\alpha_1} \cdots z_{k,\alpha_k}.$$

$\ker \phi$ *is generated by binomials of degree* ≤ 3.

They did not originally state their result in this language, instead proving the degree bound for the truncations of $\ker \phi$, but by Proposition 1.4.6 this is equivalent.

A trend in these results is that in each case the orbits of variables in the codomain ring each have at most one index that runs to infinity, similar to the rings considered in Theorem 1.3.3. Several other examples where this occurred were also conjectured to be finitely generated up to symmetry. In Chapter 2 it is proved that this trend holds in general.

CHAPTER II

NOETHERIANITY OF SYMMETRIC TORIC IDEALS

2.1 Statement of main theorem

Let $R = K[Y]$ where Y is a set of variables with an action of $\mathfrak{S}_\infty$. Assume that Y consists of a finite number of $\mathfrak{S}_\infty$-orbits, and that every variable has finite width. Let $K[Z]$ have variable set $Z = \{z_{i,j} \mid i \in [k], j \in \mathbb{N}\}$ with $\mathfrak{S}_\infty$ acting on the second index (the same form described in Theorem 1.3.3).

Theorem 2.1.1. *Let $\phi : K[Y] \to K[Z]$ be a $\mathfrak{S}_\infty$-equivariant homomorphism that maps each $y \in Y$ to a* monomial *in the z_{ij}. Then* $\ker \phi$ *is generated by finitely many* $\mathrm{Inc}(\mathbb{N})$*-orbits of binomials, and* $\operatorname{im} \phi \cong K[Y]/\ker \phi$ *is an* $\mathrm{Inc}(\mathbb{N})$*-Noetherian ring.*

The proof of Theorem 2.1.1 is joint work with Jan Draisma, Rob Eggermont and Anton Leykin, and occupies the remainder of the section. This work originally appeared in [19].

If an ideal is $\mathfrak{S}_\infty$-invariant, then it is $\mathrm{Inc}(\mathbb{N})$-invariant, so the last statement implies that $K[Y]/\ker \phi$ is $\mathfrak{S}_\infty$-Noetherian. The conditions in the theorem are sharp in the following senses.

1. The ring $K[Y]$ itself is typically *not* $\mathfrak{S}_\infty$-Noetherian, let alone $\mathrm{Inc}(\mathbb{N})$-Noetherian, as shown by Example 1.3.4.

2. The R-algebra $K[Z]$ is $\mathfrak{S}_\infty$-Noetherian, and even $\mathrm{Inc}(\mathbb{N})$-Noetherian [11, 35]—this is the special case of our theorem where $Y = Z$ and ϕ is the identity—but $\mathfrak{S}_\infty$-stable subalgebras of $K[Z]$ need not be, even when generated by finitely many $\mathfrak{S}_\infty$-orbits of polynomials. For instance, an (as yet) unpublished theorem

due to Krasilnikov says that in characteristic 2, the ring generated by all 2×2-minors of a $2 \times \mathbb{N}$-matrix of variables is not $\mathfrak{S}_\infty$-Noetherian. Put differently, we do not know if the finite generatedness of $\ker \phi$ in the Main Theorem continues to hold if ϕ is an arbitrary $\mathfrak{S}_\infty$-equivariant homomorphism, but certainly the quotient is not, in general, $\mathfrak{S}_\infty$-Noetherian.

3. Moreover, subalgebras of $K[Z]$ generated by finitely many $\mathrm{Inc}(\mathbb{N})$-orbits of *monomials* need not be $\mathrm{Inc}(\mathbb{N})$-Noetherian; see Krasilnikov's example in [35]. However, our Main Theorem implies that subalgebras of $K[Z]$ generated by finitely many $\mathfrak{S}_\infty$-orbits of monomials *are* $\mathrm{Inc}(\mathbb{N})$-Noetherian.

Our Main Theorem applies to many problems on Markov bases of families of point sets. In such applications, the following strengthening is sometimes useful.

Corollary 2.1.2. *Assume that $\mathfrak{S}_\infty$ has only finitely many orbits on Y, and let S be an K-algebra with trivial $\mathfrak{S}_\infty$-action. Let $\phi : K[Y] \to S[Z]$ be a $\mathfrak{S}_\infty$-equivariant K-algebra homomorphism that maps each $y \in Y$ to an element of S times a monomial in the z_{ij}. Then $\ker \phi$ is generated by finitely many $\mathrm{Inc}(\mathbb{N})$-orbits of binomials, and $\operatorname{im} \phi \cong K[Y]/\ker \phi$ is an $\mathrm{Inc}(\mathbb{N})$-Noetherian ring.*

Proof of the Corollary given Theorem 2.1.1. Let $y_p, p \in [N]$ be representatives of the $\mathfrak{S}_\infty$-orbits on Y. Then for all $p \in [N]$ and $\pi \in \mathfrak{S}_\infty$ we have $\phi(\pi y_p) = s_p \pi u_p$ for some monomial u_p in the z_{ij} and some s_p in S. Apply the Main Theorem to $Y' := Y \times \mathbb{N}$ and $Z \cup Z'$ with $Z' := \{z'_{p,j} \mid p \in [N], j \in \mathbb{N}\}$ and ϕ' the map that sends the variable $(\pi y_p, j)$ to $z'_{p,j} \pi u_p$. Consider the commutative diagram

$$\begin{array}{ccc} K[Y'] & \xrightarrow{\phi'} & K[Z \cup Z'] \\ \downarrow{\scriptstyle \rho:(y,j)\mapsto y} & & \downarrow{\scriptstyle \psi:z'_{pj}\mapsto s_p} \\ K[Y] & \xrightarrow{\phi} & S[Z] \end{array}$$

of $\mathfrak{S}_\infty$-equivariant R-algebra homomorphisms. By the Theorem 2.1.1, $\operatorname{im} \phi'$ is $\mathrm{Inc}(\mathbb{N})$-Noetherian, hence so is its image under ψ; and this image equals $\operatorname{im} \phi$ because ρ is

surjective. Similarly, $\ker(\psi \circ \phi')$ is generated by finitely many $\mathrm{Inc}(\mathbb{N})$-orbits (because this is the case for both $\ker \phi'$ and $\ker \psi|_{\mathrm{im}\,\phi'}$), hence so is its image under ρ; and this image is $\ker \phi$ because ρ is surjective. □

Here are some consequences of Theorem 2.1.1.

1. Theorem 2.1.1 implies [4, Conjecture 5.10] that chains of ideals arising as kernels of monomial maps of the form $y_{i_1,\ldots,i_k} \mapsto z_{i_1}^{a_1} \cdots z_{i_k}^{a_k}$, where the indices $i_1, \ldots, i_k$ are required to be distinct, stabilize. In [4] this is proved in the squarefree case, where the a_j are equal to 1. In the Laurent polynomial setting more is known [33].

2. A consequence of [16] is that for any $n \geq 4$ the vertex set $\{v_{ij} := e_i + e_j \mid i \neq j\} \subseteq \mathbb{R}^n$ of the $(n-1)$-dimensional second hypersimplex has a Markov basis corresponding to the relations $v_{ij} = v_{ji}$ and $v_{ij} + v_{kl} = v_{il} + v_{kj}$. Here is a qualitative generalisation of this fact. Let m and k be fixed natural numbers. For every $n \in \mathbb{N}$ consider a finite set $P_n \subseteq \mathbb{Z}^m \times \mathbb{Z}^{k \times n}$. Let $\mathfrak{S}_n$ act trivially on $\mathbb{Z}^m$ and by permuting columns on $\mathbb{Z}^{k \times n}$. Assume that there exists an n_0 such that $\mathfrak{S}_n P_{n_0} = P_n$ for $n \geq n_0$; here we think of $\mathbb{Z}^{k \times n_0}$ as the subset of $\mathbb{Z}^{k \times n}$ where the last $n - n_0$ columns are zero. Then Corollary 2.1.2 implies that there exists an n_1 such that for any Markov basis M_{n_1} for the relations among the points in P_{n_1}, $\mathfrak{S}_n M_{n_1}$ is a Markov basis for P_n for all $n \geq n_1$. For the second hypersimplex, n_0 equals 2 and n_1 equals 4.

3. A special case of the previous consequence is the Independent Set Theorem of [35]. We briefly illustrate how to derive it directly from Corollary 2.1.2. Let m be a natural number and let Γ be a family of subsets of a finite set $[m]$. Let T be a subset of $[m]$ and assume that each $F \in \Gamma$ contains at most one element of T. In other words, T is an independent set in the hypergraph determined by Γ. For $t \in [m] \setminus T$ let r_t be a natural number. Set $Y := \{y_\alpha \mid \alpha \in \mathbb{N}^T \times \prod_{t \in [m] \setminus T} [r_t]\}$

and $Z := \{z_{F,\alpha} \mid F \in \Gamma, \alpha \in \mathbb{N}^{F\cap T} \times \prod_{F\setminus T}[r_t]\}$, and let ϕ be the homomorphism $\mathbb{Z}[Y] \to \mathbb{Z}[Z]$ that maps y_α to $\prod_{F\in\Gamma} z_{F,\alpha|_F}$, where $\alpha|_F$ is the restriction of α from $[m]$ to F. Then ϕ is equivariant with respect to the action of $\mathfrak{S}_\infty$ on the variables induced by the diagonal action of $\mathfrak{S}_\infty$ on $\mathbb{N}^T$, and (a strong form of) the Independent Set Theorem boils down to the statement that $\ker\phi$ is generated by finitely many $\mathfrak{S}_\infty$-orbits of binomials. By the condition that T is an independent set, each z-variable has at most one index running through all of $\mathbb{N}$. Setting S to be $\mathbb{Z}[z_{F,\alpha} \mid F \cap T = \emptyset]$, we find that Y, S, the remaining $z_{F,\alpha}$-variables, with $|F\cap T| = 1$, and the map ϕ satisfy the conditions of the corollary. The conclusion of the corollary now implies the Independent Set Theorem.

The remainder of the proof is organized as follows: In Section 2.2 we reduce Theorem 2.1.1 to a particular class of maps ϕ related to *matching monoids* of complete bipartite graphs. For these maps, finite generation of the kernel follows from recent results on the Birkhoff model [59]; see Section 2.3, where we also describe the image of ϕ. In Section 2.4 we prove Noetherianity of $\operatorname{im}\phi$, still for our special ϕ. As in [11, 35], the strategy in Section 2.4 is to prove that a partial order on certain monoids is a well-partial-order. In our case, these are said matching monoids, and the proof that they are well-partially-ordered is quite subtle.

2.2 Reduction to matching monoids

In this section we reduce the Theorem 2.1.1 to a special case to be treated in the next two sections. To formulate this special case, let $N \in \mathbb{N}_0$ and for each $p \in [N]$ let $k_p \in \mathbb{N}_0$. First, introduce a set Y' of variables $y'_{p,J}$ where $p \in [N]$ and $J = (j_l)_{l\in[k_p]} \in \mathbb{N}^{[k_p]}$ is a k_p-tuple of *distinct* natural numbers. The group $\mathfrak{S}_\infty$ acts on Y' by $\pi y'_{p,J} = y'_{p,\pi(J)}$ where $\pi(J) = (\pi(j_l))_{l\in[k_p]}$. This action has finitely many orbits and every variable has finite width. Second, let X be a set of variables $x_{p,l,j}$ with $p \in [N], l \in [k_p], j \in \mathbb{N}$ and let $\mathfrak{S}_\infty$ act on X by its action on the last index.

Proposition 2.2.1. *Let $\phi' : K[Y'] \to K[X]$ be the R-algebra homomorphism sending $y'_{p,J}$ to $\prod_{l\in[k_p]} x_{p,l,j_l}$. Then Theorem 2.1.1 implies that $\ker\phi'$ is generated by finitely many $\mathrm{Inc}(\mathbb{N})$-orbits of binomials, and that $\operatorname{im}\phi'$ is an $\mathrm{Inc}(\mathbb{N})$-Noetherian ring. Conversely, if these two statements hold for all choices of $N, k_1, \ldots, k_N \in \mathbb{N}_0$, then Theorem 2.1.1 holds.*

Proof. The first statement is immediate—note that the pair (p, l) comprising the first two indices of the variables $x_{p,l,j}$ takes on finitely many, namely, $\sum_p k_p$ values.

For the second statement, consider a monomial map $\phi : K[Y] \to K[Z]$ with $Z = \{z_{i,j} \mid i \in [k], j \in \mathbb{N}\}$ as in the Main Theorem. Let N be the number of $\mathfrak{S}_\infty$-orbits on Y and let $y_p,\ p \in [N]$ be representatives of the orbits. Set $k_p := k_{y_p}$ for $p \in [N]$, so that πy_p depends only on the restriction of $\pi \in \mathfrak{S}_\infty$ to $[k_p]$. We have thus determined the values of N and the k_p, and we let Y', X be as above.

Let $\psi : K[Y'] \to K[Y]$ be the K-algebra homomorphism defined by sending $y'_{p,J}$ to πy_p for any $\pi \in \mathfrak{S}_\infty$ satisfying $\pi(l) = j_l,\ l \in [k_p]$. This homomorphism is $\mathfrak{S}_\infty$-equivariant. The composition $\phi'' := \phi \circ \psi : K[Y'] \to K[Z]$ satisfies the conditions of the Main Theorem. Since ψ is surjective, it maps any generating set for $\ker\phi''$ onto a generating set for $\ker\phi$; moreover, we have $\operatorname{im}\phi'' = \operatorname{im}\phi$. Hence the conclusions of the Main Theorem for ϕ'' imply those for ϕ.

Next write $\phi''(y_{p,J}) = \prod_{i\in[k],j\in\mathbb{N}} z_{i,j}^{d_{p,i,j}}$. Observe that $d_{p,i,j} = 0$ whenever $j \notin J$, using the fact that any permutation that fixes J also fixes $y_{p,J}$, and hence must also fix $\phi''(y_{p,J})$ by $\mathfrak{S}_\infty$-equivariance. Now let $\phi' : K[Y'] \to K[X]$ be as above and define $\rho : K[X] \to K[Z]$ by $\rho(x_{p,l,j}) = \prod_{i\in[k]} z_{i,j}^{d_{p,i,j}}$. By construction, we have $\rho \circ \phi' = \phi''$.

Now $\operatorname{im}\phi''$ is a quotient of $\operatorname{im}\phi'$ and $\ker\phi''$ is generated by $\ker\phi'$ together with pre-images of generators of $\ker(\rho|_{\operatorname{im}\phi'})$, hence the conclusions of the Main Theorem for ϕ' imply those for ϕ'', as desired. □

In what follows, we will drop the accents on the y-variables and write Y for the set of variables $y_{p,J}$, X for the set of variables $x_{p,l,j}$, and ϕ for the R-algebra

homomorphism

$$\phi : K[Y] \to K[X],\ y_{p,J} \mapsto \prod_{l \in [k_p]} x_{p,l,j_l}. \tag{2.2.1}$$

Monomials in the $x_{p,l,j}$ will be denoted x^A where $A \in \prod_{p\in[N]} \mathbb{N}_0^{[k_p]\times\mathbb{N}}$ is an $[N]$-tuple of finite-by-infinite matrices A_p. Note that $\phi(y_{p,J})$ equals x^A where only the p-th component A_p of A is non-zero and in fact has all row sums equal to 1, all column sums labelled by J equal to 1, and all other column sums equal to 0. Thus A_p can be thought of as the adjacency matrix of a matching of the maximal size k_p in the complete bipartite graph with bipartition $[k_p] \bigsqcup \mathbb{N}$. Thus the monomials in $\operatorname{im}\phi$ form the commutative monoid generated by such matchings (with p varying). We call a monoid like this a *matching monoid*. In the next section we characterize these monomials among all monomials in the $x_{p,l,j}$, and find a bound on the relations among the $\phi(y_{p,J})$.

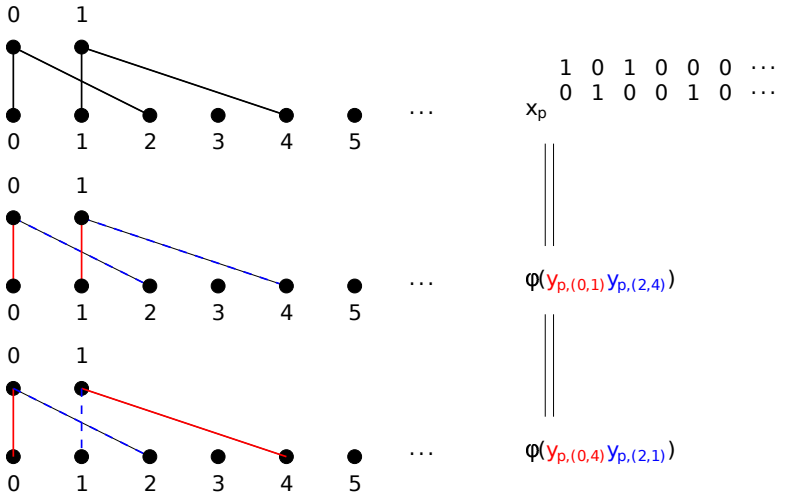

Figure 1: A bipartite graph on $[2] \bigsqcup \mathbb{N}$ and its corresponding monomial $x_p^{A_p}$ (top). Each decomposition of the graph into matchings represents a monomial in the preimage $\phi^{-1}(x_p^{A_p})$.

2.3 Relations among matchings

We retain the setting at the end of the previous section: Y is the set of variables $y_{p,J}$ with p running through $[N]$ and $J \in \mathbb{N}^{[k_p]}$ running through the $[k_p]$-tuples of *distinct* natural numbers; X is the set of variables $x_{p,l,j}$ with $p \in [N], l \in [k_p], j \in \mathbb{N}$, and ϕ is the map in (2.2.1). In this section we describe both the kernel and the image of ϕ. Note that if some k_p is zero, then the corresponding (single) variable $y_{p,()}$ is mapped by ϕ to 1. The image of ϕ does not change if we disregard those p, and the kernel changes only in that we forget about the generators $y_{p,()} - 1$. Hence we may and will assume that all k_p are strictly positive. The following lemma gives a complete characterization of the x^A in the image of ϕ.

Proposition 2.3.1. *For an $[N]$-tuple $A \in \prod_{p\in[N]} \mathbb{N}_0^{[k_p]\times\mathbb{N}}$ the monomial x^A lies in the image of ϕ if and only if for all $p \in [N]$ the matrix $A_p \in \mathbb{N}_0^{[k_p]\times\mathbb{N}}$ has all row sums equal to a number $d_p \in \mathbb{N}_0$ and all column sums less than or equal to d_p.*

We call the cone of such A satisfying these inequalities $\mathcal{M}$. Proposition 2.4.1 can then be restated as $\operatorname{im}\phi \cong K\mathcal{M}$, by considering $\mathcal{M}$ with addition as a monoid.

Note that d_p is unique since all k_p are strictly positive. We call the vector $(d_p)_p$ the *multi-degree* of A and of x^A.

Remark 2.3.2. By replacing $\mathbb{N}$ with $[n]$ for some natural number n greater than or equal to the maximum of the k_p, the proposition boils down to the statement that for each p the lattice polytope in $\mathbb{R}^{[k_p]\times[n]}$ with defining inequalities $\forall_{ij} a_{ij} \geq 0$, $\forall_i \sum_j a_{ij} = 1$, and $\forall_j \sum_i a_{ij} \leq 1$ is normal (in the case where $n = k_p$ this is the celebrated *Birkhoff polytope*). This is a not new result; in fact, this polytope satisfies a stronger property, namely, it is *compressed*. This follows, for instance, from [58, Theorem 2.4] or from the main theorem of [51]; see also [59, Section 4.2]. For completeness, we include a proof of the proposition using elementary properties of matchings in bipartite graphs.

Proof. Let x_p denote the vector of variables $x_{p,l,j}$ for $l \in [k_p]$ and $j \in \mathbb{N}$. By definition of ϕ, the monomial x^A lies in $\operatorname{im}\phi$ if and only if the monomial $x_p^{A_p}$ lies in $\operatorname{im}\phi$ for all $p \in [N]$. Thus it suffices to prove that $x_p^{A_p}$ lies in $\operatorname{im}\phi$ if and only if all row sums of A_p are equal, say to $d \in \mathbb{N}_0$, and all column sums of A_p are at most d. The "only if" part is clear, since every variable $y_{p,J}$ is mapped to a monomial x_p^B where $B \in \mathbb{N}_0^{[k_p]\times\mathbb{N}}$ has all row sums 1 and all column sums at most 1. For the "if" part we proceed by induction on d: assume that the statement holds for $d-1$, and consider a matrix A_p with row sums d and column sums $\leq d$, where d is at least 1. Clearly, the "if" part is true in the case $d = 0$.

Think of A_p as the adjacency matrix of a bipartite graph Γ (with multiple edges) with bipartition $[k_p] \bigsqcup \mathbb{N}$ (see Figure 1). With this viewpoint in mind, we will invoke some standard results from combinatorics, and refer to [53, Chapter 16]. The first observation is that Γ contains a matching that covers all vertices in $[k_p]$. Indeed, otherwise, by Hall's marriage theorem, after permuting rows and columns, A_p has the block structure

$$A_p = \begin{bmatrix} A_{11} & 0 \\ A_{12} & A_{22} \end{bmatrix}$$

with $A_{11} \in \mathbb{N}_0^{[l]\times[l-1]}$ for some $l, 1 \leq l \leq k_p$. But then the entries of A_{11} added row-wise add up to ld, and added column-wise add up to at most $(l-1)d$, a contradiction. Hence Γ contains a matching that covers all of $[k_p]$. Next, let $S \subseteq \mathbb{N}$ be the set of column indices where A_p has column sum equal to the upper bound d. We claim that Γ contains a matching that covers all of S. Indeed, otherwise, again by Hall's theorem, after permuting rows and columns A_p has the structure

$$A_p = \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix}$$

with $A_{11} \in \mathbb{N}_0^{[l-1]\times[l]}$ for some $l, 1 \leq l \leq |S|$; here the first l columns correspond to a subset of the original S. Now the entries of A_{11} added columnwise yield ld, while the

entries of A_{11} added rowwise yield at most $(l-1)d$, a contradiction.

Finally, we invoke a standard result in matching theory (see [53, Theorem 16.8]), namely that since Γ contains a matching that covers all of $[k_p]$ and a matching that covers all of S, it also contains a matching that covers both. Let B be the adjacency matrix of this matching, so that B has all row sums 1 and all column sums ≤ 1, with equality at least in the columns labelled by S. Then $A'_p := A_p - B$ satisfies the induction hypothesis for $d-1$, so $x_p^{A'_p} \in \operatorname{im}\phi$. Also, $x_p^B = \phi(y_{p,J})$, where $j_a \in \mathbb{N}$ is the neighbour of $a \in [k_p]$ in the matching given by B. Hence, $x_p^{A_p} = x_p^{A'_p} x_p^B \in \operatorname{im}\phi$ as claimed. □

This concludes the description of the image of ϕ.

Next we show that the kernel of ϕ is finitely generated. Variables from Y in separate orbits are mapped by ϕ to monomials of separate sets of variables in X, so there are no relations in $\ker\phi$ between variables from different orbits. Therefore we can compute generating sets in each orbit separately and then take the union. Fixing p and letting $k = k_p$, the restriction of ϕ to the pth orbit of variables is a map of the form

$$\phi^{(k)} : K[y_{(i_1,\ldots,i_k)} \mid i_1,\ldots,i_k \in \mathbb{N} \text{ distinct}] \to K[x_{i,j} \mid i \in [k], j \in \mathbb{N}]$$

$$y_{(i_1,\ldots,i_k)} \mapsto \prod_{j=1}^{k} x_{j,i_j}.$$

Note that this map $\phi^{(k)}$ is exactly the one treated in Theorem 1.4.11 [59], which states that $\ker\phi^{(k)}$ is generated by binomials of degree at most 3. A consequence is that the kernel is finitely generated up to symmetry.

Taking the union over all p of sets of generators for each individual p yields a set of generators for the kernel of ϕ. Bounding the degree of the generators is sufficient to show that there are finitely many up to $\mathfrak{S}_\infty$ action. Each variable $y_{p,J}$ has index support of size k_p, so a degree d binomial in the pth orbit has index support of size $\leq 2dk_p$. The binomial has a $\mathfrak{S}_\infty$ orbit representative in width $\leq 2dk_p$ and there are

only a finite number of binomials in bounded width of bounded degree.

Corollary 2.3.3. *The kernel of ϕ from* (2.2.1) *is generated by finitely many* $\mathrm{Inc}(\mathbb{N})$*-orbits of binomials.*

In the cases of $k = 2$ a generating set up to symmetry of $\ker \phi^{(2)}$ is given in Theorem 1.4.10, which consists of the 3-cycle cubic $y_{1,2}y_{2,3}y_{3,1} - y_{2,1}y_{3,2}y_{1,3}$ and the basic quadric $y_{1,2}y_{3,4} - y_{1,4}y_{3,2}$ generate $\ker \phi^{(2)}$ up to symmetry.

We give a short proof here due to Jan Draisma and Jan-Willem Knopper, for the sake of completeness.

Proof of Proposition 1.4.10. Representing a variable $y_{i,j}$ as a directed edge $i \to j$, monomials in $K[y_{i,j}]$ correspond to finite loop-free directed multigraphs on $\mathbb{N}$. For each such graph G, let y^G denote corresponding monomial. A binomial $y^G - y^H \in \ker(\phi)$ corresponds to a pair of graphs with the same in-degree and out-degree on each vertex. The proof is by induction on the degree d of the binomial. If G and H share an edge, we can divide by that edge and are done by induction. If they don't share an edge, then it suffices to find an applicable 3-cycle cubic or basic quadric to either G or H and obtain a new graph G' or H' which shares an edge with H or G, respectively.

Without loss of generality, let $(1, 2) \in G$ be an edge. Then H has an edge out from 1, which we can assume is $(1, 3)$, and an edge $(i, 2)$ with $i \neq 1$. If $i \neq 3$, apply the basic quadric to the edges $(1, 3)$ and $(i, 2)$ to get a graph H' with edges $(1, 2)$ and $(i, 3)$. Now G and H' share the edge $(1, 2)$. If $i = 3$, then G has edges $(3, j)$ and $(k, 3)$ with $j \neq 2$ and $k \neq 1$. If $j \neq 1$ then apply the basic quadric to $(3, j)$ and $(1, 2)$ to get G' with $(3, 2)$ and $(1, j)$, sharing $(3, 2)$ with H. Similarly, if $k \neq 2$, apply the basic quadric to $(k, 3)$ and $(1, 2)$. Finally, if $j = 1$ and $k = 2$, then G has a 3-cycle $(1, 2)$, $(2, 3)$, $(3, 1)$. Applying the 3-cycle cubic to reverse the direction produces G' with $(2, 1)$, $(3, 2)$, $(1, 3)$ which has edges in common with H. □

2.4 Noetherianity of matching monoid rings

By Corollary 2.3.3 and Proposition 2.2.1, Main Theorem follows from the following proposition.

Proposition 2.4.1. *The ring* $S = K[x^A \mid A \in \mathcal{M}] \cong K\mathcal{M}$ *is* $\mathrm{Inc}(\mathbb{N})$*-Noetherian, where* $\mathcal{M} \subseteq \prod_{p\in[N]} \mathbb{N}_0^{[k_p]\times\mathbb{N}}$ *is the cone defined in Proposition .*

The actions of $\mathfrak{S}_\infty$ and $\mathrm{Inc}(\mathbb{N})$ on $\mathcal{M}$ must be such that $\pi x^A = x^{\pi A}$ so they act by permuting or shifting columns. The $\pi(j)$-th column of the matrix $(\pi A)_p$ equals the j-th column of A_p. Let $d_A = (d_{A,p})_p \in \mathbb{N}_0^{[N]}$ denote the multi-degree of A; recall that this means that all row sums of A_p are equal to $d_{A,p}$. To prove Noetherianity we will prove that the $\mathrm{Inc}(\mathbb{N})$-divisibility partial order $\preceq$ on $\mathcal{M}$ is a well-partial-order.

Note that $K\mathcal{M}$ can be given a monomial order which respects the $\mathrm{Inc}(\mathbb{N})$-action. For example, take the lexicographic order, where the variables $x_{p,i,j}$ are ordered by their indices: $x_{p,i,j} < x_{p',i',j'}$ if and only if $p < p'$; or $p = p'$ and $j < j'$; or $p = p'$, $j = j'$, and $i < i'$. Therefore if we can show $\preceq$ is a wpo then Proposition holds.

Note that $A \preceq B$ if and only if there is $\pi \in \mathrm{Inc}(\mathbb{N})$ such that $B - \pi A \in \mathcal{M}$. Note that $A \preceq B$ not only implies there is some $\pi \in \mathrm{Inc}(\mathbb{N})$ such that all $A_{p,i,j} \leq B_{p,i,\pi(j)}$, but additionally that all (N-tuples of) column sums of $B - \pi A$ are at most $d_B - d_A \in \mathbb{N}_0^{[N]}$. This prevents us from applying Higman's Lemma directly to $(\mathcal{M}, \preceq)$. To encode this condition on column sums, for any $A \in \mathcal{M}$, let $\tilde{A} \in \prod_{p\in[N]} \mathbb{N}_0^{[k_p+1]\times\mathbb{N}}$ be the N-tuple of matrices such that for all $p \in [N]$, the first k_p rows of $\tilde{A}_p$ are equal to A_p, and the last row of $\tilde{A}_p$ is such that all column sums equal $d_{A,p}$:

$$\tilde{A}_{p,i,j} = \begin{cases} A_{p,i,j} & \text{for } \ i < k_p, \text{ and} \\ d_{A,p} - \sum_{l=0}^{k_p-1} A_{p,l,j} & \text{for } \ i = k_p. \end{cases}$$

We let $\tilde{\mathcal{M}}$ be the set of N-tuples of matrices of the form $\tilde{A}$ with $A \in \mathcal{M}$. It is precisely the set of N-tuples of matrices of the form $\tilde{A} \in \prod_{p\in[N]} \mathbb{N}_0^{[k_p+1]\times\mathbb{N}}$ with the property that there exists a $d_A \in \mathbb{N}_0^{[N]}$ such that for each $p \in [N]$ the first k_p row sums of A_p

are equal to $d_{A,p}$ and all column sums of A_p are equal to $d_{A,p}$. Since $A \in \mathcal{M}$ has only finitely many N-tuples of non-zero columns, $\tilde{A}$ will have all but finitely many N-tuples of columns equal to $((0,\dots,0,d_{A,p})^T)_{p\in[N]}$. Such N-tuples of columns will be called *trivial* (of degree d_A). The N-tuple of jth columns of $\tilde{A}$ will be denoted $\tilde{A}_{\cdot\cdot j}$. We define the action of $\mathrm{Inc}(\mathbb{N})$ on $\tilde{\mathcal{M}}$ as $\pi(\tilde{A}) = \widetilde{\pi(A)}$. Note that for any $j \notin \mathrm{im}(\pi)$, the column $(\pi\tilde{A})_{\cdot\cdot j}$ is trivial of degree d_A, rather than uniformly zero.

Proposition 2.4.2. *For $A, B \in \mathcal{M}$, $A \preceq B$ if and only if there is $\pi \in \mathrm{Inc}(\mathbb{N})$ such that $\pi\tilde{A} \leq \tilde{B}$ entry-wise.*

Proof. The condition that $(\pi\tilde{A})_{p,i,j} \leq \tilde{B}_{p,i,j}$ for all $p \in [N]$, all $i < k_p$, and all $j \in \mathbb{N}$ is equivalent to the condition that $B - \pi A$ is non-negative. Using the fact that

$$\tilde{B}_{p,k_p,j} - (\pi\tilde{A})_{p,k_p,j} = (d_{B,p} - d_{A,p}) - \sum_{i=0}^{k_p-1} (B_p - \pi A_p)_{i,j},$$

the condition that $\tilde{B}_{p,k_p,j} - (\pi\tilde{A})_{p,k_p,j} \geq 0$ for all $p \in [N]$ and all $j \in \mathbb{N}$ is equivalent to the condition that every N-tuple of column sums of $B - \pi A$ is less than or equal to $d_B - d_A$. Therefore $\pi\tilde{A} \leq \tilde{B}$ if and only if $B - \pi A \in \mathcal{M}$. □

Example 2.4.3. Let A and B be the following matrices in $\mathbb{N}_0^{[2]\times\mathbb{N}}$, which are in $\mathcal{M}$:

$$A = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 1 & 1 & 0 & \cdots \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 2 & 1 & 1 & 0 & \cdots \end{bmatrix}.$$

Note that $\pi A \leq B$ when π is the identity, however $A \not\preceq B$. Consider

$$\tilde{A} = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 1 & 1 & 0 & \cdots \\ 0 & 2 & 2 & 2 & 3 & \cdots \end{bmatrix}, \quad \tilde{B} = \begin{bmatrix} 3 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 2 & 1 & 1 & 0 & \cdots \\ 1 & 1 & 3 & 3 & 4 & \cdots \end{bmatrix},$$

and note that there is no $\pi \in \mathrm{Inc}(\mathbb{N})$ such that $\pi\tilde{A} \leq \tilde{B}$.

We will work with finite truncations of N-tuples of matrices in $\tilde{\mathcal{M}}$. Let H be the set of N-tuples of matrices $A \in \bigcup_{\ell=0}^{\infty} \prod_{p\in[N]} \mathbb{N}_0^{[k_p+1]\times[\ell]}$ such that there exists $d_A \in \mathbb{N}_0^{[N]}$

such that for all p, all column sums of A_p are equal to $d_{A,p}$ and the first k_p row sums are *at most* $d_{A,p}$; we call d_A the *multi-degree* of A. Note that the condition on row sums is relaxed, which will allow us to freely remove columns from matrices while still remaining in the set H. For $A \in \mathrm{H}$ the number of columns of A is called the *length* of A and denoted ℓ_A. We give H the partial order $\preceq$ defined as follows. For $A, B \in \mathrm{H}$, $A \preceq B$ if and only if there is a strictly increasing map $\rho : [\ell_A] \to [\ell_B]$ such that $\rho A \leq B$. Just as in $\tilde{\mathcal{M}}$, here ρA is defined by $(\rho A)_{\cdot\cdot j} = A_{\cdot\cdot \rho^{-1}(j)}$ for $j \in \mathrm{im}(\rho)$, and $(\rho A)_{\cdot\cdot j}$ trivial (of degree d_A) for $j \in [\ell_B] \setminus \mathrm{im}(\rho)$. For an N-tuple of matrices A and a set $J \subset \mathbb{N}$, let $A_{\cdot\cdot J}$ denote the N-tuple of matrices obtained from A by taking only the columns $A_{\cdot\cdot j}$ with $j \in J$.

Some care must be taken in the definition of H since we allow matrices with no columns. In all other cases, the degree of $A \in \mathrm{H}$ is uniquely determined by its entries. However for the length 0 case the degree is arbitrary, so we will consider H as having a distinct length 0 element Z^d with degree d for each $d \in \mathbb{N}_0^{[N]}$, and we define $Z^d \preceq A$ if and only if $d \leq d_A$. Additionally, define $A_{\cdot\cdot\emptyset} = Z^{d_A}$.

Definition 2.4.4. For $A \in \mathrm{H}$, the N-tuple of jth columns of A is *bad* if for some $p \in [N]$, we have $A_{p,k_p,j} < d_{A,p}/2$. If $A_{p,k_p,j} < d_{A,p}/2$, we will call j a *bad index* of A (with respect to p). Let H_t denote the set of N-tuples of matrices in H with exactly t bad indices.

We will use induction on t to show that $(\mathrm{H}_t, \preceq)$ is well-partially ordered for all $t \in \mathbb{N}_0$. This will in turn be used to prove that $(\mathrm{H}, \preceq)$ and then $(\tilde{\mathcal{M}}, \preceq)$ are well-partially ordered. First we prove the base case:

Proposition 2.4.5. $(\mathrm{H}_0, \preceq)$ *is well-partially ordered.*

Proof. Let $A^{(1)}, A^{(2)}, \ldots$ be any infinite sequence in H_0. We will show that there are $r < s$ such that $A^{(r)} \preceq A^{(s)}$.

Fix $p \in [N]$. There are now two possibilities: either the degrees of the elements of the sequence $A_p^{(1)}, A_p^{(2)}, \ldots$ are bounded by some $d_p \in \mathbb{N}_0$, or they are not. In the former case, it follows that the number of non-trivial columns in any $A_p^{(r)}$ is bounded by $d_p k_p$. Then there is a subsequence $B_p^{(1)}, B_p^{(2)}, \ldots$ of $A_p^{(1)}, A_p^{(2)}, \ldots$ such that every element has the same degree and same number of non-trivial columns. In the latter case, $A_p^{(1)}, A_p^{(2)}, \ldots$ has a subsequence with strictly increasing degree and moreover a subsequence $B_p^{(1)}, B_p^{(2)}, \ldots$ with the property that $d_{B^{(s+1)},p} \geq 2d_{B^{(s)},p}$ for all $s \in \mathbb{N}$.

In either case, without loss of generality, we replace $A^{(1)}, A^{(2)}, \ldots$ by $B^{(1)}, B^{(2)}, \ldots$. We repeat this procedure for all $p \in [N]$, and we find that $A^{(1)}, A^{(2)}, \ldots$ contains a subsequence $B^{(1)}, B^{(2)}, \ldots$ such that for all $p \in [N]$, one of the following two statements holds.

1 Both $d_{B^{(t)},p}$ and the number of non-trivial columns in B_p are constant.

2 We have $d_{B^{(t+1)},p} \geq 2d_{B^{(t)},p}$ for all t.

It now suffices to show that there are $r < s$ such that $B^{(r)} \preceq B^{(s)}$ for all $r < s$. Define the partial order $\sqsubseteq$ on H_0 by $A \sqsubseteq B$ if and only if there exists strictly increasing $\rho : [\ell_A] \to [\ell_B]$ such that $A_{\cdot,j} \leq B_{\cdot,\rho(j)}$ for all $j \in [\ell_A]$. By Higman's Lemma (Lemma 1.3.11), $\sqsubseteq$ is a wpo. This means that there exist $r < s$ such that $B^{(r)} \sqsubseteq B^{(s)}$. Fix such a pair $r < s$. We will show that $B^{(r)} \preceq B^{(s)}$.

Let $\rho : [\ell_{B^{(r)}}] \to [\ell_{B^{(s)}}]$ be a strictly increasing map that witnesses $B^{(r)} \sqsubseteq B^{(s)}$. We claim that it also witnesses $B^{(r)} \preceq B^{(s)}$. For this, we have to show that $\rho B^{(r)} \leq B^{(s)}$. By the properties of $\sqsubseteq$, we already have $(\rho B^{(r)})_{\cdot,\rho(j)} \leq B^{(s)}_{\cdot,\rho(j)}$, which is to say that it suffices to show that for all $j \notin \mathrm{im}(\rho)$, we have $d_{B^{(r)}} \leq (B^{(s)}_{p,k_p,j})_{p \in [N]}$.

Let $p \in [N]$. Suppose we are in the case that both $d_{B^{(t)},p}$ and the number of non-trivial columns in B_p are constant. Since ρ must map non-trivial columns of $B_p^{(r)}$ to non-trivial columns of $B_p^{(s)}$, we conclude that if $j \notin \mathrm{im}(\rho)$, then the j-th column of

$B_p^{(s)}$ is trivial, and hence $(B_{p,k_p,j}^{(s)}) = d_{B^{(s)},p}$. But the latter equals $d_{B^{(r)},p}$, so certainly $d_{B^{(r)},p} \leq (B_{p,k_p,j}^{(s)})$.

Alternatively, suppose we have $d_{B^{(t+1)},p} \geq 2d_{B^{(t)},p}$ for all t. Since $B_p^{(s)}$ has no bad columns, we have

$$B_{p,k_p,j}^{(s)} \geq \frac{1}{2} d_{B^{(s)},p} \geq d_{B^{(r)},p}.$$

This is exactly what we wanted to show.

So in both cases, we find that $d_{B^{(r)},p} \leq B_{p,k_p,j}^{(s)}$ for all $j \notin \mathrm{im}(\rho)$. This is true for all p, so we have $d_{B^{(r)}} \leq (B_{p,k_p,j}^{(s)})_{p\in[N]}$. We conclude that $B^{(r)} \preceq B^{(s)}$, as we wanted to show. □

Proposition 2.4.6. $(\mathrm{H}_t, \preceq)$ *is well-partially ordered for all* $t \in \mathbb{N}_0$.

Proof. The base case, $t = 0$, is given by Proposition 2.4.5. For $t > 0$, assume by induction that $(\mathrm{H}_{t-1}, \preceq)$ is well-partially ordered. For any $A \in \mathrm{H}_t$, let j_A be the largest bad index of A. Then A can be decomposed into three parts: the N-tuple of matrices of all N-tuples of columns before j_A, $A_{\cdot\cdot j_A}$ itself, and the N-tuple of matrices of all N-tuples of columns after j_A. This decomposition is represented by the map

$$\delta : \mathrm{H}_t \to \mathrm{H}_{t-1} \times \prod_{p\in[N]} \mathbb{N}_0^{[k_p+1]} \times \mathrm{H}_0$$
$$A \mapsto (A_{\cdot\cdot\{0,\ldots,j_A-1\}}, A_{\cdot\cdot j_A}, A_{\cdot\cdot\{j_A+1,\ldots,\ell_A-1\}}).$$

Let the partial order $\sqsubseteq$ on $\mathrm{H}_{t-1} \times \prod_{p\in[N]} \mathbb{N}_0^{[k_p+1]} \times \mathrm{H}_0$ be the product order of the wpos $(\mathrm{H}_{t-1}, \preceq)$, $(\mathbb{N}_0^{[k+1]}, \leq)$ and $(\mathrm{H}_0, \preceq)$. Note that the product order of any finite number of wpos is also a wpo. Suppose for some $A, B \in \mathrm{H}_t$ that $\delta(A) \sqsubseteq \delta(B)$. This implies that $A_{\cdot\cdot j_A} \leq B_{\cdot\cdot j_B}$ and that there exist strictly increasing maps ρ and σ such that $\rho(A_{\cdot\cdot[j_A]}) \leq B_{\cdot\cdot[j_B]}$ and $\sigma(A_{\cdot\cdot\{j_A+1,\ldots,\ell_A-1\}}) \leq B_{\cdot\cdot\{j_B+1,\ldots,\ell_B-1\}}$. We combine these into a single strictly increasing map $\tau : [\ell_A] \to [\ell_B]$ defined by

$$\tau(j) = \begin{cases} \rho(j) & \text{for } 0 \leq j < j_A \\ j_B & \text{for } j = j_A \\ \sigma(j - j_A - 1) + j_B + 1 & \text{for } j_A < j < \ell_A \end{cases},$$

illustrated in Figure 2. Then $\tau A \leq B$ so $A \preceq B$. Since $\sqsubseteq$ is a wpo, $(\mathrm{H}_t, \preceq)$ is also a wpo. $\square$

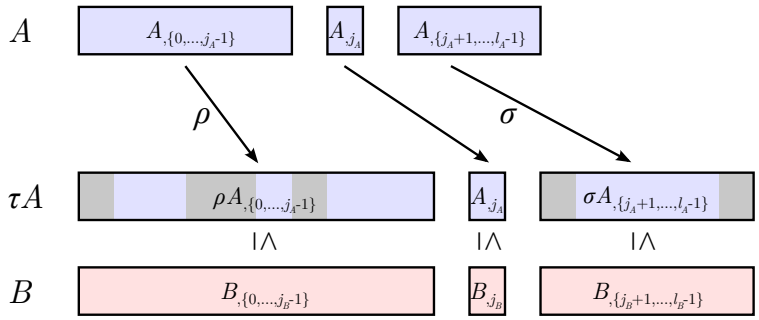

Figure 2: $\delta(A) \sqsubseteq \delta(B)$ implies $A \preceq B$.

Proposition 2.4.7. $(\mathrm{H}, \preceq)$ *is well-partially ordered.*

Proof. For any $A \in \mathrm{H}$, if j is a bad index of A, then for some $p \in [N]$, we have $d_{A,p}/2 > \sum_{i \in [k_p]} A_{p,i,j}$. Letting $J_p \subset \mathbb{N}$ be the set of bad indices of A with respect to p and let $J \subset \mathbb{N}$ be the union of the J_p. Then

$$|J_p| \frac{d_{A,p}}{2} < \sum_{j \in J_p} \sum_{i \in [k_p]} A_{p,i,j} \leq \sum_{i \in [k_p]} \sum_{j \in \mathbb{N}} A_{p,i,j} \leq k_p d_A$$

with the last inequality due to the row sum condition on A_p. Therefore $|J_p| \leq 2k_p - 1$, and hence $|J| \leq 2 \sum_{p \in [N]} k_p - N$.

Let $A^{(1)}, A^{(2)}, \ldots$ be any infinite sequence in H. Since the numbers of bad N-tuples of columns of elements of H are bounded by $2 \sum_{p \in [N]} k_p - N$ there exists a subsequence which is contained in H_t for some $0 \leq t \leq 2 \sum_{p \in [N]} k_p - N$. By Proposition 2.4.6 there is $r < s$ with $A^{(r)} \preceq A^{(s)}$. $\square$

Proposition 2.4.8. $(\mathcal{M}, \preceq)$ *is well-partially ordered.*

Proof. Let $A^{(1)}, A^{(2)}, \ldots$ be any infinite sequence in $\mathcal{M}$. Each $A^{(r)}$ has some $j_r > 0$ such that all N-tuples of columns $A^{(r)}_{\cdot\cdot m}$ are zero for $m \geq j_r$. Consider the sequence $\tilde{A}^{(1)}_{\cdot\cdot[j_1]}, \tilde{A}^{(2)}_{\cdot\cdot[j_2]}, \ldots$ in H obtained by truncating each $\tilde{A}^{(r)}$ to the first j_r N-tuples of

columns. By Proposition 2.4.7 there is some $r < s$ and $\rho : [j_r] \to [j_s]$ such that $\rho \tilde{A}^{(r)}_{\cdot\cdot[j_r]} \leq \tilde{A}^{(s)}_{\cdot\cdot[j_s]}$. Note that this implies $d_{A^{(r)}} \leq d_{A^{(s)}}$. Extend ρ to some $\pi \in \mathrm{Inc}(\mathbb{N})$ so then

$$(\pi \tilde{A}^{(r)})_{\cdot\cdot[j_s]} = \rho(\tilde{A}^{(r)}_{\cdot\cdot[j_r]}) \leq \tilde{A}^{(s)}_{\cdot\cdot[j_s]}.$$

The remaining N-tuples of columns of $\pi \tilde{A}^{(r)}$ and $\tilde{A}^{(s)}$ are trivial, so $\pi \tilde{A}^{(r)} \leq \tilde{A}^{(s)}$ follows from the fact that $d_{A^{(r)}} \leq d_{A^{(s)}}$. Therefore $A^{(r)} \preceq A^{(s)}$ by Proposition 2.4.2.

□

Applying Proposition 2.4 to the monoid $\mathcal{M}$ proves that the ring $K\mathcal{M}$ is $\mathrm{Inc}(\mathbb{N})$-Noetherian. This concludes the proof of Proposition 2.4.1.

CHAPTER III

EQUIVARIANT MARKOV BASES AND LATTICE BASES

3.1 Equivariant Markov bases

In light of the Independent Set Theorem (Theorem 1.4.7) of Hillar and Sullivant [34] and Theorem 2.1.1 that generalizes it, many symmetric toric ideals are known to be finitely generated up to symmetry. However computing generating sets of such ideals is still a difficult task in general. One strategy is to use equivariant Gröbner basis algorithms, but often much smaller generating sets exist. We make some preliminary progress on the problem by producing explicit formulas for the minimal generating sets of the first family of equivariant ideals for which they were not previously known. The work in this chapter is joint with Thomas Kahle and Anton Leykin, and appears in [37]

The case we consider is the kernel of $\mathfrak{S}_\infty$-equivariant monomial map $\pi : K[Y] \to K[Z]$ where Y has one $\mathfrak{S}_\infty$ orbit with $k_1 = 2$. Here $Y := \{y_{ij} \mid i, j \in \mathbb{N},\, i \neq j\}$ and $Z := \{z_{ij} \mid i \in [k], j \in \mathbb{N}\}$ with $\mathfrak{S}_\infty$ acting on Y and Z by

$$\sigma(z_{ij}) = z_{i\sigma(j)} \text{ and } \sigma(y_{ij}) = y_{\sigma(i)\sigma(j)}.$$

One could hope to compute an equivariant Markov basis of $\ker(\pi)$ by computing a (usual) Markov basis M_n for some n-th truncation $\ker(\pi)_n = \ker(\pi) \cap K[Y_n]$ and check if it S_{n+l}-generates $\ker(\pi)_{n+l}$, for sufficiently many l. Unfortunately it is unknown how large l needs to be to guarantee stabilization.

We factor the map π as in the previous chapter

$$\pi : K[Y] \xrightarrow{\phi} K[X] \xrightarrow{\psi} K[Z], \tag{3.1.1}$$

$$y_{ij} \mapsto x_{1i}x_{2j}$$

$$x^B \mapsto z^{A_\psi B},$$

where A_ψ is a $k \times 2$ matrix with non-negative integer entries.

Since $\ker \pi$ is completely determined by $\ker A_\psi$, there are three cases to consider based on the rank of A_ψ. If $\operatorname{rank} A_\psi = 0$ then $\ker \pi = \langle y_{12} - 1 \rangle_{\mathfrak{S}_\infty}$. If $\operatorname{rank} A_\psi = 2$ then $\ker \pi = \ker \phi$ and this case has been solved in Theorem 1.4.10.

The outstanding non-trivial case is when $\operatorname{rank} A_\psi = 1$. Here $\ker A_\psi$ will be spanned by a vector $(b, -a)^T$ where a, b are non-negative integers. The case that $a = 0$ is also trivial with $\ker \pi = \langle y_{21} - y_{31} \rangle_{\mathfrak{S}_\infty}$ and similarly for $b = 0$. We then assume without loss of generality that $A_\psi = \begin{bmatrix} a & b \end{bmatrix}$ for relatively prime positive integers a, b. This is the case that $Z = \{z_i \mid i \in \mathbb{N}\}$ and

$$\pi : y_{ij} \mapsto z_i^a z_j^b. \tag{3.1.2}$$

The union of a Markov basis for $\ker(\phi)$ and the pullback of a Markov basis of $\operatorname{im}(\phi) \cap \ker(\psi)$ forms a Markov basis for $\ker(\pi)$. Generators of $\ker(\phi)$ are proved in Theorem 1.4.10 to be $\{y_{12}y_{23}y_{31} - y_{21}y_{32}y_{13},\ y_{12}y_{34} - y_{14}y_{32}\}$.

It remains to find generators for $\operatorname{im}(\phi) \cap \ker(\psi)$. For the remainder of this section, we consider the restriction of ψ to $\operatorname{im}(\phi)$, the matching monoid ring:

$$\operatorname{im}(\phi) = K[x_{1i}x_{2j} \mid i, j \in \mathbb{N},\ i \neq j] \subseteq K[X].$$

Proposition 3.1.1. *As an ideal in the matching monoid ring,* $\ker(\psi)$ *is generated by the* $\mathfrak{S}_\infty$*-orbits of the binomials* $x^A - x^B$ *from the following two finite families:*

1. *For each* $0 \leq n \leq a - b$,

$$A = \begin{bmatrix} b+n & n & c_{13} & c_{14} & \cdots \\ 0 & a & c_{23} & c_{24} & \cdots \end{bmatrix}, \quad B = \begin{bmatrix} n & b+n & c_{13} & c_{14} & \cdots \\ a & 0 & c_{23} & c_{24} & \cdots \end{bmatrix}$$

where $\sum_{j \geq 3} c_{1j} = a - b - n$ *and* $\sum_{j \geq 3} c_{2j} = n$.

2. For each $1 \leq n \leq b$,

$$A = \begin{bmatrix} b & 0 & a-b+n & 0 & \cdots \\ 0 & a & n & 0 & \cdots \end{bmatrix}, \quad B = \begin{bmatrix} 0 & b & a-b+n & 0 & \cdots \\ a & 0 & n & 0 & \cdots \end{bmatrix}.$$

Additionally, all these binomials are minimal with respect to division in the matching monoid ring.

The remainder of this section comprises the proof of Proposition 3.1.1. To deal with divisibility in the matching monoid, recall that a monomial $x^A \in K[X]$ is contained in the matching monoid if and only if there is some d such that both row sums of A are equal to d and all column sums of A are $\leq d$ (the matching monoid is normal). Consequently, a monomial is divisible by a generator if we can subtract one in two different columns (reducing the row sum), without violating the new column bound $d-1$.

Proposition 3.1.2. *As an ideal in the matching monoid ring,* $\ker(\psi)$ *is generated up to symmetry by binomials* $x^A - x^B$ *with*

$$A - B = \begin{bmatrix} b & -b & 0 & \cdots \\ -a & a & 0 & \cdots \end{bmatrix}.$$

Proof. Let $x^A - x^B \in \ker(\psi)$. The map π sends each variable in Y to a monomial of degree $a+b > 0$, so $\ker(\pi)$ is homogeneous. Therefore $A-B$ has row sums equal to 0. Moreover $A-B$ is annihilated by $\begin{bmatrix} a & b \end{bmatrix}$ so each column is a multiple of $(b,-a)^T$. Then $A-B$ must be of the form

$$\begin{bmatrix} b \\ -a \end{bmatrix} \begin{bmatrix} n_1 & n_2 & \cdots \end{bmatrix}$$

where the row vector $n = [n_1 \ n_2 \ \ldots]$ has entries summing to zero. Such a vector can be expressed as a sum $n = v_1 + \cdots + v_s$ where each v_i is in the $\mathfrak{S}_\infty$-orbit of

$\begin{bmatrix} 1 & -1 & 0 & \dots \end{bmatrix}$. Even more, the decomposition can be chosen *sign-consistently*, that is, each v_i has 1 in a position j where $n_j > 0$ and has -1 where $n_j < 0$.

Consider the sequence $B = B_0, B_1, \dots, B_s = A$ of matrices in $\psi^{-1}(B)$ defined by

$$B_i = B + \begin{bmatrix} b \\ \\ -a \end{bmatrix} (v_1 + \cdots + v_i).$$

The sequence is monotonic in each entry, and every column sum is also monotonic. Note that the all row sums of all B_i are equal to d. Since A and B are in the matching monoid, they have non-negative entries and all column sums $\leq d$. By the monotonicity of the sequence, each B_i also satisfies these properties and therefore is also in the matching monoid. The proof is complete since $x^{B_i} - x^{B_{i-1}} \in \ker(\psi)$ for any i, and

$$B_i - B_{i-1} = \begin{bmatrix} b \\ \\ -a \end{bmatrix} v_i = \sigma_i \begin{bmatrix} b & -b & 0 & \cdots \\ \\ -a & a & 0 & \cdots \end{bmatrix}$$

for some $\sigma_i \in \mathfrak{S}_\infty$. □

To prove Proposition 3.1.1 we need to intersect the matching monoid ring with the equivariant ideal generated by binomials $x^A - x^B$ with

$$A - B = \begin{bmatrix} b & -b & 0 & \cdots \\ \\ -a & a & 0 & \cdots \end{bmatrix}.$$

A general such pair A, B is of the form

$$A = \begin{bmatrix} c_{11} + b & c_{12} & c_{13} & c_{14} & \cdots \\ \\ c_{21} & c_{22} + a & c_{23} & c_{24} & \cdots \end{bmatrix} \quad B = \begin{bmatrix} c_{11} & c_{12} + b & c_{13} & c_{14} & \cdots \\ \\ c_{21} + a & c_{22} & c_{23} & c_{24} & \cdots \end{bmatrix}.$$

Let $C_j = c_{1j} + c_{2j}$ and $R_i = \sum_{j=1}^{\infty} c_{ij}$ be the column and row sums, respectively, *excluding* the contributions a and b in the first two columns.

We show that either the pair (A, B) is on the list in Proposition 3.1.1, or A and B are both divisible (in the matching monoid ring) by a common generator. Let

$d = R_1 + b = R_2 + a$ be the degree of A and B which gives a bound on column sums: $C_j \leq d - a$ for $j = 1, 2$ and $C_j \leq d$ otherwise. We say that a column is *loaded* if it achieves its bound. Loaded columns are obstacles to dividing by a common factor, since the degree can't be decreased without also decreasing the loaded columns by the same amount. A and B have a common factor if there exist positive c_{1j} and c_{2k} such that $j \neq k$ and there are no loaded columns outside of j and k.

Proof of Proposition 3.1.1. We distinguish four cases depending on the locations of the (at most two) loaded columns.

Case 1: No columns are loaded. We have $d > a$, so R_1 and R_2 are both positive. The monomials x^A and x^B have a common factor if there are positive c_{1j} and c_{2k} in different columns $j \neq k$, therefore $c_{ij} > 0$ only for one particular column j. If $j = 1$, then $C_1 = R_1 + R_2 = 2d - a - b > d - a$ which is a contradiction, and similarly for $j = 2$. Consequently $j \geq 3$ and thus A, B are of the second type for some $1 \leq n < b$.

Case 2: Column $j \geq 3$ is loaded. Let $C_j = d$. Since $\sum_j C_j = 2d - a - b$, any other column has $C_k \leq d - a - b$ and is not loaded. Because of the bounds $c_{1j} \leq R_1 = d - b$ and $c_{2j} \leq R_2 = d - a$ and the sum $c_{1j} + c_{2j} = d$, both c_{1j} and c_{2j} are positive. Again, all other values of c must be zero or else A and B have a common factor. Then we have $d = c_{1j} + c_{2j} = b + c_{1j} = a + c_{2j}$ and thus $c_{1j} = a$ and $c_{2j} = b$. Up to symmetry, this is the binomial of type 2 with $n = b$.

Case 3: Exactly one of Columns one and two is loaded. Say column one is loaded. In this case no column j can be loaded for $j \geq 3$: If $c_{11} > 0$ then by the divisibility argument $c_{2j} = 0$ for all $j \neq 1$, and similarly if $c_{21} > 0$, then $c_{1j} = 0$ for $j \neq 1$. Thus either $C_j = 0$ for $j > 1$ or one of R_1 or R_2 is zero. The first case leads to a contradiction as in Case 1. So all positive c values are in one row, which must be the first row since $R_1 > R_2$. This implies $d = a$ and thus that column one is loaded contradicting the assumption. By the same argument, we cannot have column two loaded and column one not loaded.

Case 4: Columns one and two are loaded. Either x^A, x^B are divisible by a common generator or we are in one of the following four situations: $c_{11} = c_{12} = 0$; $c_{21} = c_{22} = 0$; $C_1 = 0$; or $C_2 = 0$. However since both column 1 and column 2 are loaded, $C_1 = C_2 = d - a$, so $C_1 = 0$ if and only if $C_2 = 0$, and these cases are subsumed by the other two. If $c_{11} = c_{12} = 0$, then $c_{21} = c_{22} = d - a$. This implies

$$2(d-a) + \sum_{j \geq 3} c_{2j} = R_2 = d - a$$

so $R_2 = 0$. Therefore we need only consider the case $c_{21} = c_{22} = 0$. Here $c_{11} = c_{12} = d - a$ and

$$2(d-a) + \sum_{j \geq 3} c_{1j} = R_1 = d - b.$$

Therefore $\sum_{j \geq 3} c_{1j} = a - b - (d - a)$ and $\sum_{j \geq 3} c_{2j} = R_2 = d - a$. With $n = d - a$ this yields the binomials of type 1. □

Proposition 3.1.3. *The $\mathfrak{S}_\infty$-orbits of the generators in Proposition 3.1.1 form a universal Gröbner basis of* $\ker(\psi)$ *as an ideal in the matching monoid ring.*

Proof. Fix any monomial x^B in the matching monoid ring and a monomial order $\leq$. Let x^A be the standard monomial in the equivalence class of x^B (that the normal form of x^B). From the proof of Proposition 3.1.2, we have a path $B = B_0, B_1, \ldots, B_s = A$ which is monotonic in each entry and such that each $x^{B_{i+1}} - x^{B_i}$ is a monomial multiple of an element in $\mathfrak{S}_\infty G$ where G is the generating set in Proposition 3.1.1.

Suppose this path is not strictly decreasing in the monomial order, so there is some $x^{B_{i+1}} > x^{B_i}$. Let $C = A + B_i - B_{i+1}$. Because of the monotonicity of the sequence, the entries of C are between A and B so x^C is in the matching monoid, and $x^A > x^C$. This contradicts the assumption that x^A is a standard monomial. Therefore $\mathfrak{S}_\infty G$ is a Gröbner basis for this order. □

Remark 3.1.4. In the theory of equivariant Gröbner bases, only monomial orders that respect the monoid action are considered. However the set $\mathfrak{S}_\infty G$ is a Gröbner basis for *any* monomial order.

To get a generating set for $\ker(\pi)$ we combine the results of Theorem 1.4.10 and 3.1.1. In particular, for each generator g of $\ker(\psi)$, we find a representative of $\phi^{-1}(g) \subset K[Y]$, and then combine the resulting list with the two generators of $\ker(\phi)$. Interestingly, each generator of $\ker(\psi)$ has a *unique* binomial preimage in $K[Y]$.

Theorem 3.1.5. *In the setup of* (3.1.2) *with coprime $a > b$, the following binomials form a Markov basis of* $\ker(\pi)$.

1. $y_{12}y_{34} - y_{14}y_{32}$;

2. $y_{12}y_{23}y_{31} - y_{21}y_{32}y_{13}$;

3. *for each* $0 \le n \le a-b$,

$$y_{12}^{b+n} \prod_{j\ge 3} y_{j2}^{c_{1j}} y_{2j}^{c_{2j}} - y_{21}^{b+n} \prod_{j\ge 3} y_{j1}^{c_{1j}} y_{1j}^{c_{2j}}$$

   where $\sum_{j\ge 3} c_{1j} = a-b-n$ *and* $\sum_{j\ge 3}^{\infty} c_{2j} = n$;

4. *for each* $1 \le n \le b$,

$$y_{12}^{b-n} y_{13}^{n} y_{32}^{a-b+n} - y_{21}^{b-n} y_{23}^{n} y_{31}^{a-b+n}.$$

The maximum degree of binomials above is $\max(a+b, 2a-b)$ *and*

$$w(\ker(\pi)) = \max(4, a-b+2).$$

Proof. The only open items, the upper bound on the degree and the width formula, are easily checked: first is achieved by generators of type (3) or (4), second – by the basic quadric (1) or a generator of type (3).

To see the sharpness we show that for $n = 0$, the two monomials of the binomial in (3) are the only two elements in their multidegree. This multidegree is

$$d = (ab, ab, a, a, \dots, a, 0, \dots)$$

where there are $a-b$ entries equal to a. Let $m \in k[Y]$ be any monomial of multidegree d. The total degree of m equals a since $2ab+(a-b)a = a(a+b)$. Because of the a entries in d, m must divisible by $y_{3j_3}y_{4j_4}\cdots y_{aj_a}$ where each j_i is either one or two. Now since the first two entries of d both equal ab, the only possibility is that all j_i are equal. Consequently the only two monomials of multidegree d are two monomials in the type (3) binomial for $n = 0$ and whenever there are only two monomials of a given multidegree, their difference appears in every Markov basis. □

Remark 3.1.6. As in Proposition 3.1.1 the list of binomials of the third type in Theorem 3.1.5 is finite up to $\mathfrak{S}_\infty$-action. In particular, we need a representative for each partition of the pair $(a-b-n, n)$ into a sum of pairs of nonnegative numbers such that in no pair both entries are zero.

Remark 3.1.7. The maximal degree of the generators in Theorem 3.1.5 matches the degrees in Table 1 of [33]. However, we stop short of proving that our generating set is an equivariant Gröbner basis and we doubt that there needs to exist a term order for which it is one. According to our experiments in truncations, we expect the degrees in Gröbner bases to exceed those in Theorem 3.1.5. For instance in width five for $a = 2$, $b = 1$, the Markov complexity in Theorem 3.1.5 is three, while among many thousand random weight orders we have not found one with complexity smaller than five. In fact, we don't even know if kernels of the form considered here always admit finite equivariant Gröbner bases.

3.2 Equivariant lattice generators

Any monomial map π is closely related to its *linearization* A_π: the $\mathbb{Z}$-linear map on exponents

$$A_\pi : \bigoplus_{\mathbb{N}\times\mathbb{N}} \mathbb{Z} \to \bigoplus_{\mathbb{N}} \mathbb{Z}, \qquad A_\pi(e_{ij}) = ae_i + be_j$$

where e_{ij} and e_i are the standard basis vectors of $\bigoplus_{\mathbb{N}\times\mathbb{N}}\mathbb{Z}$ and $\bigoplus_{\mathbb{N}}\mathbb{Z}$, respectively, and $\bigoplus$ denotes the direct sum of modules. Each $v \in \bigoplus_{\mathbb{N}\times\mathbb{N}}\mathbb{Z}$ translates to a binomial

$y^{v_+} - y^{v_-} \in K[Y]$ where $(v_\pm)_i = \max\{\pm v_i, 0\}$ are the positive and negative parts of v, respectively. The binomials of this form are exactly those whose terms have greatest common divisor equal to one. All minimal generators of toric ideals are of this form.

The kernel $L = \ker(A_\pi)$ is an infinite-dimensional *(integer) lattice*. We call $V \subset \bigoplus_{\mathbb{N}\times\mathbb{N}} \mathbb{Z}$ an *equivariant lattice generating set* (or *equivariant lattice generators*) if the $\mathfrak{S}_\infty$-orbits of its elements generate L. This happens if and only if the $\mathfrak{S}_\infty$-orbits of $\{y^{v_+} - y^{v_-} \mid v \in V\}$ generate the extension of $\ker(\pi)$ in the ring of *Laurent polynomials* $K[Y^{\pm}]$. Note that any equivariant Markov basis also spans $\ker(\pi)K[Y^{\pm}]$ and so is an equivariant lattice generating set as well.

The goal of this section is to compute equivariant lattice generators for certain $\mathfrak{S}_\infty$-invariant toric ideals of the form appearing in Theorem 2.1.1. This is a strictly easier problem than computing Markov bases, but we will be able to push the results further. We consider $\mathfrak{S}_\infty$-equivariant maps $\pi : K[Y] \to K[Z]$ where Y has one $\mathfrak{S}_\infty$ orbit with general $k_1 = k$ and Z with a general number of orbits m. Here $Y := \{y_{(\alpha_1,\ldots,\alpha_k)} \mid \alpha_1, \ldots, \alpha_k \in \mathbb{N} \text{ distinct}\}$ and $Z := \{z_{ij} \mid i \in [m], j \in \mathbb{N}\}$ with $\mathfrak{S}_\infty$ acting on Y and Z by

$$\sigma(z_{ij}) = z_{i\sigma(j)} \text{ and } \sigma(y_{\alpha_1,\ldots,\alpha_k}) = y_{(\sigma(\alpha_1),\ldots,\sigma(\alpha_k))}.$$

Remark 3.2.1. Ideally, one would like to define an *equivariant lattice basis*, a generating set whose orbits freely generate the lattice. However, already in the finite-dimensional case this seems hard: Consider the sublattice of $\mathbb{Z}^3$ generated by S_3 acting on $(1, -1, 0)$. One would like to call $\{(1, -1, 0)\}$ an equivariant lattice basis, but there is a nontrivial linear relation among the elements of the orbit:

$$(1, 0, -1) + (-1, 1, 0) + (0, -1, 1).$$

Even if there are no relations among elements of the orbit, one has the problem that lattice bases can not be defined by inclusion minimality (the integers 2 and 3 span $\mathbb{Z}$, but no subset does). One remedy (in the finite-dimensional setting) are matroids

over rings as defined by Fink and Moci [23]. There each subset of the base set is assigned a module, instead of just its rank.

A width bound is given in [33] on lattice generators when $m = 1$ where π is defined by

$$y_\alpha \mapsto z_{\alpha_1}^{a_1} \cdots z_{\alpha_k}^{a_k}.$$

Their bound is $2d - 1$, where $d = a_1 + \cdots + a_k$ is the degree of the image monomial. We improve this bound and give an explicit construction of the equivariant lattice generators (Theorem 3.2.6) which generalizes to any m. The width of our basis is $k + 2$ and thus independent of m and degree d (Corollary 3.2.7). We proceed by the same general strategy as the previous chapter, factoring π as

$$\begin{aligned} \pi : K[Y] &\xrightarrow{\phi} K[X] \xrightarrow{\psi} K[Z], \\ y_\alpha &\mapsto x_{1\alpha_1} \cdots x_{k\alpha_k} \\ x^B &\mapsto z^{A_\psi B}, \end{aligned}$$

where A_ψ is a $m \times k$ matrix with non-negative integer entries. We compute a lattice generating set for $\ker(\psi) \cap \mathrm{im}(\phi)$, pull it back to $K[Y]$ and add in lattice generators for $\ker(\phi)$.

We first consider the case of width two ($k = 2$) to compare with the Markov bases discovered in the previous section. That is, consider the map $\pi : K[Y] \to K[X]$, defined by

$$y_{ij} \mapsto x_i^a x_j^b.$$

Proposition 3.2.2. *For π with width two, $\ker(\pi)K[Y^{\pm}]$ is generated up to symmetry by two binomials:*

$$y_{12}y_{34} - y_{14}y_{32} \quad \text{and} \quad y_{21}^b y_{31}^{a-b} - y_{12}^b y_{32}^{a-b}.$$

Proof. The *basic quadric* $y_{12}y_{34} - y_{14}y_{32}$ suffices to generate $\ker(\phi)K[Y^{\pm}]$ up to symmetry. This is a classic result in commutative algebra (see [52] for the early history)

and used often in algebraic statistics: (2×2)-minors are a Markov basis for the independence model (see Remark 3.2.4 and [21, § 1.1]). The non-existing diagonal variables pose no problem for us since we only need the Laurent case.

By Proposition 3.1.2 $\ker(\psi) \cap \mathrm{im}(\phi)$ is generated as an ideal in $\phi(K[Y])$ by all binomials $x^A - x^B$ with

$$A - B = \begin{bmatrix} b & -b & 0 & \cdots \\ -a & a & 0 & \cdots \end{bmatrix}.$$

Thus they also generate the lattice. Unlike in the Markov case, we need not find all minimal binomials with this difference. Instead, a single representative is enough. One such representative is $x_{12}^b x_{21}^a x_{13}^{a-b} - x_{11}^b x_{22}^a x_{13}^{a-b}$ which has preimage

$$y_{21}^b y_{31}^{a-b} - y_{12}^b y_{32}^{a-b}.$$

□

Remark 3.2.3. A generating set in $K[Y]$ for the kernel of $\phi^{(2)}$ requires the 3-cycle cubic $y_{12}y_{23}y_{31} - y_{21}y_{32}y_{13}$ (see Theorem 1.4.10). However in the Laurent ring $K[Y^{\pm}]$, this binomial is redundant modulo the basic quadric $y_{12}y_{34} - y_{14}y_{32}$.

$$\begin{aligned} y_{12}y_{23}y_{31} - y_{21}y_{32}y_{13} = \\ y_{12}y_{23}y_{24}^{-1}(y_{24}y_{31} - y_{21}y_{34}) \\ +y_{21}y_{23}y_{24}^{-1}(y_{12}y_{34} - y_{14}y_{32}) \\ +y_{21}y_{32}y_{24}^{-1}(y_{14}y_{23} - y_{13}y_{24}). \end{aligned}$$

We now generalize Proposition 3.2.2 to arbitrary k. When necessary, we write $\phi^{(k)}$ instead of ϕ to emphasize the width of the image monomial but usually the level of generality is clear from the context and we avoid overloading the notation too much. Elements of $\bigoplus_{\mathbb{N}^k} \mathbb{Z}$ should be thought of as k-dimensional tables of infinite size with integer entries. Our setup additionally requires that these tables be zero along their

diagonals (defined as entries indexed by $(i_1, \ldots, i_k)$ with any $i_j = i_l$ for $j \neq l$). Let $e_{i_1 \ldots i_k}$ denote the standard basis elements of $\bigoplus_{\mathbb{N}^k} \mathbb{Z}$. Then Y consists of indeterminates $y_{i_1 \ldots i_k} = y^{e_{i_1 \cdots i_k}}$. The factorization (3.1.1) gives a map $\phi^{(k)}$ as follows:

$$\phi^{(k)} : K[Y^{\pm}] \to K[Z^{\pm}], \qquad \phi^{(k)}(y_{i_1 \ldots i_k}) = z_{1i_1} z_{2i_2} \cdots z_{ki_k}.$$

Remark 3.2.4. In algebraic statistics, the *independence model on k factors* is (the non-negative real part of) the image of the monomial map $y_{i_1 \ldots i_k} \mapsto z_{1i_1} z_{2i_2} \cdots z_{ki_k}$ where $i_j \in [l_j]$ for some integers l_j [21]. In algebraic geometry, this map represents the Segre embedding $\mathbb{P}^{l_1 - 1} \times \cdots \times \mathbb{P}^{l_k - 1} \hookrightarrow \mathbb{P}^{l_1 l_2 \cdots l_k - 1}$. The coordinate ring of the Segre embedding is presented by quadrics of the form

$$y_{i_1 \ldots i_r \ldots i_s \ldots i_k} y_{i_1 \ldots i'_r \ldots i'_s \ldots i_k} - y_{i_1 \ldots i'_r \ldots i_s \ldots i_k} y_{i_1 \ldots i_r \ldots i'_s \ldots i_k},$$

where $i_j, i'_j \in [l_j]$. This setup differs from ours because diagonal entries like y_{11} are forbidden for us. In the analysis of contingency tables, this restriction is known as a specific *subtable-sum condition*, namely the sum over all diagonal entries equals zero [28]. Subtable-sum models have more complicated Markov bases than just independence models, but their lattice bases are still quadratic.

Proposition 3.2.5. *The lattice elements*

$$\mathrm{Quad}^{(k)} := \{e_{i_1 \ldots i_r \ldots i_s \ldots i_k} + e_{i_1 \ldots i'_r \ldots i'_s \ldots i_k} - e_{i_1 \ldots i'_r \ldots i_s \ldots i_k} - e_{i_1 \ldots i_r \ldots i'_s \ldots i_k}, \mid i_l, i'_l \in [k+2]\}$$

are an equivariant lattice generating set of $\ker(A_{\phi^{(k)}})$.

The elements of $\mathrm{Quad}^{(k)}$ are moves which take two elements differing in their indices at exactly two positions and then swap the values in one of those positions.

Proof of Proposition 3.2.5. It is easy to see that $\mathrm{Quad}^{(k)} \subseteq \ker(\phi^{(k)})$. To see $\langle \mathrm{Quad}^{(k)} \rangle \supseteq \ker(\phi^{(k)})$, we first show that $\langle \mathrm{Quad}^{(k)} \rangle$ contains all elements of the form

$$e_{a_1 \ldots a_k} + e_{b_1 \ldots b_k} - e_{a_1 \ldots a_{k-1}, b_k} - e_{b_1 \ldots b_{k-1}, a_k}$$

where $a_1, \ldots, a_k, b_k$ are distinct and also $b_1, \ldots, b_k, a_k$ are distinct. Now denote $N = \max\{a_1, \ldots, a_k, b_1, \ldots, b_k\}$ and consider the following telescopic sum in $\mathrm{Quad}^{(k)}$:

$$\begin{aligned}
&e_{a_1\ldots a_k} - e_{a_1\ldots a_{k-1}b_k} - (e_{(N+1)a_2\ldots a_k} - e_{(N+1)a_2\ldots a_{k-1}b_k}) \\
&+e_{(N+1)a_2\ldots a_k} - e_{(N+1)a_2\ldots a_{k-1}b_k} - (e_{(N+1)(N+2)a_3\ldots a_k} - e_{(N+1)(N+2)a_3\ldots a_{k-1}b_k}) \\
&\vdots \\
&+e_{(N+1)\ldots(N+k-2)a_{k-1}a_k} - e_{(N+1)\ldots(N+k-2)a_{k-1}b_k} - (e_{(N+1)\ldots(N+k-1)a_k} - e_{(N+1)\ldots(N+k-1)b_k}) \\
&= e_{a_1\ldots a_k} - e_{a_1\ldots a_{k-1}b_k} - (e_{(N+1)\ldots(N+k-1)a_k} - e_{(N+1)\ldots(N+k-1)b_k}).
\end{aligned}$$

Similarly, $e_{b_1\ldots b_k} - e_{b_1\ldots b_{k-1}a_k} - (e_{(N+1)\ldots(N+k-1)b_k} - e_{(N+1)\ldots(N+k-1)a_k}) \in \langle \mathrm{Quad}^{(k)} \rangle$ and taking the sum of the two yields the claim.

Now let $C := \sum_{I\in\mathbb{N}^k} c_I e_I \in \ker(\phi^{(k)})$. For any $m \in \mathbb{N}$ let C_m denote the slice of C of entries whose last index value is m, so $C_m := \sum_{I\in\mathbb{N}^{k-1}} c_{Im} e_{Im}$. The sum of the entries of C_m is zero, so C_m can be decomposed into a sum of terms of the form $e_{a_1\ldots a_{k-1}m} - e_{b_1\ldots b_{k-1}m}$. For each such summand, there is a corresponding element $e_{a_1\ldots a_{k-1}m} - e_{b_1\ldots b_{k-1}m} - (e_{a_1\ldots a_{k-1}M} - e_{b_1\ldots b_{k-1}M}) \in \langle \mathrm{Quad}^{(k)} \rangle$, where M is some fixed constant larger than any index value appearing in C. Summing up these moves shows

$$C_m - \sum_{I\in\mathbb{N}^{k-1}} c_{Im} e_{IM} \in \langle \mathrm{Quad}^{(k)} \rangle.$$

Summing over m shows that $C - D \in \langle \mathrm{Quad}^{(k)} \rangle$ where $D := \sum_{I\in\mathbb{N}^k} c_I e_{i_1\ldots i_{k-1}M}$. Since $\langle \mathrm{Quad}^{(k)} \rangle \subseteq \ker(\phi^{(k)})$, also $D \in \ker(\phi^{(k)})$. All non-zero entries of D have M as their last index entry and dropping it we get an element $D' \in \ker(\phi^{(k-1)})$. In the base case $k = 2$, $\phi^{(k-1)}$ is an isomorphism, so D' and then D are 0 and therefore $C \in \langle \mathrm{Quad}^{(k)} \rangle$. For $k > 2$, we can assume by induction that $\langle \mathrm{Quad}^{(k-1)} \rangle = \ker(\phi^{(k-1)})$, so D' can be decomposed into moves in $\mathrm{Quad}^{(k-1)}$. Since D' doesn't depend of the the choice of M, we can choose M larger than any index value used in this decomposition. Therefore appending M as the k-th index value produces a decomposition of D in $\mathrm{Quad}^{(k)}$, which proves that $C \in \langle \mathrm{Quad}^{(k)} \rangle$. □

To describe $\ker(\pi)K[Y^{\pm}]$, we proceed to describe $\ker(\psi)$ and its intersection with $\mathrm{im}(\phi)$, working directly with the respective linearizations A_π, A_ϕ, and A_ψ. The

linearization of $\psi : z_{ij} \mapsto \prod_{l=1}^{m} x_{lj}^{a_{li}}$ acts on lattice elements by left multiplication with the $m \times k$ matrix $A_\psi = (a_{ij})$. We will assume that $\operatorname{rank} A_\psi > 0$. The kernel of A_ψ is a p-dimensional sublattice of $\mathbb{Z}^k$ for some $0 \leq p < k$. Let $B = (b_1, \ldots, b_p)$ be a $k \times p$ matrix whose columns $b_1, \ldots, b_p$ are a lattice basis of that kernel. Any element in $\ker(\psi \circ \phi)$ is homogeneous: the entries of its exponent vector sum to zero. Consequently the columns of any $C \in A_\phi(\ker(A_{\psi\circ\phi})) = \operatorname{im}(A_\phi) \cap \ker(A_\psi)$ also sum to zero. With the basis B, if $C = BC'$ with $C' \in \bigoplus_{[k-1]\times\mathbb{N}} \mathbb{Z}$, then the columns of C' sum to zero as well. The lattice of matrices in $\bigoplus_{[k-1]\times\mathbb{N}} \mathbb{Z}$ with zero row sums is generated by the matrices with a 1 and -1 in any two entries of a particular row, and zero elsewhere. Therefore $\operatorname{im}(A_\phi) \cap \ker(A_\psi)$ is contained in the lattice generated by the orbits of

$$B_i := \begin{bmatrix} b_i & -b_i & 0 & \cdots \end{bmatrix}$$

for $i = 1, \ldots, p$. More specifically $\operatorname{im}(A_\phi) \cap \ker(A_\psi) \subseteq \langle B_1, \ldots, B_p \rangle_{\mathfrak{S}_\infty} \subseteq \ker(A_\psi)$. We show constructively that $B_i \in \operatorname{im}(A_\phi)$, so in fact the orbits of $B_1, \ldots, B_p$ generate $\operatorname{im}(A_\phi) \cap \ker(A_\psi)$. For each $1 \leq j \leq k$ consider the lattice element

$$f_j := e_{\alpha_1 \ldots \alpha_{j-1} 1 \, \alpha_{j+1} \ldots \alpha_k} - e_{\alpha_1 \ldots \alpha_{j-1} 2 \, \alpha_{j+1} \ldots \alpha_k} \in \bigoplus_{\mathbb{N}^k} \mathbb{Z} \text{ with } \alpha_l \geq 3 \text{ arbitrary.}$$

Applying A_ϕ, all entries cancel except for the two in the j-th row, producing the matrix with 1 in the $(j, 1)$ entry and -1 in the $(j, 2)$ entry. Any B_i can be expressed as a linear combination of such matrices. In particular if b_i has entries $c_1, \ldots, c_k$ then

$$w_i := c_1 f_1 + \cdots + c_k f_k \in A_\phi^{-1}(B_i).$$

This proves the following theorem.

Theorem 3.2.6. *Up to symmetry,* $\operatorname{Quad}^{(k)} \cup \{w_1, \ldots, w_p\}$ *is an equivariant lattice generating set of* $\ker(A_\pi)$*, where* k *is the width of the map* π *and* $p < k$*.*

Corollary 3.2.7. *The lattice* $\ker(A_\pi)$ *has an equivariant lattice generating set consisting of at most* $(k^2 + k - 2)/2$ *elements of width* $k + 2$*.*

Proof. Up to $\mathfrak{S}_\infty$-action, each element of $\mathrm{Quad}^{(k)}$ is determined by the two index positions where the swap takes place. So $\mathrm{Quad}^{(k)}$ contributes $\binom{k}{2}$ generators. Additionally we have $w_1, \ldots, w_{k-1}$, which totals $(k^2+k-2)/2$. Choosing every f_j with $\alpha_1, \ldots, \hat{a}_j, \ldots, \alpha_k$ being $3, \ldots, k+1$ produces the width bound. □

This generating set is often not minimal in size. In fact, we can do away with all of $\mathrm{Quad}^{(k)}$ at the expense of increasing the width of the w_i.

Corollary 3.2.8. *The lattice* $\ker(A_\pi)$ *has an equivariant lattice generating set consisting of* $k-1$ *elements of width* $2k$.

Proof. Suppose b_l is a generator of $\ker(A_\psi)$ which is non-zero in the i-th coordinate for some $1 \leq i \leq k$. Choose w_l as in Corollary 3.2.7, except that one copy of f_i is replaced by

$$f_i' := e_{\alpha_1' \ldots \alpha_{i-1}' 1 \, \alpha_{i+1}' \ldots \alpha_k'} - e_{\alpha_1' \ldots \alpha_{i-1}' 2 \, \alpha_{i+1}' \ldots \alpha_k'}$$

which has $\alpha_1', \ldots, \hat{\alpha_i'} \ldots, \alpha_k'$ equal to $k+2, \ldots, 2k$. Then for any $j \neq i$ consider the lattice element $w_l - \sigma w_l$ where $\sigma \in \mathfrak{S}_\infty$ is the permutation switching α_j' and $2k+1$. All terms cancel except for $f_i' - \sigma f_i'$ which (up to permutation) is the element of $\mathrm{Quad}^{(k)}$ which switches the indices at positions i and j.

For any generating set $b_1, \ldots, b_p$ of $\ker(A_\psi)$, by Hall's marriage theorem we can assign to each b_l a distinct i_l such that the the i_l-th coordinate of b_l is non-zero. Then $i_1, \ldots, i_{k-1}$ include all but $k-p$ of the values from 1 to k. Construct each w_l as above so that it generates the elements of $\mathrm{Quad}^{(k)}$ corresponding to all pairs (i_l, j) with $j \neq i_l$. Let $i_{p+1}, \ldots, i_k$ be the values of i not included in $i_1, \ldots, i_p$. For $p < l \leq k$ let $w_l = f_i' - \sigma f_i'$ where $\sigma \in \mathfrak{S}_\infty$ is the permutation switching α_j' and $2k+1$. Then $w_1, \ldots, w_k$ generates all of $\mathrm{Quad}^{(k)}$ but in fact we can leave out w_k since every pair of distinct elements (i, j) includes at least one of $i_1, \ldots, i_{k-1}$, Therefore $w_1, \ldots, w_{k-1}$ is a lattice generating set. □

Note that neither the bounds in Corollary 3.2.7 nor 3.2.8 are sharp: For example, the kernel of $y_{ij} \mapsto x_i^2 x_j$ in $K[Y^{\pm}]$ is generated by a single binomial of width three: $y_{12}y_{32} - y_{21}y_{31}$.

We would like to be able to extend these techniques to a more general domain ring $K[Y^{\pm}]$ with $Y = \{y_{i\alpha} \mid i \in [N], \alpha \in \mathbb{N}^k, \alpha_j \text{ distinct}\}$ for $N > 1$, but there are obstacles. Here the lattice $Z^{\pm}$ is represented by $Nk \times \mathbb{N}$ matrices, with k rows in the image of each of the N orbits of Y. Our previous argument breaks down because the matrices corresponding to binomials in $\phi(\ker(\pi))$ need not have all row sums equal to zero, which was critical to the construction used when $N = 1$. Binomials in $\ker(\pi)$ need not be homogeneous, and even homogeneous binomials need not correspond to matrices in $Z^{\pm}$ with zero row sums.

CHAPTER IV

EQUIVARIANT GRÖBNER BASES

Gröbner bases are a ubiquitous tool in computational algebraic geometry. First introduced by Buchberger in 1965, they now play a crucial role in symbolic algorithms for solving polynomial systems, testing ideal membership of polynomials, intersecting ideals, variable elimination, primary decomposition, computing syzygies and much more. Cohen and later Aschenbrenner, Hillar, Brouwer and Draisma [11][3][7] developed the notion of Π-equivariant Gröbner bases, which we can define as follows. We will assume throughout this chapter that K is a field.

Definition 4.0.9. Let $R = K\,\mathrm{M}$ be a monoid ring with Π action on M, and let $\leq$ be a Π respecting monomial order. Given a Π-invariant ideal $I \subseteq R$, a Π-equivariant Gröbner basis of I is a set $G \subseteq I$ such that the Π orbits of G form a Gröbner basis of I,

$$\langle \mathrm{in}_{\geq}\, \Pi G \rangle = \mathrm{in}_{\geq}\, I.$$

We require $\leq$ to be a Π respecting order because it is equivalent to the condition that

$$\mathrm{in}_{\geq}\, \sigma f = \sigma\, \mathrm{in}_{\geq}\, f$$

for all $f \in R$ and $\sigma \in \Pi$. Therefore with such an order, the lead terms of G determine $\mathrm{in}_{\geq}\, I$ in that

$$\langle \mathrm{in}_{\geq}\, G \rangle_{\Pi} = \langle \mathrm{in}_{\geq}\, \Pi G \rangle = \mathrm{in}_{\geq}\, I.$$

This also implies that $\mathrm{in}_{\geq}\, I$ is a Π-invariant ideal. Note that since the Π orbits of G are a Gröbner basis of I, they also generate I, and so $\langle G \rangle_{\Pi} = I$.

Recall that R with non-trivial $\mathfrak{S}_\infty$ action has no $\mathfrak{S}_\infty$ respecting monomial orders, but that any $\mathfrak{S}_\infty$-invariant ideal is naturally $\mathrm{Inc}(\mathbb{N})$-invariant. When computing Gröbner bases of $\mathfrak{S}_\infty$-invariant ideals we will work exclusively with the $\mathrm{Inc}(\mathbb{N})$ action instead. Generally the rings we are interested in will have $\mathrm{Inc}(\mathbb{N})$ respecting monomial orders.

If R is Π-Noetherian with a Π respecting monomial order, then any Π-invariant ideal $I \subseteq R$ will have a finite Π-equivariant Gröbner basis. This follows from the fact that $\mathrm{in}_{\geq} I$ is Π-finitely generated. When R is not Π-Noetherian, we do not know in general if a Π-finitely generated ideal I has a finite Π-equivariant Gröbner basis, or if so, for which monomial orders. However we will prove in Section 4.2 that $\mathfrak{S}_\infty$-invariant toric ideals of the type considered in Theorem 2.1.1 do have finite $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner bases for specifically chosen monomial orders.

Analogous to the usual Gröbner basis theory, Π-reductions and Π-normal forms can defined as follows. Suppose $f, g \in R$ and $\mathrm{in}_{\geq} g \preceq \mathrm{in}_{\geq} f$ where $\preceq$ is the Π-divisibility partial order (Definition 1.3.5). We say that g Π-*reduces* f. There exists $c \in \mathrm{M} * \Pi$ such that $c \,\mathrm{LM}\, g = \mathrm{LM}\, f$, and a Π-*reduction* of f by g is

$$f - \frac{\mathrm{LC}\, f}{\mathrm{LC}\, g} cg$$

which cancels the lead term of f. Here $\mathrm{LM}\, f$ and $\mathrm{LC}\, f$ denote the lead monomial and lead coefficient of f respectively. Note that unlike usual reductions, c is not necessarily unique, and the reduction may depend on the choice of c.

For $f \in R$ and $G \subseteq R$, a Π-*normal form* of f with respect to G, $\mathrm{NF}_G(f)$ is an element obtained by performing Π-reductions of f by elements of G until no further reductions are possible. By definition $\mathrm{in}_{\geq} \mathrm{NF}_G(f) \notin \langle \mathrm{in}_{\geq} G \rangle_\Pi$ and $\mathrm{NF}_G(f) \equiv f \mod \langle G \rangle_\Pi$. If G is a Π-equivariant Gröbner basis of $\langle G \rangle_\Pi$ then $\mathrm{NF}_G(f)$ is uniquely determined and is zero if and only if $f \in \langle G \rangle_\Pi$, but this is not true for general G.

4.1 Equivariant Buchberger algorithm

An equivariant version of Buchberger's algorithm for computing equivariant Gröbner bases was first proposed in [3] with the details worked out in [7].

Let $R = K\,\mathrm{M}$ with Π acting on M, and let $\leq$ be a Π respecting monomial order. The input will be a finite set F which generates Π-invariant ideal I up to symmetry, and the output (if the algorithm terminates) will be G, a finite Π-equivariant Gröbner basis of I. The algorithm starts with $G = F$, forms S-polynomials from all pairs of elements $f, g \in G$, which are polynomials of the form

$$cf - \frac{\mathrm{LC}\, f}{\mathrm{LC}\, g} dg$$

for $c, d \in \mathrm{M}*\Pi$ such that $\mathrm{in}_{\geq}\, cf = \mathrm{in}_{\geq}\, dg$. For each S-polynomial s the algorithm computes the Π-normal form of s by G. If $\mathrm{NF}_G(s) \neq 0$ then it is appended to G, and the additional S-polynomials are formed between this new element and the old ones. Once all S-polynomials are reduced to 0 by G, the algorithm returns G.

The main departure from the usual Buchberger algorithm is that for a given pair $f, g \in R$ there will be many S-polynomials rather than just one. Given f, g, consider the set of pairs

$$\mathcal{S}_{f,g} = \{(cf, dg) \mid c, d \in \mathrm{M}*\Pi,\ \mathrm{in}_{\geq}\, cf = \mathrm{in}_{\geq}\, dg\}.$$

This set is closed under the diagonal action of $\mathrm{M}*\Pi$ making $\mathcal{S}_{f,g}$ a $\mathrm{M}*\Pi$-module. When Π is trivial and R is a polynomial ring (the context of the usual Buchberger algorithm), $\mathcal{S}_{f,g}$ is generated by a single pair $(\frac{m}{\mathrm{LM}(f)} f,\ \frac{m}{\mathrm{LM}(g)} g)$ where $m = \mathrm{lcm}(\mathrm{in}_{\geq} f, \mathrm{in}_{\geq} g)$. This corresponds to the usual S-polynomial $S(f, g)$. In the more general situation, a generating set of $\mathcal{S}_{f,g}$ may be much larger. If $\mathcal{S}_{f,g}$ is not finitely generated, the Equivariant Buchberger algorithm cannot check the set in finite time. Therefore the following condition will be necessary to apply the algorithm.

Definition 4.1.1. A Π-algebra $R = K\,\mathrm{M}$ has the *finite S-pair condition* if for any

$f, g \in R$, the set $\mathcal{S}_{f,g}$ is finitely generated as a $\mathrm{M} * \Pi$-module. In [7] this condition is referred to as "EGB4."

Proposition 4.1.2. *If $\Pi = \mathrm{Inc}(\mathbb{N})$ and R is a finite width polynomial ring $R = K[Y]$ then R has the finite S-pair condition.*

Proof. Fix $f, g \in R$. Since R is a polynomial ring, for fixed $\sigma_1, \sigma_2 \in \mathrm{Inc}(\mathbb{N})$, all elements of $\mathcal{S}_{f,g}$ of the form $(m_1\sigma_1 f, m_2\sigma_2 g)$ with $m_1, m_2 \in \mathrm{M}$ are monomial multiplies of the usual S-pair of $\sigma_1 f, \sigma_2 g$,

$$\left(\frac{m}{\mathrm{in}_{\geq} \sigma_1 f} \sigma_1 f,\ \frac{m}{\mathrm{in}_{\geq} \sigma_2 g} \sigma_2 g \right)$$

where $m = \mathrm{lcm}(\mathrm{in}_{\geq} \sigma_1 f, \mathrm{in}_{\geq} \sigma_2 g)$.

Any $f, g \in R$ have finite width so $\sigma_1 f$ depends only on where σ_1 sends $[w(f)]$, and similarly for $\sigma_2 g$. In fact we can always factor the pair as

$$(\sigma_1 f, \sigma_2 g) = \tau(\rho_1 f, \rho_2 g)$$

for some $\tau \in \mathrm{Inc}(\mathbb{N})$, while $\rho_1 : [w(f)] \to [w(f)+w(g)]$ and $\rho_2 : [w(g)] \to [w(f)+w(g)]$ are strictly increasing functions. Here ρ_1 and ρ_2 are chosen to "interlace" the variables of f and g in the same way as σ_1, σ_2. (To consider ρ_1, ρ_2 as elements of $\mathrm{Inc}(\mathbb{N})$, take any choice of extensions to maps on $\mathbb{N}$.)

Then $\mathcal{S}_{f,g}$ is generated by the finite set of pairs of the form

$$\left(\frac{m}{\mathrm{in}_{\geq} \rho_1 f} \rho_1 f,\ \frac{m}{\mathrm{in}_{\geq} \rho_2 g} \rho_2 g \right)$$

with $\rho_1 : [w(f)] \to [w(f) + w(g)]$ and $\rho_2 : [w(g)] \to [w(f) + w(g)]$ where $m = \mathrm{lcm}(\mathrm{in}_{\geq} \rho_1 f, \mathrm{in}_{\geq} \rho_2 g)$. □

Assuming R satisfies the finite S-pair condition, let $O_{f,g}$ denote the set of S-polynomials formed from a finite minimal generating set of $\mathcal{S}_{f,g}$. Then we can precisely describe the algorithm.

Algorithm 4.1.3 (Brouwer–Draisma [7]). $G = \text{Buchberger}(F)$

Require: F is a finite set of elements in $R = K\,\mathrm{M}$ with Π acting on M and satisfying the finite S-pair condition.

Ensure: G is Π-equivariant Gröbner basis of $\langle F\rangle_\Pi$.

$G \leftarrow F$

$S \leftarrow \bigcup_{f,g\in G} O_{f,g}$

while $S \neq \emptyset$ **do**

  pick $f \in S$

  $S \leftarrow S \setminus \{f\}$

  $h \leftarrow \mathrm{NF}_G(f)$

  if $h \neq 0$ **then**

    $G \leftarrow G \cup \{h\}$

    $S \leftarrow S \cup \left(\bigcup_{g\in G} O_{g,h}\right)$

  end if

end while

---

proof of correctness. Suppose G satisfies the equivariant version of Buchberger's criterion: that for all $f, g \in G$, every $s \in O_{f,g}$ has $\mathrm{NF}_G(s) = 0$. The criterion implies that all S-polynomials s formed from pairs in ΠG have Π-normal form equal to 0, which is to say they are reduced to zero by the set ΠG. By the usual Buchberger's criterion this means ΠG is a Gröbner basis of $\langle F\rangle_\Pi$, and so G is a Π-equivariant Gröbner basis. □

We note that Algorithm 4.1.3 is not guaranteed to terminate, except in particular situations such as when R is Π-Noetherian. In the Noetherian case, let $G_0, G_1, \ldots$ be the value of G at each step. The initial ideals of these sets form a strictly increasing chain of Π-invariant monomial ideals

$$\langle \mathrm{in}_{\geq} G_0\rangle_\Pi \subsetneq \langle \mathrm{in}_{\geq} G_1\rangle_\Pi \subsetneq \cdots$$

which must terminate.

In general, it may be that $\langle F \rangle_\Pi$ does not have a finite Π-equivariant Gröbner basis for the chosen monomial order. But even when a finite Π-equivariant Gröbner basis is known to exist, we have no guarantee for termination of the algorithm as stated above. We can fix this when $\Pi = \mathrm{Inc}(\mathbb{N})$ and certain conditions on R are met, which is addressed below.

4.1.1 Termination of $\mathrm{Inc}(\mathbb{N})$-equivariant Buchberger

Let $R = K\,\mathrm{M}$ with $\mathrm{Inc}(\mathbb{N})$ action on M, with R satisfying the finite S-pair condition, and with each truncation R_n a Noetherian ring. (These conditions are satisfied for example when $R = K[Y]$ where Y consists of a finite number of orbits of variables, as in Theorem 2.1.1.) Let $I \subseteq R$ be a $\mathrm{Inc}(\mathbb{N})$-invariant ideal which is $\mathrm{Inc}(\mathbb{N})$-generated by finite set F, and moreover has finite $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis G. Define the *generator truncation* of I to be $\tilde{I}_{F,n} := \langle \mathrm{Inc}(\mathbb{N})F \cap R_n \rangle \cap R_n$. Note that $\tilde{I}_{F,n} \subseteq I_n$ but in general equality does not hold. For $f \in I$ define $w_F(f)$ to be the minimum value of n for which $f \in \tilde{I}_{F,n}$.

Consider the following variation of the equivariant Buchberger algorithm on input F. For each successive $n \geq w(F)$, compute a set G_n such that $\mathrm{Inc}(\mathbb{N})G_n \cap R_n$ is a Gröbner basis for $\tilde{I}_{F,n}$. Then check if G_n is a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of I using the equivariant Buchberger criterion, and if so return G_n.

Algorithm 4.1.4. $G = \mathrm{TruncatedEGB}(F)$

Require: F is a finite set of elements in $R = K\,\mathrm{M}$ with $\mathrm{Inc}(\mathbb{N})$ acting on M, R satisfies the finite S-pair condition, and each R_n is Noetherian.

Ensure: G is a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of $I := \langle F \rangle_{\mathrm{Inc}(\mathbb{N})}$.

1: $G \leftarrow F$

2: $n \leftarrow w(F)$

3: **while** G not a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of I **do**

4: $\quad G \leftarrow$ Gröbner basis of $\tilde{I}_{F,n}$

5: $n \leftarrow n + 1$

6: **end while**

proof of termination. For each n, let G_n denote the value of G after that step. Computing G_n is a finite process since it takes place in R_n which is Noetherian. G_n is a finite set and so it has a finite number of S-pairs to be checked. Therefore testing whether G_n is a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis is finite.

It remains to be proved that G_n is a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis for some value of n. If H is a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of I, for any $h \in H$ we have $h \in \tilde{I}_{F,n}$ for all $n \geq w_F(h)$, so $\mathrm{LM}(h) \in \mathrm{LM}(\tilde{I}_{F,n})$. Therefore there is some element $g \in G_n$ with $\mathrm{LM}(g)|_{\mathrm{Inc}(\mathbb{N})}\, \mathrm{LM}(h)$. For $n = \max_{h \in H} w_F(h)$, the initial ideal $\langle \mathrm{LM}(G_n) \rangle_{\mathrm{Inc}(\mathbb{N})}$ contains $\langle \mathrm{LM}(H) \rangle_{\mathrm{Inc}(\mathbb{N})}$ and so G_n is a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of I. □

In practice, G_n can be computed either using a traditional Gröbner basis algorithm on input $\mathrm{Inc}(\mathbb{N})F \cap R_n$, or using an equivariant Buchberger algorithm on input F with the following two caveats:

- consider only S-pairs (cf, dg) with cf and dg both having width $\leq n$,
- perform only reductions such that the outcome has width $\leq n$.

Moreover we do not need to restart the algorithm from scratch at each n. Instead $G_{n-1} \cup F$ can be used as the input for the nth step instead of F.

Suppose R has the form $S[Y]$ and each $R_n = S[Y_n]$ for some $Y_n \subseteq Y$. If $\leq$ is a width order (a monomial order such that $w(a) < w(b)$ implies $a < b$), the second condition is satisfied automatically since reductions cannot increase the width. Therefore the normal form of a given S-pair does not depend on n, and does not need to be recomputed each time. As a result we can use Algorithm 4.1.3, queuing S-pairs by width so that the smallest width S-pairs are considered first. The algorithm

terminates once the queue is empty. A separate check for whether G_n is a Inc($\mathbb{N}$)-equivariant Gröbner basis for I is not needed since this is equivalent to reducing all S-pairs in the queue.

4.2 Symmetric Gröbner bases of toric ideals

The previous section an algorithm was given that is capable of computing a n Inc($\mathbb{N}$)-equivariant Gröbner basis of an ideal in a ring of the form $K[Y]$ with Inc($\mathbb{N}$) action on Y and Y having a finite number of orbits, with guaranteed termination *if* a finite Gröbner basis for the ideal exists. In this section we prove that any $\mathfrak{S}_\infty$-invariant toric ideal $\ker\phi$ of form in Theorem 2.1.1 has a finite Gröbner basis with respect to a particularly chosen monomial order. We then show that a Gröbner basis can be computed given the monomial map ϕ, using elimination (so generators of $\ker\phi$ are not needed as input).

This gives a general algorithm to compute a generating set up to symmetry of such toric ideals.

4.2.1 Existence of equivariant Gröbner bases of toric ideals

For $\mathfrak{S}_\infty$-equivariant monomial map $\pi : R[Y] \to R[X]$ factor the map as in Chapter 2,

$$R[Y] \xrightarrow{\phi} R[Z] \xrightarrow{\psi} R[X].$$

Let $\mathcal{M}$ denote the monoids of monomials $\phi[Y] \subseteq [Z]$. Choose an Inc($\mathbb{N}$)-compatible monomial order $\leq_1$ on $\mathcal{M}$ and an Inc($\mathbb{N}$)-compatible reverse lexicographic order $\leq_2$ on $[Y]$. Let $\leq$ be the monomial order on $[Y]$ defined by $a < b$ if $\phi(a) <_1 \phi(b)$ or $\phi(a) = \phi(b)$ and $a <_2 b$.

Theorem 4.2.1. $\ker\pi$ *has a finite* Inc($\mathbb{N}$)*-equivariant Gröbner basis H with respect to* $\leq$.

To prove this, we will first prove the existence of a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of $\ker\phi$ for order $\leq$. Recall that ϕ is determined by a sequence of integers $(k_1, \ldots, k_N)$ corresponding to the number of indices in each orbit of variables in Y. The map ϕ restricted to the pth orbit of variables has the form of $\phi^{(k_p)}$ defined by

$$\phi^{(k_p)} : y_{p,(\alpha_1,\ldots,\alpha_{k_p})} \mapsto \prod_{i=1}^{k_p} z_{p,i,\alpha_i}.$$

Proposition 4.2.2. *The kernel of ϕ has a Gröbner basis for order $\leq$ consisting of binomials of degree at most $2\max_p k_p - 1$.*

Note that this implies that $\ker\phi$ has finite $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis. Theorem 1.4.11 already showed that $\ker\phi$ is $\mathrm{Inc}(\mathbb{N})$-finitely generated (and in fact gives a better degree bound for $k > 2$), but the generating set produced here is also a Gröbner basis. The argument of the following proof is due to Jan Draisma, originally used to show a degree bound on generators of $\ker\phi$.

Proof. It suffices to prove the theorem for a single orbit $p \in [N]$. Given monomial v in the variables $y_{p,J},\ J \in \mathbb{N}^{[k_p]}$, let u be the minimal monomial with $\phi(u) = \phi(v) =: x_p^A$, i.e. the standard monomial of $\ker\phi$ in the fiber of $\phi(v)$. It suffices to show that there exists a chain $v = v_0 > v_1 > \ldots > v_t = u$ such that $\phi(v_s) = \phi(u)$ for all s and v_s, v_{s+1} differ in at most $2k_p - 1$ variables.

Proceed by induction on the degree of v. Suppose v and u have a variable $y_{p,J}$ in common. By the induction hypothesis there is a chain from $v/y_{p,j}$ to $u/y_{p,J}$ satisfying the desired conditions, since $u/y_{p,J}$ is also a standard monomial. This gives a chain from v to u.

Assume then that v and u have no variables in common and let $y_{p,J}$ be the smallest variable in u. Then $\phi(v)$ is divisible by $\phi(y_{p,J}) =: x_p^B$, and in fact v has a divisor v' of v of degree $e \leq k_p$ such that $\phi(v') =: x_p^{A'}$ is already divisible by x_p^B. Let S be the set of columns of A' where the column sum is equal to e, and let J be the set of column indices where B is non-zero. If S is contained in J, then $A' - B$ has all

column sums at most $e-1$, and hence $\phi(v')/x^B = \phi(v_1')$ for some monomial v_1'. Take $v_1 := \frac{v}{v'} \cdot v_1' \cdot y_{p,J}$. By construction, $\phi(v_1) = \phi(v)$ and v_1 shares the variable $y_{p,J}$ with u. Note that since $u < v$ and $\leq$ is reverse lexicographic on each fiber of ϕ, every variable in v is larger than $y_{p,J}$, so $v > v_1$ as well. Since $\deg v_1 = \deg v$ but v_1 and u share a variable, by the induction hypothesis there is a chain from v_1 to u satisfying the desired conditions.

If, on the other hand, $S \setminus J$ is non-empty, then for each $j \in S \setminus J$ the monomial v has a variable $y_{p,J'}$ with j not among the entries of J' (since otherwise all variables $y_{p,J'}$ in u would have j among the entries of J', which contradicts that $y_{p,J}$ is in u). Since $|S \setminus J| \leq k_p - 1$, we find by multiplying v' with at most that many variables in v a divisor v'' of v such that $\phi(v'')/\phi(y_{p,J}) \in \operatorname{im}\phi$, and we can proceed as above. The degree of v' is bounded by k_p so the degree of v'' is bounded by $2k_p - 1$. □

Let F denote such a finite $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of $\ker\phi$. We also know there exists G, a finite $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of $\ker\psi \cap \operatorname{im}\phi$ with respect to $\leq_1$, because $\operatorname{im}\phi$ is $\mathrm{Inc}(\mathbb{N})$-Noetherian by Theorem 2.1.1. The goal is to combine F with a "lift" of G to form a Gröbner basis of $\ker\pi$, and then show that this Gröbner basis has bounded degree.

Here we will use reductions (not $\mathrm{Inc}(\mathbb{N})$-reductions). We say $g \in \mathrm{Inc}(\mathbb{N})G$ *reduces* $a \in \mathcal{M}$ if $\mathrm{LM}_{\leq_1}(g)|a$, and the reduction is

$$b = a - \frac{a}{\mathrm{LM}_{\leq_1}(g)}g.$$

For each such pair a, g let u_a denote the minimal monomial in the fiber $\phi^{-1}(a)$ (a standard monomial of $\ker\phi$) and let $v_{a,g}$ be the monomial in $\phi^{-1}(b)$ that is closest to u_a. By this we mean the monomial which minimizes the total degree of the binomial

$$h_{a,g} := \frac{u_a - v_{a,g}}{\gcd(u_a, v_{a,g})}.$$

Note that $u_a > v_{a,g}$ and $\phi(h_{a,g}) = mg$ for some monomial $m \in \mathcal{M}$ so $h_{a,g}$ is a lift of

g. Let

$$\mathcal{H} = \mathrm{Inc}(\mathbb{N})F \cup \{h_{a,g} \mid a \in \mathcal{M},\ g \in \mathrm{Inc}(\mathbb{N})G \text{ reducing } a\}.$$

Proposition 4.2.3. *$\mathcal{H}$ is a Gröbner basis of $\ker \pi$ with respect to $\leq$.*

Proof. It's clear that $\mathcal{H} \subseteq \ker \pi$. For a monomial $m \in [Y]$, if m is not a standard monomial of $\ker \phi$ then m is reduced by some $f \in \mathrm{Inc}(\mathbb{N})F$. Assume then that m is a standard monomial of $\ker \phi$ so $m = u_a$ for some $a \in \mathcal{M}$. If a is a standard monomial of $\ker \psi$ then m is a standard monomial of $\ker \pi$. Otherwise a is reduced by some $g \in \mathrm{Inc}(\mathbb{N})G$, so m is reduced by $h_{a,g}$. □

If we can show that the elements of $\mathcal{H}$ have bounded degree, then $\mathcal{H}$ is contained in the $\mathrm{Inc}(\mathbb{N})$-orbits of a finite set H, which is then a finite $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis of $\ker \pi$, proving Theorem 4.2.1. This is shown in Proposition 4.2.4, below.

For monomial $z^A \in \mathcal{M}$, define the degree of z^A to be $d = (d_1, \ldots, d_N)$ if $z^A = \phi(m)$ with $\deg m = d$, or equivalently if $\|A_p\|_1 = k_p d_p$ for all $p = 1, \ldots, N$.

Proposition 4.2.4. *For every pair a, g with g reducing a, $\deg h_{a,g} \leq (d_1(3k_1 + 1), \ldots, d_N(3k_N + 1))$ where $d = (d_1, \ldots, d_N)$ bounds the degree of G.*

Proof. Express $h_{a,g}$ as $y^U - y^V$ where y^U and y^V have degrees n and m respectively, and g as $z^C - z^D$ with C, D in the matching monoid each of degree $\leq d$. Note that $\phi(U) - \phi(V) = C - D$, and as a consequence $|n_p - m_p| \leq d_p$ for each $p \in [N]$.

We can also express y^U as a product of variables

$$y^U = \prod_{p=1}^{N} \prod_{i=1}^{n_p} y_{p,J_{p,i}}.$$

If there is some (p, i) such that $\phi(y_{p,J_{p,i}})$ divides $b := \phi(y^V)$, then there is some other monomial $y^{V'} \in \phi^{-1}(b)$ which is divisible by $y_{p,J_{p,i}}$. Then $y^{V'}$ has the same degree as y^V but it has a common factor with y^U, contradicting the fact that $v_{a,g}$ was chosen to make $\deg h_{a,g}$ minimal. Therefore no $\phi(y_{p,J_{p,i}})$ divides b for any (p, i).

On the other hand, $\phi(U)$ and $\phi(V)$ can't be too far apart because of the degree bound on G. Fix any $p \in [N]$. Since $\phi(V_p) = \phi(U_p) - C_p + D_p$ and $\|C_p\|_1 \leq k_p d_p$, there are at most $k_p d_p$ values of i for which $\phi(e_{p,J_{p,i}}) \not\leq \phi(V)$. The remaining $e_{p,J_{p,i}}$ must have $\phi(e_{p,J_{p,i}}) \leq \phi(V)$, but not $\phi(y_{p,J_{p,i}})$ dividing $\phi(y^V)$. We will bound the number of variables in y^U that can satisfy this.

For A in the matching monoid, let $A_{p,+l}$ denote the lth column sum of A_p. Let $S_p \subset \mathbb{N}$ be the set of indices l such that $\phi(V)_{p,+l} = m_p$ (the maximum possible value). Note that if $y_{p,J}$ has $\phi(y_{p,J}) \leq \phi(V)$, then $\phi(y_{p,J})$ divides b if and only if S_p is a subset of the support of J. For any given l, exactly $\phi(U)_{p,+l}$ of the elements of $J_{p,1}, \ldots, J_{p,n_p}$ have l in their support and $\phi(U)_{p,+l} = \phi(V)_{p,+l} + C_{p,+l} - D_{p,+l}$. When $l \in S_p$, $\phi(U)_{p,+l} \geq m_p - D_{p,+l}$ so there are at most $n_p - m_p + D_{p,+l} \leq d_p + D_{p,+l}$ elements which do not have l in their support. Since $|S_p| \leq k_p$, there are at most $k_p d_p + \sum_{l \in S_p} D_{p,+l}$ which fail at some $l \in S_p$. Clearly $\sum_{l \in S_p} D_{p,+l} \leq \|D_p\|_1 \leq k_p d_p$ so the number of elements $J_{p,i}$ of the sequence which do not have S_p as a subset in their support is bounded by $2k_p d_p$. Combining these with the set of $J_{p,i}$ such that $\phi(e_{p,J_{p,i}}) \not\leq \phi(V)$, in total there are at most $3k_p d_p$ elements $J_{p,i}$ of $J_{p,1}, \ldots, J_{p,n_p}$ such that $\phi(y_{p,J_{p,i}})$ fails to divide b. Since no factor of y^{U_p} divides b, it must be that $n_p \leq 3k_p d_p$.

Since $\deg_p h_{a,g} = \max\{n_p, m_p\}$ and $|n_p - m_p| \leq d_p$, then $\deg_p h_{a,g} \leq 3k_p d_p + d_p$. □

This concludes the proof of Theorem 4.2.1. It is not known if $\ker \pi$ has finite $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner bases monomial orders other than those of the form in Theorem 4.2.1.

4.2.2 Computing equivariant Gröbner bases of toric ideals

To compute a Gröbner basis of $\ker \pi$ from the description of π we first compute a Gröbner basis of the graph of π, denoted $\Gamma_\pi \subseteq R[Y][X]$, with respect to an elimination order for X. Therefore we must prove that the graph has a finite $\mathrm{Inc}(\mathbb{N})$-equivariant

Gröbner basis with respect to such an elimination order. Algorithm 4.1.4 would then provide a way to compute the Gröbner basis.

$\Gamma_\pi := \langle y - \pi(y) \mid y \in Y \rangle$ is itself a $\mathfrak{S}_\infty$-invariant toric ideal. It is the kernel of the monomial map $\pi' : R[Y][X] \to R[X]$ defined by $\pi'(y^A x^C) = \pi(y^A)x^C$ for any monomial $y^A x^C$. Factoring π' in the prescribed way produces

$$R[Y][X] \xrightarrow{\phi'} R[Z][X] \xrightarrow{\psi'} R[X]$$

where $\phi'(y^A x^C) = \phi(y^A)x^C$ and $\psi'(z^B x^C) = \psi(z^B)x^C$ for all monomials $y^A \in [Y]$, $z^B \in [Z]$ and $x^C \in [X]$.

The monoid order $\leq_1$ on $\operatorname{im}\phi$ can be extended to an order $\leq_1'$ on $\operatorname{im}\phi' = (\operatorname{im}\phi)[X]$ that eliminates X. Define $\leq'$ to be the order on $[Y][X]$ such that $y^A x^C < y^B x^D$ if $\phi(y^A)x^C <_1' \phi(y^B)x^D$ or $\phi(y^A)x^C = \phi(y^B)x^D$ and $y^A <_2 y^B$. The restriction of $\leq'$ to $[Y]$ is the hybrid order $\leq$ constructed previously from $\leq_1$ and $\leq_2$. The order $\leq'$ eliminates $[X]$, and satisfies the hypotheses for Theorem 4.2.1 so there exists a finite $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis H' for Γ_π with respect to $\leq'$. Using the above algorithm, H' can be explicitly computed from the $\mathrm{Inc}(\mathbb{N})$-generators of Γ_π, which are

$$\{\sigma y_p - \pi(\sigma y_p) \mid p \in [N],\ \sigma \in \mathfrak{S}_{k_p}\}$$

where $y_1, \ldots, y_N$ are representatives of the $\mathfrak{S}_\infty$-orbits of Y. Then $H := H' \cap R[Y]$ is a $\mathrm{Inc}(\mathbb{N})$-equivariant Gröbner basis for $\ker\pi = \Gamma_\pi \cap R[Y]$ for the order $\leq$.

CHAPTER V

MACAULAY DUAL SPACES

5.1 Dual spaces in numerical algebraic geometry

An algorithmic approach to complex algebraic geometry known as *numerical algebraic geometry* (see [57, 56]) provides fast approximate methods to *solve* systems of polynomial equations. In case when the solution set is a finite set of points *polynomial homotopy continuation* techniques are able to find approximations to all solutions. In case when the solution set is positive-dimensional, it is a union of irreducible complex affine varieties and *numerical irreducible decomposition* [55] is performed to capture the information about the irreducible pieces with numerical data stored in the so-called *witness sets*. In ideal-theoretic terms, given a generating set of an ideal I in the polynomial ring $R = \mathbb{C}[x] = \mathbb{C}[x_1, \ldots, x_N]$, the numerical irreducible decomposition gives a numerical description of the components corresponding to the prime ideals P_i in the decomposition of the radical $\sqrt{I} = P_1 \cap \cdots \cap P_r$.

Our goal is to use the same numerical algebraic geometry approach to solve the problem of *numerical primary decomposition* [44]. That is to find a generic point on every component of the affine scheme $\mathrm{Spec}(R/I)$; in ideal-theoretic terms, find a generic[1] point on the component $\mathbb{V}(P)$ for every associated prime ideal $P \in \mathrm{Ass}(R/I)$. In general a primary decomposition will include *embedded components* not found in an irreducible decomposition, whose corresponding primes strictly contain other associated primes of I.

[1]Here and throughout the paper we say a "generic point on component" to refer to a point in the complement of a proper Zariski closed subset of the component containing the "degeneracy locus" dictated by the context. One can trust numerical methods mentioned so far to produce random points on components that avoid a the degeneracy locus "with probability 1".

A major tool we will use to compute information about the local algebraic structure of ideal I at a point is the *Macaulay dual space*. Given generators of I and a point p in its vanishing set, the dual space of I at p is the vector space dual of the extension of I in the local ring at p, and it uniquely encodes the local properties of I there. Certain combinatorial information about the dual space, such as dimension, can be accurately computed even when p is only known approximately but with high enough precision. Many computations are reduced to linear algebra, allowing numerical linear algebra techniques to be applied.

The idea of studying systems of polynomials through dual spaces dates back to Macaulay [47]. Most of the recent work using Macaulay's machinery concerns zero-dimensional ideals or, geometrically speaking, isolated points. This includes algorithms for computing a basis of the dual space [49, 12] and the local Hilbert function at an isolated point [27], as well as various deflation procedures [43, 45, 31]. Several studies depart from the zero-dimensional setting: the local dimension test [6], computations using dual spaces for homogeneous ideals [30].

In this work dual spaces will be used in several numerical algorithms. First it is used to compute local Hilbert polynomials in the general case, which is work originally published in [41]. We will also give an algorithm for determining ideal membership of a polynomial in an ideal in a local ring. Additionally dual space algorithms will play a key role in the embedded component test algorithms for numerical primary decomposition.

For $\alpha \in (\mathbb{Z}_{\geq 0})^N$ and $y \in \mathbb{C}^N$, define

- $x^\alpha = x_1^{\alpha_1} \cdots x_N^{\alpha_N}$,
- $|\alpha| = \sum_{i=1}^N \alpha_i$,
- $\alpha! = \alpha_1! \alpha_2! \ldots \alpha_N!$,
- $\partial^\alpha = \frac{1}{\alpha!} \frac{\partial^{|\alpha|}}{\partial x^\alpha}$, and

- $\partial^\alpha[y] : R \to \mathbb{C}$ defined by $\partial^\alpha[y](g) = (\partial^\alpha g)(y)$.

The differential functional $\partial^\alpha[y]$ sometimes would be written $\partial^{x^\alpha}[y]$ (e.g. $\partial^1 - \partial^y + \partial^{x^2yz}$) and when the point y is implied $\partial^\alpha[y]$ would be written as ∂^α. For $y \in \mathbb{C}^N$, let $D_y = \operatorname{span}_{\mathbb{C}} \left\{ \partial^\alpha[y] \mid \alpha \in (\mathbb{Z}_{\geq 0})^N \right\}$ be the vector space of differential functionals at y. This linear space is graded by *order*, for a finite sum $q = \sum c_\alpha \partial^\alpha$,

$$\operatorname{ord} q = \max_{c_\alpha \neq 0} |\alpha|.$$

The *homogeneous* part of order i of $q \in D_y$ is referred to as q_i. This grading is the associated graded linear space of the filtration D_y^*:

$$D_y^0 \subset D_y^1 \subset D_y^2 \subset \ldots, \text{ where } D_y^i = \{q \in D_y \mid \operatorname{ord} q \leq i\}\}.$$

Definition 5.1.1. The *Macaulay dual space*, or simply *dual space*, of differential functionals that vanish at y for an ideal $I \subset \mathbb{C}[x] = \mathbb{C}[x_1, \ldots, x_N]$ is

$$D_y[I] = \{q \in D_y \mid q(g) = 0 \text{ for all } g \in I\}. \tag{5.1.1}$$

The dual space $D_y[I]$ is a linear subspace of D_y, a basis of $D_y[I]$ is called a *dual basis* for I.

The following theorem of Macaulay describes the dimension of the dual space at an isolated solution y. The following statement appears in the classical text of Macaulay [47].

Theorem 5.1.2. *A solution $y \in \mathbb{V}(I)$ is isolated with multiplicity m if and only if $\dim_{\mathbb{C}} D_y[I] = m$.*

Definition 5.1.3. A subspace $S \subset D_y$ is *homogeneous* if it is spanned by homogeneous functionals $q \in D_y^{\operatorname{ord} q} \setminus D_y^{\operatorname{ord} q - 1}$. If, in addition, S is spanned by $\partial^\alpha[y],\ \alpha \in A$ for some subset $A \subset (\mathbb{Z}_{\geq 0})^N$, then S is called *monomial*.

5.2 Local ring vs. Dual space

For the purpose of this section, without a loss of generality, we may assume $y = 0 \in \mathbb{C}^N$. Consider the local ring $R_0 = R_{\mathfrak{m}}$ where $\mathfrak{m} = (x_1, \ldots, x_N)$. Let the space of dual functionals be defined as above replacing R (polynomial) with R_0 (rational functions with denominators not vanishing at 0).

Remark 5.2.1. Ideals in R with no primary components away from the origin are in one-to-one correspondence with ideals in the local ring R_0:

- an ideal $I \subset R$ defines the extension $IR_0 \subset R_0$;
- an ideal $I \subset R_0$ corresponds to the ideal $I \cap R \subset R$ with no primary components away from the origin.

Proposition 5.2.2. *For ideal $I \subset R$, the dual space $D_0[I]$ is identical to the dual space of its extension in R_0, $D_0[IR_0]$.*

Proof. Any rational function $g \in R_0$ can be expressed as a power series $g = \sum_\alpha c_\alpha x^\alpha$. If $q \in D_0[I]$, then for any $f \in I$, $q(x^\alpha f) = 0$ for all monomials x^α. Then

$$q(gf) = \sum_{\alpha \in (\mathbb{Z}_{\geq 0})^N} c_\alpha q(x^\alpha f) = 0$$

so $q \in D_0[IR_0]$. For q not in $D_0[I]$ there is some $f \in I$ with $q(f) \neq 0$, and f is also in IR_0. □

As a result we will speak interchangeably about the dual space of an ideal I at the point 0 and the dual space of its extension in the localization of R at 0, IR_0.

The following lemma provides another characterization of the extension of an ideal I in the local ring, which will help describe the close connection between IR_0 and the Macaulay dual space.

Lemma 5.2.3. *For any ideal $I \subset R$,*

$$IR_0 \cap R = \bigcap_{k=1}^{\infty} (I + \mathfrak{m}^k).$$

Proof. Let $\hat{R}$ denote the completion of R with respect to the maximal ideal $\mathfrak{m}$ (the formal power series ring $\hat{R} = \mathbb{C}[[x_1, \ldots, x_N]]$). The kernel of the map of R-modules $R/I \to \widehat{R/I}$ is $\bigcap_k \mathfrak{m}^k(R/I)$, and by the exactness of completion $\widehat{R/I} \cong \hat{R}/I\hat{R}$ (see [5] Chapter 10). Composing the quotient map $R \to R/I$ with the above, we see that $I\hat{R} \cap R$, which is the kernel of natural map $R \to \hat{R}/I\hat{R}$, is $\bigcap_k (I + \mathfrak{m}^k)$.

For any $f \in I\hat{R} \cap R$, there is $h \in I$, $g \in \hat{R}$ such that $f = hg$, so $g = h/f$ is a rational function in R_0. Therefore $f \in IR_0 \cap R$, and so $IR_0 \cap R = I\hat{R} \cap R$. □

Proposition 5.2.4. *For ideal $I \subset R$, $f \in IR_0 \cap R$ if and only if $q(f) = 0$ for all $q \in D_0[I]$.*

Proof. It follows from the definition that $f \in I$ implies $q(f) = 0$ for all $q \in D_0[I]$.

Let R^k be the space of polynomials with degree $\leq k$, let f^k denote the truncation of f to degree k and let $I^k \subset R^k$ be the set $\{f^k : f \in I\}$. Since R^k is a finite dimensional vector space,

$$(I^k)^\perp = D_0^k[I] = D_0[I + \mathfrak{m}^{k+1}].$$

Suppose for some polynomial f that $q(f) = 0$ for all $q \in D_0[I] = \bigcup_k D_0^k[I]$. Because $(I^k)^{\perp\perp} = I^k$, we have $f^k \in I^k$ which implies $f \in I + \mathfrak{m}^{k+1}$. By Lemma 5.2.3, $f \in IR_0 \cap R$. □

Corollary 5.2.5. *For ideals $J_1, J_2 \subset R_0$, $J_1 \subset J_2$ if and only if $D_0[J_1] \supset D_0[J_2]$.*

Proof. It's clear that $J_1 \subset J_2$ implies $D_0[J_1] \supset D_0[J_2]$. Suppose $J_1 \not\subset J_2$, so there is polynomial $f \in J_1$ with $f \notin J_2$. By Proposition 5.2.4 there is $q \in D_0[J_2]$ with $q(f) \neq 0$, so $D_0[J_2] \not\subset D_0[J_1]$. □

An immediate consequence of this corollary is that an ideal $J \subset R_0$ is uniquely determined by its dual space $D_0[J]$.

Corollary 5.2.6. *The dual space $D_0[J]$ is homogeneous (respectively, monomial) iff the ideal $J \subset R_0$ is homogeneous (respectively, monomial), i.e., generated by homogeneous elements with respect to filtration $\{\mathfrak{m}^k\}_{k\geq 0}$ (respectively, by monomials).*

Proof. Given a homogeneous (respectively, monomial) dual space $L = D_0[J]$ of an ideal $J \subset R_0$ it is straightforward to write down homogeneous (respectively, monomial) $I \subset R$ such that $D_0[I] = L$. Namely, its homogeneous part of order k is the set of polynomials orthogonal to L^k/L^{k-1}; for the monomial case, it is particularly explicit: a monomial x^α belongs to I iff $\partial^\alpha \notin L$. The extension IR_0 is determined by L uniquely according to Proposition 5.2.5, hence, $IR_0 = J$. □

Remark 5.2.7. One could easily extend the definition of homogeneous and monomial ideals to the local ring R_y for an arbitrary point $y \in \mathbb{C}^N$: in particular, an ideal is called monomial if it is generated by elements of the form $(x-y)^\alpha$, $\alpha \in (\mathbb{Z}_{\geq 0})^N$.

Macaulay dual bases allow for testing ideal membership at a solution [48] as stated in the following proposition. This can be readily generalized for homogeneous ideals using the following corollary, Remark 5.2.1, and Proposition 5.2.5.

Corollary 5.2.8 (Lemma 11 of [30])**.** *A polynomial $f \in R$ of degree d is a member of a homogeneous ideal $I \subset R$ iff f is annihilated by $D_0^d[I]$.*

Proof. It follows from the proof of Corollary 5.2.6 that $D_0^d[I]$ determines $J = IR/\mathfrak{m}^{d+1}$. Now, $f \in I$ iff its image $\bar{f} \in J$ iff f is annihilated by $D_0^d[I]$. □

The statement of Corollary 5.2.8 corrects that of Theorem 4.6 of [44] where the assumption of homogeneity was missed as shown in [29]. The local membership test without the assumption of homogeneity is a much harder task, addressed in [41].

5.3 Action of differentiation on the dual space

An alternative characterization of the dual space can be given via Proposition 5.3.2. There is a natural action of R_0 on D_0 by pre-multiplication. Specifically for $q \in D_0$

and $g \in R_0$ let $g \cdot q \in D_0$ denote the functional defined by $(g \cdot q)(f) = q(gf)$. It can be checked that this gives D_0 an R_0-module structure. The action of each variable x_i can also be considered as *differentiating* functionals in D_0 by ∂_i (up to normalization). Let $\sigma_{x_i} : D_0 \to D_0$ denote the map defined by the action of x_i.

$$\begin{aligned} \sigma_{x_i} : D_0 &\to D_0 \\ \partial^\alpha &\mapsto \partial^{\alpha - e_i}, \quad (i = 1, \ldots, N), \end{aligned}$$

where ∂^β is taken to be 0 when any entry of β is less than zero.

The following statements (from Proposition 5.3.1 to Corollary 5.3.5) appear, perhaps in alternative phrasing, in many works addressing the duality at hand (see, for example, [49]). We collect the essential pieces, stated in our language, and complete with our own short proofs to guide reader's intuition for this paper.

Proposition 5.3.1. *For a subspace $L \subset D_0$ the following are equivalent:*

- *L is the dual space of some ideal $J_L \subset R_0$.*
- *L is closed under differentiation by each variable: $x_i \cdot L \subset L$ for all $1 \leq i \leq N$.*
- *L is an R_0-submodule of D_0.*

Proof. For any $L \subset D_0$ define

$$J_L = \{f \in R_0 : q(f) = 0 \text{ for all } q \in L\}.$$

If L is closed under differentiation, then J_L is closed under multiplication by each x_i, and therefore under multiplication by all monomials in R_0. Express any $g \in R_0$ as $g = \sum_\alpha c_\alpha x^\alpha$. Then if $f \in J_L$ and $q \in L$, $q(gf) = \sum_\alpha c_\alpha q(x^\alpha f)$ and each term is zero, so $gf \in J_L$. Therefore J_L is an ideal and $D_0[J_L] = L$. Conversely if $L = D_0[J_L]$ and $q \in L$ then $(x_i \cdot q)(f) = q(x_i f) = 0$ for all $f \in J_L$ so $x_i \cdot q \in L$. □

Consider the map

$$\text{Dual} : \{\text{ideals of } R_0\} \to \{R_0\text{-submodules of } D_0\}$$

defined by $\text{Dual}(J) = D_0[J]$. By Corollary 5.2.5 and Proposition 5.3.1, this map is a bijection. This provides another way to characterize the dual space.

Proposition 5.3.2. *For ideal $J = \langle f_1, \ldots, f_n \rangle \subset R_0$, let L be the maximal R_0-submodule of D_0 that satisfies $q(f_i) = 0$ for all $q \in L$ and all $0 \leq i \leq n$. Then $L = D_0[J]$.*

Proof. $D_0[J]$ is closed under differentiation and satisfies $q(f_i) = 0$ for all $q \in D_0[J]$ and $0 \leq i \leq n$, so $D_0[J] \subseteq L$. The ideal J_L contains $\{f_1, \ldots, f_n\}$, so $J \subseteq J_L$ which implies $L \subseteq D_0[J]$. □

Remark 5.3.3. For an ideal $J \subset R_0$, the dual space $D_0[J]$ is finitely-generated as an R_0-module only when it is a finite dimensional vector space. If $D_0[J]$ is generated by a single functional p, then J is exactly the *apolar ideal* of p (see, for instance, [36] for the definition).

A result of Proposition 5.3.2 is that for $I = \langle f_1, \ldots, f_n \rangle$, a dual element q is in $D_0[I]$ if and only if $q(f_i) = 0$ and $x_j \cdot q \in D_0[J]$ for each $0 \leq i \leq n$ and $0 \leq j \leq N$. Note that this leads to a completion scheme for computing $D_y^k[I]$ proposed in [49], assuming y is in the vanishing set of I:

$D_y^0[I] \leftarrow \text{span}_{\mathbb{C}}(\partial^0)$

for $i = 1 \to k$ **do**

$D_y^i[I] \leftarrow \{q \in D_y \mid x_j \cdot q \in D_y^{i-1}[I]$ for all $j = 1, \ldots, N$ and $q(f_i) = 0$ for all $i = 1, \ldots, n\}$

end for

Moreover, the above algorithm makes apparent that if $D_y^i[I] = D_y^{i+1}[I]$ for some $i \geq 0$ then $D_y^i[I]$ is equal to all higher truncations, and so is equal to $D_y[I]$. This gives an effective stopping criterion for computing $D_y[I]$ when it is finite dimensional.

Proposition 5.3.4. *For ideals $J_1, J_2 \subset R_0$,*

- $D_0[J_1 + J_2] = D_0[J_1] \cap D_0[J_2]$.
- $D_0[J_1 \cap J_2] = D_0[J_1] + D_0[J_2]$.

Proof. The first statement follows from the definition of the dual space, as does $D_0[J_1] + D_0[J_2] \subset D_0[J_1 \cap J_2]$.

Let $L = D_0[J_1] + D_0[J_2]$. It's clear that L is an R_0-submodule, so it is the dual space of an ideal J_L. The fact that $D_0[J_1] \subset L$ implies $J_L \subset J_1$ and similarly $J_L \subset J_2$. Therefore $D_0[J_1 \cap J_2] \subset L$. □

Corollary 5.3.5. *If J_1 and J_2 are homogeneous ideals of R_0, then the equality holds for the truncated dual spaces:*

$$D_0^d[J_1 \cap J_2] = D_0^d[J_1] + D_0^d[J_2], \text{ for all } d \in \mathbb{N}_0.$$

Proof. This follows from the fact that if $q \in D_0[J]$ for a homogeneous J, then q_d, the part of q of order d, is also in $D_0[J]$. □

Remark 5.3.6. For truncated dual space, in general, only one inclusion holds:

$$D_0^k[J_1 \cap J_2] \supset D_0^k[J_1] + D_0^k[J_2].$$

However, because $D_0^k[J_1 \cap J_2]$ is finite dimensional, it follows that

$$D_0^k[J_1 \cap J_2] \subset D_0^l[J_1] + D_0^l[J_2]$$

for l large enough.

Example 5.3.7. Let $I_1 = \langle x_1 \rangle$ and $I_2 = \langle x_1 - x_2^2 \rangle$ in $R = \mathbb{C}[x_1, x_2]$. Then

$$D_0^1[I_1] + D_0^1[I_2] = \text{span}\{1, \partial_2\},$$

$$D_0^1[I_1 \cap I_2] = \text{span}\{1, \partial_1, \partial_2\},$$

$$D_0^2[I_1] + D_0^2[I_2] = \mathrm{span}\{1, \partial_2, \partial_2^2, \partial_2^2 + \partial_1\}.$$

There are strict inclusions

$$D_0^1[I_1] + D_0^1[I_2] \subsetneq D_0^1[I_1 \cap I_2] \subsetneq D_0^2[I_1] + D_0^2[I_2].$$

CHAPTER VI

DUAL SPACE ALGORITHMS

In this chapter, the tools relating to the Macaulay dual space from Chapter 5 are used to produce algorithms for computing local properties of an ideal I at a point p. In particular we give algorithms for the local Hilbert polynomial and Hilbert regularity of I at p and for testing local membership of a polynomial in I. We also introduce the notion of "eliminating dual spaces," which can be used to compute dual spaces of quotient ideals in some situations.

These algorithms take as input a generating set of the ideal I and a point p, and are *consistent with respect to numerical error* of p. This means that they will give the correct output even if the value of p is not given exactly, but instead a numerical approximation of p with sufficiently high precision. This makes these algorithms compatible with other tools from numerical algebraic geometry.

The algorithms developed in this chapter will in turn be used toward solving problems in numerical primary decomposition in Chapter 7.

6.1 Numerical Hilbert function

6.1.1 Primal and dual monomial order

Let $\geq$ be a local monomial order (1 is the largest monomial), which we shall refer to as a *primal order*. For $g = \sum_\alpha a_\alpha x^\alpha$, a nonzero polynomial, the *initial term* with respect to $\geq$ is the largest monomial with respect to $\geq$ that has a nonzero coefficient, namely

$$\text{in}_{\geq}(g) = \max_{\geq}\{x^\alpha \mid a_\alpha \neq 0\}.$$

For an ideal I, the *initial terms* of I with respect to $\geq$ is the set of initial terms with respect to $\geq$ of all the elements of I, namely

$$\mathrm{in}_{\geq}(I) = \{\mathrm{in}_{\geq}(f) \mid f \in I\}.$$

A monomial is called a *standard monomial* of I with respect to $\geq$ if it is not a member of $\mathrm{in}_{\geq}(I)$.

We shall order the monomial differential functionals via the *dual order*:

$$\partial^{\alpha} \succeq \partial^{\beta} \;\Leftrightarrow\; x^{\alpha} \leq x^{\beta},$$

the order opposite to $\geq$.

The *initial term* $\mathrm{in}_{\succeq}(q)$ of q is the largest monomial differential functional that has a nonzero coefficient. The *initial support* of a dual space with respect to $\succeq$ is the set of initial terms with respect to $\succeq$ of all the elements in the dual space (which can be considered as a subset of $(\mathbb{Z}_{\geq 0})^N$).

A dual basis that has distinct initial terms is called a *reduced dual basis*. Using a (possibly infinite dimensional) Gaussian elimination procedure, it is easy to see that any dual basis can be transformed into a reduced dual basis.

Theorem 6.1.1 (Theorem 3.1 of [45])**.** *Let I_0 be a 0-dimensional ideal of R_0. The initial support of the dual space $D_0[I_0]$ is the set of standard monomials for $I = I_0 \cap R$, i.e.,*

$$\mathrm{in}_{\succeq}(D_0[I_0]) = \mathrm{in}_{\succeq}(D_0[I]) = \{\partial^{\alpha} \mid x^{\alpha} \notin \mathrm{in}_{\geq}(I)\}. \tag{6.1.1}$$

Proof. Note that $D_0[I]$ is finite dimensional. Choose a monic reduced basis B for $D_0[I]$ such that the lead term of each element does not occur in any other element (using Gaussian elimination).

Suppose $\partial^{\alpha} \in \mathrm{in}_{\succeq}(D_0[I])$ so some $p \in B$ has $\mathrm{in}_{\succeq}(p) = \partial^{\alpha}$. For any monic polynomial f with $\mathrm{in}_{\geq}(f) = x^{\alpha}$, f and p have no terms with the same exponent except their respective lead terms, so $p(f) = 1$ and $f \notin I$.

Suppose $\partial^\alpha \notin \mathrm{in}_\geq(D_0[I])$. Let $\{p_1, \ldots, p_s\} \subset B$ be the basis elements with ∂^α in their monomial support. For each p_i let c_i be the coefficient of ∂^α and let $\partial^{\beta_i} = \mathrm{in}_\geq(p_i)$. The following polynomial

$$f = x^\alpha + \sum_{i=1}^{s} \frac{x^{\beta_i}}{c_i}$$

has $p(f) = 0$ for all $p \in B$, and $\mathrm{in}_\geq(f) = x^\alpha$. By Proposition 5.2.4, $f \in I_0$ so $x^\alpha \in \mathrm{in}_\geq(I_0) = \mathrm{in}_\geq(I)$. □

Corollary 6.1.2. *For an ideal $I \subset R_0$, $\dim_{\mathbb{C}} \left(R_0/(I + \mathfrak{m}^{k+1})\right) = \dim_{\mathbb{C}} D_0^k[I]$ where $\mathfrak{m} = \langle x_1, \ldots, x_N \rangle$.*

Proof. Choosing a graded primal order $\geq$, a vector space basis for the quotient $R_0/(I + \mathfrak{m}^{k+1})$ is the set of monomials

$$\{x^\alpha \mid x^\alpha \notin \mathrm{in}_\geq(I), \text{ and } |\alpha| \leq k\}.$$

By Theorem 6.1.1 this is corresponds to a basis for $\mathrm{in}_\geq(D_0^k[I])$ which has the same dimension as $D_0^k[I]$. □

We can extend Theorem 6.1.1 to ideals of arbitrary dimensions.

Theorem 6.1.3. *For an ideal $I \subset R$ the monomial lattice $\mathbb{N}_0^N$ is a disjoint union of $\mathrm{in}_\geq D_0[I]$ and $\mathrm{in}_\geq I$.*

Proof. By Theorem 6.1.1, $\mathbb{N}_0^N \setminus \mathrm{in}_\geq D_0[I + \mathfrak{m}^{k+1}] = \mathrm{in}_\geq(I + \mathfrak{m}^{k+1})$, so then

$$\mathbb{N}_0^N \setminus \bigcup_k \mathrm{in}_\geq D_0[I + \mathfrak{m}^{k+1}] = \bigcap_k \mathrm{in}_\geq(I + \mathfrak{m}^{k+1}).$$

By definition $\bigcup_k \mathrm{in}_\geq D_0[I + \mathfrak{m}^{k+1}] = \mathrm{in}_\geq D_0[I]$, while by Lemma 5.2.3

$$\bigcap_k \mathrm{in}_\geq(I + \mathfrak{m}^{k+1}) = \mathrm{in}_\geq(IR_0 \cap R) = \mathrm{in}_\geq(I)\,.$$

□

6.1.2 Hilbert function and regularity index

The Hilbert function of an ideal $I \subset R_0$ provides combinatorial information about I that can be computed numerically using truncated dual spaces.

Definition 6.1.4. For an ideal $I \subset R_0$ define the *Hilbert function* as

$$H_I(k) = \dim_{\mathbb{C}}(\mathfrak{gr}(R_0/I)_k) = \dim_{\mathbb{C}}\left(\frac{I+\mathfrak{m}^k}{I+\mathfrak{m}^{k+1}}\right)$$

$$= \dim_{\mathbb{C}}\left(R_0/(I+\mathfrak{m}^{k+1})\right) - \dim_{\mathbb{C}}\left(R_0/(I+\mathfrak{m}^k)\right)$$

This is the same as $HS_{R_0/I,\mathfrak{m}}$, the Hilbert-Samuel function of the R_0-module R_0/I where R_0 is filtered by $\{\mathfrak{m}^k\}$.

The Hilbert function is determined by the initial ideal with respect to the primal monomial order (that respects the degree).

Proposition 6.1.5. *For an ideal $I \subset R_0$*

$$H_I(k) = H_{I,0}(k) = H_{\mathrm{in}_{\geq}(I\cap R)}(k), \text{ for all } k \in \mathbb{N}_0.$$

Alternatively, truncated dual spaces determine the Hilbert function. By Corollary 6.1.2 it can be seen that

$$H_I(k) = \dim_{\mathbb{C}} D_0^k[I] - \dim_{\mathbb{C}} D_0^{k-1}[I], \text{ for } k \geq 0,$$

where $\dim_{\mathbb{C}} D_0^{-1}[I]$ is taken to be 0.

For some $m \geq 0$ the Hilbert function is a polynomial in k for all $k \geq m$ (see, e.g., [26, Lemma 5.5.1]), the *Hilbert polynomial* $\mathrm{HP}_I(k)$. If the dimension of $I \subset R_0$ is d, then $\mathrm{HP}_I(k)$ is a polynomial of degree $d-1$. In particular if I is 0-dimensional then $\mathrm{HP}_I(k) = 0$ since R_0/I is finite dimensional.

Definition 6.1.6. The *regularity index* of the Hilbert function is

$$\rho_0(I) = \min\{\, m \,:\, H_I(k) = \mathrm{HP}_I(k) \text{ for all } k \geq m \,\}.$$

The regularity index of an ideal is used as a stopping criterion for many algorithms which work iteratively by degree. In particular we will make use of it in Algorithm 7.2.1.

The Hilbert polynomial is closely tied to the notion of multiplicity.

Definition 6.1.7. For a 0-dimensional ideal I, the *multiplicity* $\mu(I)$ is defined as $\dim_{\mathbb{C}}(R_0/I)$. For I of dimension $d > 0$ with Hilbert polynomial $\mathrm{HP}_I(k) = a_{d-1}k^{d-1} + \cdots + a_0$ the multiplicity is defined as

$$\mu(I) = a_{d-1}(d-1)!.$$

The multiplicity of I can be interpreted geometrically as follows. For $I \subset R_0$ with dimension d, let $L \subset R$ be a system of affine hyperplanes with codimension d. If L is chosen generically, then $J = (I \cap R) + L$ is a 0-dimensional ideal and the points of $\mathbb{V}(J)$ are smooth points of $\mathbb{V}(I \cap R)$. The multiplicity $\mu(I)$ is equal to $\dim_{\mathbb{C}}(R/J)$. It follows that if $Q_1, \ldots, Q_s$ are the primary components of I that have maximal dimension, then $\mu(I) = \sum_{i=1}^{s} \mu(Q_i)$. For detailed discussion of multiplicity see [26, Sec 5.5].

Definition 6.1.8. The *regularity index* of the Hilbert function is

$$\rho_0(I) = \min\{\, m \,:\, H_I(k) = \mathrm{HP}_I(k) \text{ for all } k \geq m \,\}.$$

Let us refer to the minimal monomial generators of a monomial ideal M as g-corners. We call a monomial x^α an *s-corner* of M when $x_i x^\alpha \in M$ for all $i = 1, \ldots, n$. For a general ideal I, the g-corners and s-corners of I will refer to the g-corners and s-corners of the monomial ideal $\mathrm{in}_{\geq} I$, respectively.[1]

The Hilbert function of I can be computed in terms of the set C of g-corners of

[1] **g-** and **s-** stand for **generators** of $\mathrm{in}_{\geq} I$ and monomials spanning the **socle** of the quotient $R_0/\mathrm{in}_{\geq} I$, respectively.

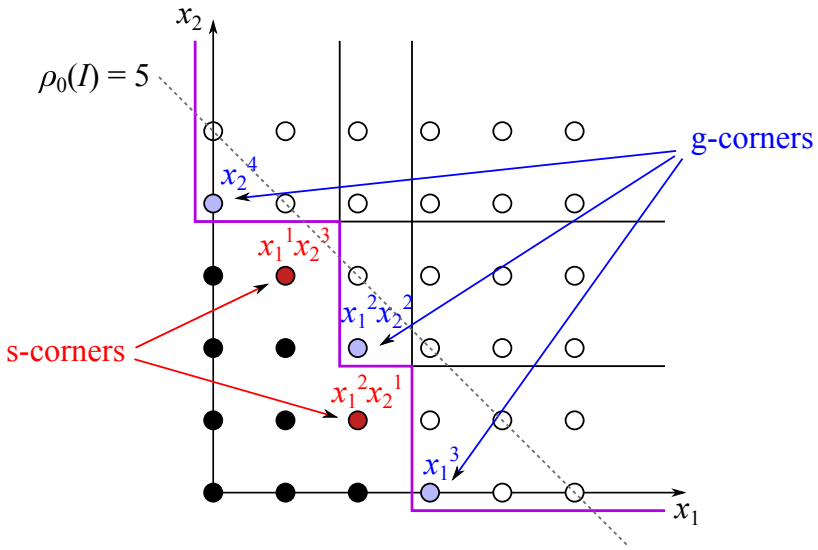

Figure 3: The "staircase" of monomial ideal $I = \langle x_1^3, x_1^2 x_2^2, x_2^4 \rangle$ in the lattice of monomials. The regularity index of the Hilbert function is $\rho_0(I) = 5$.

$\text{in}_{\geq}(I)$. The following formula is derived from a simple counting argument

$$H_I(k) = \sum_{S \subseteq C} (-1)^{|S|} \binom{k - \deg \operatorname{lcm}(S) + N - 1}{N - 1} \tag{6.1.2}$$

where $\binom{k-\deg \operatorname{lcm}(S)+N-1}{N-1}$ is taken to be 0 for all $k < \deg \operatorname{lcm}(S)$. For $k - \deg \operatorname{lcm}(S) + N - 1 \geq 0$ this binomial coefficient is a polynomial in k of degree $N-1$. The formula provides a way to explicitly produce the Hilbert polynomial from the set of g-corners. It also provides a bound on the regularity index,

$$\rho_0(I) \leq \deg \operatorname{lcm}(C) - N + 1.$$

Remark 6.1.9. For a 0-dimensional ideal I, The Hilbert regularity index

$$\rho_0(I) = \max\{|\alpha| \, : \, x^\alpha \text{ is an s-corner of } \text{in}_{\geq} I\} + 1.$$

6.1.3 Computing the Hilbert polynomial of an ideal

We will compute the Hilbert polynomial of an ideal I by computing the set of g-corners, which in turn will be done by computing truncated dual spaces. The algorithm given here that accomplishes this was originally published in [38]. Theorem

6.1.3 shows that $\text{in}_{\geq} D_0^k[I]$ determines the monomials of $\text{in}_{\geq} I$ of degree $\leq k$. If monomial $m \in \text{in}_{\geq} I$ is not divisible by any lower degree monomials in $\text{in}_{\geq} I$, then m is a g-corner of I. This gives a procedure to find g-corners degree by degree. We need only a stopping criterion for when all g-corners have been found.

When I is homogeneous, the following proposition suggests such a stopping criterion.

Proposition 6.1.10. *Let I be a homogeneous ideal given by homogeneous generating set F, let G be a homogeneous minimal standard basis for I, and let $G^k = \{g \in G : \deg g \leq k\}$. For any $k \geq \max_{f \in F}(\deg f)$, one of the following must be true:*

- $G^k = G$,
- *or there is $f \in G \setminus G^k$ with*

$$\deg f \leq \max_{g,h \in G^k} (\deg \text{lcm}\{\text{in}_{\geq} g, \text{in}_{\geq} h\}) \leq 2k.$$

Proof. This statement follows from Buchberger's criterion for a standard basis. Since k is chosen larger than the degrees of the generators, G^k generates J. If G^k is not a standard basis, then there must be some $g, h \in G^k$ with S-polynomial $S(g,h)$ that does not reduce to 0. Since g and h are homogeneous, $\deg S(g,h) = \deg \text{lcm}\{\text{in}_{\geq} g, \text{in}_{\geq} h\}$, and the normal form of $S(g,h)$ has the same degree. □

Note that the assumption of homogeneity of I is necessary. With a local order, an S-polynomial may in general have higher degree than the LCM of the lead terms of it's constituent polynomials.

For the non-homogeneous case let $F \subset R$ be a finite set of generators of I and let $F^h \subset R[h]$ denote the homogenization of F. The above ideas will be applied to the homogeneous ideal $\langle F^h \rangle$ to find its g-corners. Note that $\langle F^h \rangle \subseteq I^h$ but in general equality does not hold. However for any $g \in I$, there is $h^k g^h \in \langle F^h \rangle$ for some

sufficiently large k. Letting $\varphi : R[h] \to R$ denote the dehomogenization map sending h to 1, then $\varphi(\langle F^h \rangle) = \langle F \rangle$.

We equip $R[h]$ with the unique graded local order $\geq$ such that for monomials $a, b \in R[h]$ with the same total degree, $a \geq b$ if and only if $\varphi(a) \geq \varphi(b)$. This monomial order ensures the following relation between g-corners of $\langle F^h \rangle$ and of $\langle F \rangle$.

Proposition 6.1.11. *If C is a set of monomial generators of $\mathrm{in}_{\geq}\langle F^h \rangle$ then $\varphi(C)$ generates $\mathrm{in}_{\geq}\langle F \rangle$.*

Proof. It is sufficient to prove that $\varphi(\mathrm{in}_{\geq}\langle F^h \rangle) = \mathrm{in}_{\geq}\langle F \rangle$. The monomial order on $R[h]$ is chosen so that for any homogeneous polynomial $f \in R[h]$,

$$\mathrm{in}_{\geq} \varphi(f) = \varphi(\mathrm{in}_{\geq} f).$$

For any $g \in \langle F \rangle$, there is $t^k g^h \in \langle F^h \rangle$ for some k and $\varphi(\mathrm{in}_{\geq} t^k g^h) = \mathrm{in}_{\geq} g$. Therefore $\varphi(\mathrm{in}_{\geq}\langle F^h \rangle) \supseteq \mathrm{in}_{\geq}\langle F \rangle$.

For any polynomial $f \in \langle F^h \rangle$, the graded pieces of f are also in $\langle F^h \rangle$ because it is a homogeneous ideal. Let $\hat{f}$ be the non-zero graded piece of f of smallest degree so $\mathrm{in}_{\geq} \hat{f} = \mathrm{in}_{\geq} f$. Since $\hat{f}$ is homogeneous,

$$\varphi(\mathrm{in}_{\geq} f) = \varphi(\mathrm{in}_{\geq} \hat{f}) = \mathrm{in}_{\geq} \varphi(\hat{f})$$

and $\varphi(\hat{f}) \in \langle F \rangle$. Therefore $\varphi(\mathrm{in}_{\geq}\langle F^h \rangle) \subseteq \mathrm{in}_{\geq}\langle F \rangle$. □

By calculating a reduced dual basis of $D_0^k[\langle F^h \rangle]$ for a given k, we find the monomials not represented in $\mathrm{in}_{\geq} D_0^k[\langle F^h \rangle]$, which by Theorem 6.1.1 correspond to the monomials of $\mathrm{in}_{\geq}\langle F^h \rangle$ of degree $\leq k$, and from these deduce the g-corners of $\langle F^h \rangle$ of degree $\leq k$. Each time we find a new g-corner of $\langle F^h \rangle$, we revise our bound on what degree to stop at according to Proposition 6.1.10. If we ever reach the bound without finding any new g-corners then all g-corners are guaranteed to be found and the algorithm stops. If C is the set of g-corners of $\langle F^h \rangle$ then $\varphi(C)$ generates $\mathrm{in}_{\geq} I$. Throwing out non-minimal elements of $\varphi(C)$ produces the g-corners of I.

Algorithm 6.1.12. $C = \text{gCorners}(F)$

Require: $F = \{f_1, \ldots, f_s\} \subset R$.

Ensure: C is the set of g-corners of $\langle F \rangle$.

$k \leftarrow 0$

$k_{max} \leftarrow 2 \max_i \{\deg f_i^h\}$

while $k \leq k_{max}$ **do**

$B \leftarrow$ reduced basis of $D_0^k[\langle F^h \rangle]$

$C_k \leftarrow$ minimal monomials of $\{x^\alpha \mid |\alpha| \leq k,\ \partial^\alpha \notin \text{in}_\geq B\}$

if $C_k \neq C_{k-1}$ and $k_{max} < 2k$ **then**

$k_{max} \leftarrow 2k$

end if

$k \leftarrow k + 1$;

end while

$C \leftarrow$ minimal monomials of $\varphi(C_{k-1})$

6.2 Testing ideal membership with quotient ideals

6.2.1 Dual spaces of quotient ideals

Recall that for $g \in R_0$, the map $\sigma_g : D_0 \to D_0$ denotes the action of g on D_0 by pre-multiplication, or equivalently by "differentiation" with respect to g.

Proposition 6.2.1. *For all non-zero $g \in R_0$, the map $\sigma_g : D_0 \to D_0$ is surjective and* $\ker \sigma_g = D_0[\langle g \rangle]$.

Proof. Note $g \cdot D_0$ is closed under differentiation. If σ_g is not surjective, then $g \cdot D_0$ is the dual space of some non-trivial ideal $I \subset R_0$ by Proposition 5.3.1. Choose some non-zero $f \in I$. Since $gf \neq 0$, there exists some functional q with $q(gf) \neq 0$. Then $g \cdot q(f) = q(gf) \neq 0$, which is a contradiction since $g \cdot q$ should annihilate f. To show $\ker \sigma_g = D_0[\langle g \rangle]$, if $q \in D_0[\langle g \rangle]$ then $g \cdot q(f) = q(gf) = 0$ for all $f \in R_0$. The

only functional that is zero on all elements of R_0 is the zero functional so $g \cdot q = 0$. Conversely if $q \notin D_0[\langle g \rangle]$ then $g \cdot q(f) = q(gf) \neq 0$ for some $f \in R$, so $g \cdot q \neq 0$. □

Theorem 6.2.2. $D_0[I : \langle g \rangle] = g \cdot D_0[I]$.

Proof. For I homogeneous, the statement is shown in [30, Theorem 22]. Here we consider the general case.

If $p \in D_0[I]$, then $g \cdot p(f) = p(gf) = 0$ for all f such that $gf \in I$. These are precisely the polynomials f in $I : \langle g \rangle$, and so $g \cdot p \in D_0[I : \langle g \rangle]$.

For any $q \in D_0[I : \langle g \rangle]$, because σ_g is surjective we can choose some $p \in D_0$ such that $g \cdot p = q$. Then for all $f \in I : \langle g \rangle$, we have $q(f) = p(gf) = 0$, so

$$p \in D_0[g(I : \langle g \rangle)] = D_0[I \cap \langle g \rangle] = D_0[I] + D_0[\langle g \rangle].$$

Therefore $p = p' + u$ for some $p' \in D_0[I]$ and $u \in D_0[\langle g \rangle]$. Then $q = g \cdot p = g \cdot p' + g \cdot u$ but $g \cdot u = 0$ so $q \in g \cdot D_0[I]$. □

6.2.2 Ideal membership test

Let $>$ be a primal order on the monomials of the local ring R_0, and $\succ$ be the dual order for the dual monomials of D_0. For any $p \in D_0$, we must have $\deg \mathrm{in}_{\succeq}(x_1 \cdot p) \leq \deg \mathrm{in}_{\succeq}(p) - 1$, since differentiation reduces the degree of each monomial by 1, but may also annihilate the lead term. Therefore taking the derivative of the dual space truncated at degree $d+1$ we have $x_1 \cdot D_0^{d+1}[I] \subset D_0^d[I : \langle x_1 \rangle]$. Equality may not hold since there may be some functionals $q \in D_0^d[I : \langle x_1 \rangle]$ with $q = x_1 \cdot p$ for some $p \in D_0[I]$ with lead term having degree higher than $d+1$ and is annihilated by x_1. In general, finding $D_0^d[I : \langle x_1 \rangle]$ from the truncated dual space of I may require calculating $D_0^c[I]$ up to a very high degree c.

Some of these issues can be side-stepped through homogenization. As in Section 6.1.3, for $f \in R$, let $f^h \in R[h]$ denote the homogenization of f. Let $\varphi : R[h] \to R$ be the dehomogenization map, which sends h to 1.

Proposition 6.2.3. $\varphi(\langle F^h\rangle : \langle g^h\rangle) = I : \langle g\rangle$.

Proof. Suppose $j \in \langle F^h\rangle : \langle g^h\rangle$, so $jg^h \in \langle F^h\rangle$. Then by dehomogenizing, $\varphi(j)g \in \langle F\rangle$ so $\varphi(j) \in I : \langle g\rangle$.

Suppose $j \in I : \langle g\rangle$. Then $jg = \sum_{f\in F} a_f f$ for some $a_f \in R$. Homogenizing, $h^c j^h g^h = \sum_{f\in F} h^{c_f} a_f^h f^h$ for some non-negative integers c and c_f. Therefore $h^c j^h \in \langle F^h\rangle : \langle g^h\rangle$ and $\varphi(h^c j^h) = j$. □

Since $\langle F^h\rangle$ and g^h are both homogeneous,

$$g^h \cdot (D_0^d[\langle F^h\rangle]) = D_0^{d-e}[\langle F^h\rangle : \langle g^h\rangle]$$

where e is the degree of g^h.

We will make use of this for an ideal membership test using the homogenized dual space. Let I be an ideal of the local ring R_0. If g is not in I then at some degree the Hilbert functions of I and $I+\langle g\rangle$ will differ. We can compute the values of the Hilbert function for successive degrees using the dual space. If g is in I then $I : \langle g\rangle = R_0$. This can be checked by computing $D_0^d[\langle F^h\rangle : \langle g^h\rangle]$ for some d and seeing that h^d is in its initial ideal. This implies that there is some $f \in \langle F^h\rangle : \langle g^h\rangle$ with $\varphi(\text{in}_{\geq} f) = 1$. Running both tests simultaneously for successive degrees d guarantees termination.

Algorithm 6.2.4. $B = \text{IdealMembership}(F, g)$

Require: $I = \langle F\rangle$, an ideal of R;

g, a polynomial in R.

Ensure: $B = (g \in IR_0)$, a Boolean value.

$e \leftarrow \deg g^h$;

$d \leftarrow 0$;

loop

$D_1 \leftarrow D_0^d[I]$;

$D_2 \leftarrow D_0^d[I + \langle g\rangle]$;

if $D_1 \neq D_2$ **then**

return $false$;

end if

$C \leftarrow g^h \cdot D_0^{d+e}[\langle F^h \rangle]$;

if $h^d \in \text{in}_{\succeq} C$ **then**

return $true$;

end if

$d \leftarrow d + 1$;

end loop

Algorithm 6.2.4 fills in the gap left by the local membership test proposed in Theorem 4.6 of [44], which missed the necessary assumption of homogeneity.

6.3 Eliminating dual spaces

Section 6.2.1 described the relationship between the dual space of an ideal $D_0[I]$, and the dual space of the quotient ideal by a principal ideal $D_0[I : \langle g \rangle]$. For applications (such as in Section 7.2) it is useful to compute information even about the simplest case, where $g = x_1$. We would like to find bases for the truncated dual spaces $D_0^d[I : \langle x_1 \rangle]$ but this proves difficult.

Let $>$ be a graded primal order on the monomials of the local ring R_0, and $\succ$ be the dual order for the dual monomials of D_0. For any $p \in D_0$, we must have $\text{ord}\,\text{in}_{\succeq}(x_1 \cdot p) \leq \text{ord}\,\text{in}_{\succeq}(p) - 1$, since differentiation reduces the degree of each monomial by 1, but may also annihilate the lead term. Therefore taking the derivative of the dual space truncated at degree $d+1$ we have $x_1 \cdot D_0^{d+1}[I] \subset D_0^d[I : \langle x_1 \rangle]$. Equality may not hold since there may be some functionals $q \in D_0^d[I : \langle x_1 \rangle]$ with $q = x_1 \cdot p$ for some $p \in D_0[I]$ with lead term having degree higher than $d + 1$ and is annihilated by x_1. In general, finding $D_0^d[I : \langle x_1 \rangle]$ from the truncated dual space of I may require calculating $D_0^c[I]$ up to a high degree c.

To overcome the difficulty of computing truncated dual spaces of colon ideals, we consider other filtrations of D_0 corresponding to gradings on R_0 other than the total degree grading. For $A \subset \{x_1, \ldots, x_n\}$ define $\operatorname{ord}_A \partial^\alpha = \sum_{x_i \in A} \alpha_i$, the total order of all ∂_i with $x_i \in A$. For general $q \in D_0$ define $\operatorname{ord}_A q$ to be the maximum order of the terms of q.

Definition 6.3.1. Fixing $A \subset \{x_1, \ldots, x_N\}$, the *eliminating truncated dual spaces* of I are

$$E_0^d[I, A] = \{q \in D_0[I] : \operatorname{ord}_A q \leq d\}$$

for all $d \in \mathbb{N}_0$.

We often drop the word *truncated* when talking about eliminating dual spaces.

The truncated dual spaces $D_0^d[I]$ give a filtration of $D_0[I]$ corresponding to the maximal ideal $\mathfrak{m}$ of R_0

$$D_0^d[I] = D_0[I + \mathfrak{m}^{d+1}].$$

Similarly, the eliminating truncated dual spaces for A correspond to the ideal $\langle A \rangle$ in that

$$E_0^d[I, A] = D_0[I + \langle A \rangle^{d+1}].$$

To see this, note that $E_0^d[I, A]$ is the intersection of $D_0[I]$ with $E_0^d[0, A] = D_0[\langle A \rangle^{d+1}]$. By Propositon 5.3.4, the intersection of these two dual spaces is $D_0[I + \langle A \rangle^{d+1}]$.

For which ever grading of R_0 (and corresponding filtration of D_0) is chosen, it is useful to pick a local order $\geq$ (and corresponding dual order $\succeq$) that is compatible with the grading. An order is compatible if for $x^\alpha \in (R_0)_i$ and $x^\beta \in (R_0)_j$ with $i < j$ then $x^\alpha > x^\beta$. In the case of the total degree grading, such an order is a graded order. For the grading given by $\langle A \rangle$ a compatible local order is an *elimination order*, eliminating the variables in A. In particular this is a block order in which the most significant block is a degree order on the variables in A and the second block is an

arbitrary order on the variables not in A. Such an order ensures that $p \in E_0^d[0, A]$ if and only if $\mathrm{in}_{\succeq} p \in E_0^d[0, A]$.

Remark 6.3.2. Dual spaces offer analogs to many operations in elimination theory. The dual space of $I \cap \mathbb{C}[x_{m+1}, \ldots, x_N]$ is equal to $D_0[I]|_{\partial_1=0,\ldots,\partial_m=0}$. The eliminating dual $E_0^0[I, A]$ is the dual space of $I + \langle A \rangle$, the variety of which is the intersection of $\mathbb{V}(I)$ with the coordinate subspace in which the variables in A are zero. For a more detailed discussion in the case if homogeneous ideals see [30].

Let $\geq$ be an local elimination order for $x_1, \ldots, x_m$ with dual order $\succeq$ and consider ring extension $R' := \mathbb{C}(x_{m+1}, \ldots, x_N)[x_1, \ldots, x_m] \supset R$. In this extension with $\succeq'$ the corresponding dual order, the monomials in $\mathrm{in}_{\succeq'} D_0[IR']$ are the monomials of $\mathrm{in}_{\succeq} D_0[I]$ considering only the $x_1, \ldots, x_m$ parts. These can be computed from $\mathrm{in}_{\succeq} E_0^d[I, \{x_1, \ldots, x_m\}]$ for sufficiently large d.

Note that the eliminating dual space generalizes the usual truncated dual space since $E_0^d[I, \{x_1, \ldots, x_N\}] = D_0^d[I]$. For general A, we have $E_0^d[I, A] \supset D_0^d[I]$. Unlike $D_0^d[I]$, the eliminating truncated dual space can be infinite-dimensional.

Proposition 6.3.3. *If I is an m-dimensional ideal that is in general position with respect to $x_1, \ldots, x_m$ then* $\dim_{\mathbb{C}} E_0^d[I, \{x_1, \ldots, x_m\}] < \infty$.

Proof. For I satisfying these hypotheses the intersection of $\mathbb{V}(I)$ with the space $\mathbb{V}(x_1, \ldots, x_m)$ is 0-dimensional. By Theorem 5.1.2, $I + \langle x_1, \ldots, x_m \rangle^{d+1}$ has dual space of finite dimension. □

In particular, if I is a curve, after a generic change of coordinates one can finitely compute its eliminating dual spaces for $A = \{x_1\}$. The following proposition provides a method to compute eliminating dual spaces of the quotient ideal $I : \langle x_1 \rangle$ as well.

Proposition 6.3.4. $E_0^d[I : \langle x_1 \rangle, \{x_1\}] = x_1 \cdot E_0^{d+1}[I, \{x_1\}]$ *for all* $d \in \mathbb{N}_0$.

Proof. Let $\succeq$ be a dual order on D_0 eliminating x_1. For any functional $p \in D_0$, either $\mathrm{in}_{\succeq}(p)$ is divisible by ∂_1, or p has no terms divisible by ∂_1. In the first case, $\mathrm{in}_{\succeq}(x_1 \cdot p) = \mathrm{in}_{\succeq}(p)/\partial_1$. In the second case $x_1 \cdot p = 0$. Therefore, in the view of Theorem 6.2.2, any non-zero $q \in E_0^d[I : \langle x_1 \rangle, \{x_1\}]$ must be the derivative of some $p \in E_0^{d+1}[I, \{x_1\}]$. □

This proposition is used in Algorithm 7.2.1; see Example 7.2.4.

Proposition 6.3.4 for curves does not hold in general (only a weaker Proposition 6.3.5 does) and we are unable to use the eliminating dual spaces outside the specialized Algorithm 7.2.1.

Proposition 6.3.5.

$$E_0^d[I : \langle x_1, \ldots, x_m \rangle, \{x_1, \ldots, x_m\}] \supset \sum_{i=1}^{m} x_i \cdot E_0^{d+1}[I, \{x_1, \ldots, x_m\}] \tag{6.3.1}$$

for all $d \in \mathbb{N}_0$.

Proof. The inclusion (6.3.1) holds, since $I : \langle x_1, \ldots, x_m \rangle = \bigcap_{i=1}^{m} I : \langle x_i \rangle$ and, by Theorem 6.2.2,

$$D_0[I : \langle x_1, \ldots, x_m \rangle] = \sum_{i=1}^{m} D_0[I : \langle x_i \rangle] = \sum_{i=1}^{m} x_i \cdot D_0[I].$$

□

Remark 6.3.6. Assuming it is finite, a basis for $E_0^d[I, \{x_1, \ldots, x_m\}]$ can be computed by finding a basis of the dual space of $I + \langle x_1, \ldots, x_m \rangle^{d+1}$. The dual space of a 0-dimensional ideal can be efficiently computed for example with the algorithm of [49] or others.

CHAPTER VII

EMBEDDED COMPONENT TESTS

7.1 Numerical primary decomposition

There is a handful of methods for *symbolic* primary decomposition with implementations carried out for decomposition over $\mathbb{Q}$. For a good overview see [17].

A method for *numerical primary decomposition* (NPD) was introduced in [44] and is intended to compute an *absolute* primary decomposition, i.e., decomposition over $\mathbb{C}$. Conceptually it relies on the numerical oracles mentioned in the Introduction and is very different from the symbolic techniques such as Gröbner bases and characteristic sets. There are several components of the NPD algorithm that are not detailed in [44]; here we fill in the gaps.

The following construction, inspired by the higher-order deflation [46], computes a superset of the primary components of an ideal. Consider an ideal $I = (f_1, \ldots, f_N) \subset R = \mathbb{C}[x]$. Let $q = \sum_{|\beta| \le d} a_\beta \partial^\beta \in \mathbb{C}[a][\partial]$ be a linear differential operator of order at most d with coefficients in the polynomial ring $\mathbb{C}[a]$. Note there is a natural action of $\mathbb{C}[a][\partial]$ on $\mathbb{C}[a][x]$.

The ideal generated by $f_1, \ldots, f_N$ and $q(x^\alpha f_i)$ for all $|\alpha| \le d-1$ and $i = 1, \ldots, N$ is called the *deflation ideal* of I of order d and denoted by $I^{(d)}$.

We also refer to the *deflated variety* of order d,

$$X^{(d)} = \mathbb{V}(I^{(d)}) \subset \mathbb{C}^{B(n,d)},$$

where $B(n,d) = n + \binom{n+d-1}{d}$ is the number of variables in $\mathbb{C}[x,a]$.

The deflation ideal $I^{(d)}$ and, therefore, the deflated variety $X^{(d)}$ does not depend on the choice of generators of the ideal I (see [44, Proposition 2.7]).

Denote by $\pi_d : X^{(d)} \to X$ the restriction of the natural projection from $\mathbb{C}^{B(n,d)}$ to $\mathbb{C}^n$. Note that this map is a surjection onto $X = X^{(0)} = \mathbb{V}(I)$.

Remark 7.1.1. For every point $x \in \mathbb{C}^n$ the fiber of π_d is isomorphic to the truncated dual space of order d, i.e.,

$$\pi_d^{-1}(x) \simeq D_x^d(I).$$

The following statement enables us to compute all (including embedded) components associated to I.

Theorem 7.1.2 (Theorem 3.8 of [44])**.** *Every component is* visible *at some order d, i.e., for every prime $P \in \mathrm{Ass}(R/I)$, there exists d such that the preimage $Y^{(d)} = \pi_d^{-1}(Y)$ of the variety $Y = \mathbb{V}(P)$ is an irreducible (isolated) component of the variety $X^{(d)} = \mathbb{V}(I^{(d)})$.*

The term "visible" reflects the tool that is used to "see" components: *numerical irreducible decomposition* (NID) algorithms such as in [55], which can detect isolated components numerically.

We call an isolated component $Y^{(d)}$ of $X^{(d)}$ a *pseudocomponent* if $\pi_d(Y^{(d)})$ is not a component of X. We call pseudocomponents and embedded components of X collectively *suspect components*.

Here is an outline of Algorithm 5.3 of [44] that computes a superset of all associated components.

Algorithm 7.1.3. $\mathcal{N} = \mathrm{NPD}(I)$

Require: I, ideal of R.

Ensure: $\mathcal{N}$, components associated to I.

$\mathcal{N} \leftarrow \emptyset$

$d \leftarrow 0$

repeat

$C_1 \leftarrow$ isolated components of $I^{(d)}$ computed with an NID algorithm

$C_2 \leftarrow \{Y \in C_1 \mid \pi_d(Y) \neq Z \text{ for all } Z \in \mathcal{N}\}$

for all $Y \in C_2$ **do**

if Y is not a *pseudocomponent* **then**

$\mathcal{N} \leftarrow \mathcal{N} \cup \{Y\}$

end if

end for

$d = d + 1$;

until a stopping criterion holds for d

There are two parts of the algorithm that need clarification:

- a routine to determine whether a subvariety of X is a pseudocomponent;
- a stopping criterion.

A stopping criterion can be provided by a bound on the regularity index of the (global) Hilbert function. However, this *a priori* bound doubly exponential in the number of variables is not practical.

The problem we solve in this chapter is that of distinguishing embedded components from pseudocomponents. The problem statement can be condensed to the following.

Problem 7.1.4. Consider an ideal $I \subset R$ and a prime ideal $P \supset I$. Let $Q_1, \ldots, Q_r \supset I$ be the primary ideals in a primary decomposition of I such that $\sqrt{Q_i} \subsetneq P$.

Given generators of I and generic points $y_0 \in \mathbb{V}(P)$ and $y_i \in \mathbb{V}(Q_i)$ $(i = 1, \cdots, r)$, determine whether P is an associated prime of R/I.

Equivalently, let $y_0 = 0 \in \mathbb{V}(P)$ be a sufficiently generic point (we may assume the origin is a generic point without a loss of generality), determine whether

$$IR_0 = Q_1R_0 \cap \cdots \cap Q_rR_0. \tag{7.1.1}$$

In Section 7.2 we first present a relatively simple algorithm for answering Question 7.1.4 in the special case when I has dimension 1, and thus any suspect component P has dimension 0. In Section 7.3 we present a different algorithm which puts no restriction on the dimension of I, but still assumes the suspect component P has dimension 0. Finally we adapt this algorithm to the fully general case in Section 7.3.1. These results are joint work with Anton Leykin and originally appeared in [40][41].

7.2 Embedded component test for a curve

We consider the case when the variety is locally a curve, namely, $\dim_{y_0} I = 1$. That means $\dim P_i = 1$ for $i \neq 0$ and $\mathbb{V}(P_0) = \{y_0\}$ is a point that may or may not be an embedded component.

Let an ideal I be given by its generators F and suppose, without a loss of generality, that the point in question is $y_0 = 0$. Let the 1-dimensional primary components in the problem be $P_1, \ldots, P_r$ with $V_i = \mathbb{V}(P_i)$ containing the origin. Saturating I by the ideal $\langle x_1 \rangle$ eliminates all the components of I that contain $\langle x_1 \rangle$. After a generic linear change of coordinates, we may assume that no V_i is contained in the hyperplane $x_1 = 0$ except for $V_0 = \mathbb{V}(Q_0)$, so $I : \langle x_1 \rangle^\infty \neq I$ if and only if the origin is an embedded component.

This leads to the following algorithm that employs the eliminating dual spaces.

Algorithm 7.2.1. $B = \text{IsOriginEmbeddedInCurve}(I)$

Require: I, a 1-dimensional ideal of R in regular position relative to x_1.

Ensure: $B =$ "origin is an embedded component of I", a Boolean value.

$r \leftarrow \rho_0(I)$;

$m \leftarrow \mu_0(I)$;

$k \leftarrow \max(r, m-1)$;

$E \leftarrow E_0^k[I, \{x_1\}]$;

return $x_1 \cdot E \subsetneq E_0^{k-1}[I, \{x_1\}]$

Here $\mu_0(I)$ denotes the *multiplicity* (or *degree*) of I at the origin. For I a curve, note the (local) Hilbert polynomial of I is the constant polynomial $\mathrm{HP}_I(k) = \mu_0(I)$. To compute $\rho_0(I)$ and $\mu_0(I)$ we can use Algorithm 6.1.12 from which we can produce the Hilbert function of I from a set of generators, and in the process the Hilbert regularity index and the Hilbert polynomial of I.

The following two lemmas are used in the proof of correctness of Algorithm 7.2.1.

Lemma 7.2.2. *Suppose ideals $I, J \subset R_0$ satisfy $I \subseteq J$ and $\dim_{\mathbb{C}} J/I$ is finite. Then $I = J$ if and only if*

$$D_0^{r-1}[I] = D_0^{r-1}[J]$$

where $r = \max\{\rho_0(I), \rho_0(J)\}$.

Proof. Since $I \subseteq J$, to show $I = J$ it is enough to show that $H_I(k) = H_J(k)$ for all $k \geq 0$. Because $\dim_{\mathbb{C}} J/I$ is finite, $\mathrm{HP}_I = \mathrm{HP}_J$ so the Hilbert functions agree for $k \geq r$. If additionally $D_0^{r-1}[I] = D_0^{r-1}[J]$, then the Hilbert functions also agree for $0 \leq k < r$. □

Lemma 7.2.3. *If J is a one-dimensional monomial ideal that is saturated at the origin ($J = J : \mathfrak{m}^\infty$), then*

$$\rho_0(J) \leq \mu_0(J) - 1.$$

Proof. We consider a *monomial cone decomposition* of the standard monomials of J. For monomial $m \in R_0$ and a set of variables $v = \{x_{i_1}, \ldots, x_{i_k}\}$ the monomial cone $C_{m,v}$ is

$$C_{m,v} := \{x_{i_1}^{a_1} \cdots x_{i_k}^{a_k} m \mid (a_1, \ldots, a_k) \in \mathbb{N}_0^k\}.$$

A monomial cone decomposition of R_0/J is a finite list of pairs

$$(m_1, v_1), \ldots, (m_s, v_s)$$

such that the standard monomials of J are a disjoint union of the cones

$$C_{m_1,v_1}, \ldots, C_{m_s,v_s}.$$

The dimension of a cone $C_{m,v}$ is defined to be the size of v. A cone decomposition is closely related to the Hilbert function of J: the maximum dimension of a cone in the decomposition is the dimension of the ideal; the number of maximal dimensional cones is the multiplicity $\mu_0(J)$; and the maximum degree of the monomials $m_1, \ldots, m_s$ bounds the regularity $\rho_0(J)$. For J a one-dimensional monomial ideal saturated at the origin, there is a cone decomposition $(m_1, \{x_{i_1}\}), \ldots, (m_s, \{x_{i_s}\})$ of R_0/J consisting only of dimension 1 cones.

Modify this decomposition slightly by letting $m'_j := m_j|_{x_{i_j}=1}$, the monomial obtained from m_j by removing x_{i_j}. The cones $C_{m'_1,v_1}, \ldots, C_{m'_s,v_s}$ also have the standard monomials of J as their union, but are generally not disjoint. To prove the proposition, it is sufficient show that for all $d \geq \mu_0(J) - 1$ each cone contains exactly one monomial of degree d and these monomials are distinct, and therefore $H_J(d) = \mu_0(J)$.

Let $M_k := \{m'_j \mid i_j = k\}$. Note that $\sum_k |M_k| = \mu_0(J)$. For each k, M_k is closed under differentiation. This follows from the fact that M_k is the set of standard monomials of $\pi(J)$ where $\pi : \mathbb{C}[x_1, \ldots, x_N] \to \mathbb{C}[x_1, \ldots, \hat{x_k}, \ldots, x_N]$ is the projection sending x_k to 1. If M_k has a monomial of degree d, it also has at least one monomial of each degree $< d$. Therefore

$$\max_{m \in M_k} \deg m \leq |M_k| - 1 \leq \mu_0(J) - 1.$$

So for $d \geq \mu_0(J) - 1$, each cone contains a monomial of degree d.

Suppose two cones in the decomposition intersect, so $n = m'_j x_{i_j}^a = m'_l x_{i_l}^b$ for some $j \neq l$ and $x_{i_j} \neq x_{i_l}$. Then $x_{i_j}^a$ divides m'_l so $a \leq \deg m'_l$.

$$\deg n = \deg m'_j + a \leq \deg m'_j + \deg m'_l \leq |M_{i_l}| + |M_{i_j}| - 2 \leq \mu_0 - 2.$$

No two cones have a monomial in common of degree $d \geq \mu_0(J) - 1$. $\square$

Proof of correctness of Algorithm 7.2.1. By Proposition 6.3.4 $x_1 \cdot E = E_0^{k-1}[I : \langle x_1 \rangle, \{x_1\}]$. If this dual space is not equal to $E_0^{r-1}[I, \{x_1\}]$ then $I : \langle x_1 \rangle \neq I$. This implies there is an embedded component at the origin.

Suppose instead $x_1 \cdot E = E_0^{k-1}[I, \{x_1\}]$. We will use Lemma 7.2.2 to prove that $I : \langle x_1 \rangle = I$. The truncated dual space of degree $r-1$ is contained in the eliminating dual space of degree r, so $D_0^{r-1}[I : \langle x_1 \rangle] = D_0^{r-1}[I]$. We know that $I \subseteq I : \langle x_1 \rangle$. Because they differ by at most a zero-dimensional component, $\dim_{\mathbb{C}}(I : \langle x_1 \rangle)/I$ is finite.

Finally it must be shown that $k \geq \max(\rho_0(I), \rho_0(I : \langle x_1 \rangle))$. It is clear that $k \geq \rho_0(I)$. To show $k \geq \rho_0(I : \langle x_1 \rangle)$, let $J = \mathrm{in}(I) : \mathfrak{m}^\infty$, which has the same Hilbert polynomial as I and $I : \langle x_1 \rangle$ and satisfies

$$\mathrm{in}(I) \subseteq \mathrm{in}(I : \langle x_1 \rangle) \subseteq J,$$

$$H_I \geq H_{I:\langle x_1 \rangle} \geq H_J.$$

By Lemma 7.2.3, $\rho_0(J) \leq \mu_0(I) - 1$. Since $H_{I:\langle x_1 \rangle}$ is sandwiched between H_I and H_J, once they stabilize to $\mu_0(I)$, so must $H_{I:\langle x_1 \rangle}$. This implies the regularity of $I : \langle x_1 \rangle$ is bounded by k. □

Example 7.2.4. Let $I = \langle x^2 - z^3, y - z^2 \rangle \subset \mathbb{C}[x, y, z]$ which defines a curve in $\mathbb{C}^3$ with a singular point at the origin. The deflation algorithm from [44] will identify the origin as a possible embedded component. Note that $\rho_0(I) = 1$, $\mu_0(I) = 2$ and no irreducible component of $\mathbb{V}(I)$ is contained in the plane $x = 0$. To test whether the origin is embedded, we compute the eliminating dual $E_0^1[I, \{x\}]$. This is the set of all dual functionals with all terms having ∂_x-degree ≤ 1.

$$E_0^1[I, \{x\}] = \mathrm{span}\{1, \partial_z^2 + \partial_y, \partial_z, \partial_x, \partial_x\partial_z^2 + \partial_x\partial_y, \partial_x\partial_z\},$$

$$x \cdot E_0^1[I, \{x\}] = \mathrm{span}\{1, \partial_z^2 + \partial_y, \partial_z\}.$$

Since $x \cdot E_0^1[I, \{x\}] = E_0^0[I, \{x\}]$ we conclude that the origin is not an embedded component of I.

Example 7.2.5. For this example we compute with an implementation of Algorithm 7.2.1 in *Macaulay2*. Let I be the ideal of the cyclic4 system, generated by

$$\{x_1 + x_2 + x_3 + x_4,\ x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1,$$

$$x_2x_3x_4 + x_1x_3x_4 + x_1x_2x_4 + x_1x_2x_3,\ x_1x_2x_3x_4 - 1\}.$$

I is a curve with several singular points, which are discovered using the algorithm described in [44] up to some numerical precision. One such point is $p =$

$$(-0.0000000000000000122 + 1.0000000000000000222i,$$

$$-0.0000000000000001128 + 0.9999999999999999889i,$$

$$0.0000000000000000459 - 0.9999999999999999889i,$$

$$-0.0000000000000000935 - 1.0000000000000000000i),$$

approximately $(i, i, -i, -i)$. Let I' denote the ideal obtained from I by a random affine change of coordinates that fixes p. This ensures that I' is in general position with respect of x_1. Using the algorithm of Section 6.1.3, the regularity index is $\rho_p(I') = 2$ and the multiplicity is $\mu_p(I') = 1$, so $k = \max(2, 0) = 2$.

Computing $E_p^1[I', \{x_1\}]$ and $x_1 \cdot E_p^2[I', \{x_1\}]$ the dimensions are 3 and 2 respectively, so they are not equal. Therefore the point being approximated by p is an embedded component of I. The code for this example can be found at [39].

7.3 Suspect component of dimension 0

We now turn to the case where I has general dimension, rather than being a curve, but first consider when the suspect component is of dimension 0. Without the loss of generality we may assume that it is the origin and also that $I = IR_0 \cap R$ because we may ignore components away from the origin. To simplify our notation, let $I = Q_0 \cap J$ where $J = Q_1 \cap \cdots \cap Q_r$ (as in Problem 7.1.4) and either

- $Q_0 = R$, i.e., V_0 is a pseudocomponent;
- Q_0 is a primary ideal with $\sqrt{Q_0} = \langle x_1, \ldots, x_n \rangle \in \mathrm{Ass}(R/I)$ and Q_0 does not contain $J = Q_1 \cap \ldots \cap Q_r$, i.e., V_0 is a (true) component.

The goal is to distinguish the two cases above. Is $I = J$ or not?

For a generic linear form ℓ (so $\ell \notin \sqrt{I}$) we have

$$I \subseteq (I : \langle \ell \rangle) \subseteq J$$

with equality at the first inclusion if and only if there is no embedded component of I at the origin. Our general strategy will be to compute information about $I : \langle \ell \rangle$ and J and compare to I in order to certify either that $I = I : \langle \ell \rangle$ in which case there is no embedded component, or that $I \neq J$ in which case there is.

A major stumbling block is that we cannot get our hands directly on $I : \langle \ell \rangle$ or J, or even on their truncated dual spaces. In the former case, as discussed in Section 6.3, we can compute $S_d := \ell \cdot D_0^{d+1}[I]$ which is a subspace of $D_0^d[I : \langle \ell \rangle]$. If for large enough d, S_d contains all s-corners of $D_0[I]$, then we conclude that $D_0[I : \langle \ell \rangle] = D_0[I]$, certifying that the origin is not embedded, but we cannot use this test to certify the origin is embedded. On the other side, we compute subspaces $J_d := J \cap R_d$ of J, where R_d denotes the space of polynomials with all terms of degree $\leq d$. If $J_d \not\subset I$ for some d then this certifies that the origin is embedded. Similarly as J_d is only a subset of J, we cannot use it to certify the origin is a pseudocomponent. Both procedures are simultaneously iterated over d until one terminates.

This algorithm is below, with the procedure IdealTruncation to compute J_d defined later as Algorithm 7.3.9. To find $\mathrm{in}_{\geq} I$ (in particular, the s-corners of the staircase) we use the algorithm of Section 6.1.3.

Algorithm 7.3.1. $B = \mathrm{IsOriginEmbedded}(I)$

Require: $I = \langle F \rangle$, an ideal of R.

Ensure: $B =$ "origin is an embedded component of I", a boolean value.

1: compute $\text{in}_{\geq} I$
2: $d \leftarrow 0$
3: $\ell \leftarrow$ a generic linear form
4: **loop**
5: $\quad J_d \leftarrow \text{IdealTruncation}(F, d)$
6: $\quad$ **if** $\text{in}_{\geq} J_d \not\subset \text{in}_{\geq} I$ **then**
7: $\quad\quad$ **return** true
8: $\quad$ **end if**
9: $\quad S_d \leftarrow \ell \cdot D_0^{d+1}[I]$
10: $\quad$ **if** $\partial^\alpha \in \text{in}_{\geq} S_d$ for all s-corners x^α of $\text{in}_{\geq} I$ **then**
11: $\quad\quad$ **return** false
12: $\quad$ **end if**
13: $\quad d \leftarrow d + 1$
14: **end loop**

Proof of correctness and termination. If the condition in Line 6 holds then there is some $f \in J_d \subset J$ such that $f \notin I$. Hence $J \neq I$ which implies the origin is an embedded component. Because $J = \bigcup_d J_d$, if $J \neq I$ then there is large enough d for which J_d will provide such a certificate.

Suppose $I \neq J$ and let M_I denote the set of standard monomials of I. Because I and $I : \langle \ell \rangle$ differ only by a component at the origin, $(I : \langle \ell \rangle)/I$ has finite $\mathbb{C}$ dimension, and so $M_I \setminus M_{I:\langle \ell \rangle}$ is also finite. $M_{I:\langle \ell \rangle}$ is closed under division, so $M_I \setminus M_{I:\langle \ell \rangle}$ contains a monomial which is maximal in M_I, which is an s-corner of I. Therefore if the condition in Line 10 holds then $I = I : \langle \ell \rangle$. Because $D_0[I : \langle \ell \rangle] = \bigcup_d S_d$, if $I = I : \langle \ell \rangle$ then there is large enough d for which S_d will provide such a certificate. □

One way to think about the algorithm is as follows. The staircases of J and $I : \langle \ell \rangle$ sit "below" the staircase of I. Since J_d is a subset of J, it provides an upper bound on

the staircase of J, which can bound it away from I, proving that $J \neq I$. On the other hand, since S_d is a subset of $D_0[I : \langle \ell \rangle]$, it provides a lower bound on the staircase of $I : \langle \ell \rangle$. If it includes the s-corners of I, then the staircases must agree. See Figure 4.

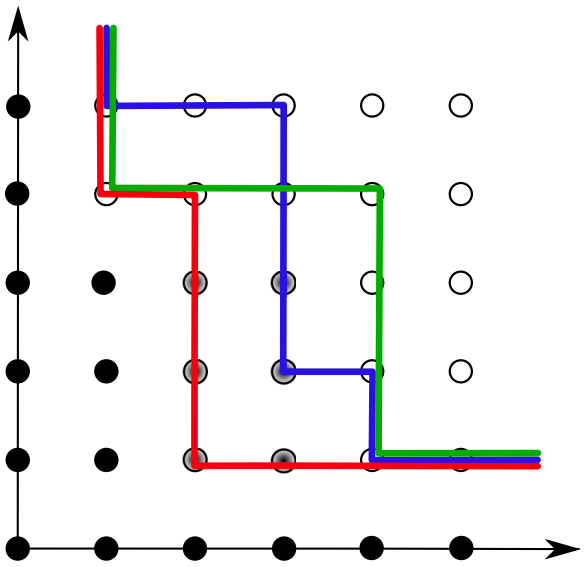

Figure 4: Both I (green) and $\langle J_d \rangle$ (blue) are contained in J (red). In general, no other containments hold. For $d \gg 0$, $\langle J_d \rangle = J$. The set $\text{in}_{\geq} J \setminus \text{in}_{\geq} I$ of monomials is finite.

7.3.1 Ideal truncation algorithm

To complete Algorithm 7.3.1 it remains to produce an algorithm for ideal truncations.

Problem 7.3.2 (Local Interpolation)**.** Let $d > 0$ and $J = Q_1 \cap \cdots \cap Q_r$ with each Q_i a primary ideal such that each $V_i = \mathbb{V}(Q_i)$ contains the origin (equivalently $J = JR_0 \cap R$). Compute $J_d = J \cap R_d$.

We assume access to oracle $\mathbf{O}_J$ which can sample random generic points x on any V_i, and for any such x and any $e \geq 0$ can compute $D^e_x[J]$.

Remark 7.3.3. We can use the tools of NPD to sample points on the suspect components of $I = J \cap Q_0$, which in particular means generic points on $\mathbb{V}(Q_i)$ can be produced. We can also compute truncated dual spaces $D^e_x[I]$ using the generators of I. The local properties of J and I agree away from the origin and the origin is

not a primary component of J. Therefore simply by excluding the origin from consideration, we have access to the tools promised by $\mathbf{O}_J$ and our oracle assumption is justified.

To solve Problem 7.3.2 we will use a form of interpolation. We will sample generic points x on the components of J, and compute dual spaces $D^e_x[J]$, which provide certain linear constraints on the evaluation and derivatives of polynomials $f \in JR_x$. Finally we require a check to know when we have enough constraints to exactly define J_d.

We first consider the *double truncations* of J:

$$J^e_d = \{f \in R_d \mid \text{for all } i,\ D^e_x[Q_i]f = 0 \text{ for any generic point } x \in V_i\}. \tag{7.3.1}$$

The following is a probabilistic algorithm to compute J^e_d whenever we have a procedure to compute $D^e_x[J]$ for any sufficiently generic point $x \in Q_i$ and any e. In our case we have access to such a procedure because for any point x away from the origin $D^e_x[J] = D^e_x[I]$. Note $D^e_x[I]$ can be computed by the usual methods since the generators of I are known.

Algorithm 7.3.4. $J^e_d = \text{TruncatedTruncation}(\mathbf{O}_J, d, e)$

Require: $\mathbf{O}_J$ an oracle as in Problem 7.3.2;

$d, e \in \mathbb{N}_0$.

Ensure: J^e_d is as defined in (7.3.1)

$K \leftarrow R_d$

repeat

$oldK \leftarrow K$

with $\mathbf{O}_J$ choose generic points $x_i \in V_i$ for $i = 1, \ldots, r$.

$K \leftarrow K \cap (D^e_{x_1}[J])^\perp \cap \cdots \cap (D^e_{x_r}[J])^\perp$

until $oldK = K$

return $J^e_d = K$

Proof of correctness and termination. Note that at every step $K \supseteq J_d^e$. Suppose at some step that $K \neq J_d^e$. There is $f \in K$ such that for some V_i and any generic point $x \in V_i$, f is not orthogonal to $D_x^e[J]$ by the definition of J_d^e. The point x_i chosen on V_i is chosen generically, so the new value of K is strictly contained in $oldK$. Therefore when K stabilizes, it must be equal to J_d^e. Since K is finite dimensional at every step, termination is guaranteed. □

Proposition 7.3.5. *For any d, the chain*

$$J_d^0 \supseteq J_d^1 \supseteq J_d^2 \supseteq \cdots$$

stabilizes to J_d. That is, $J_d^e = J_d$ for all e sufficiently large.

Proof. For any point x recall from Proposition 5.2.4 that polynomial f has $p(f) = 0$ for all $p \in D_x[I]$ if and only if $f \in IR_x \cap R$, and note that $IR_x \cap R = \bigcap_{x \in V_i} Q_i$. Choosing a point x_i from each V_i, the set $\bigcup_e J_d^e$ is the set of polynomials $f \in R_d$ orthogonal to each dual space $D_{x_i}[I]$. Because every V_i contains at least one of the points $x_1, \ldots, x_r$,

$$\bigcap_i (D_{x_i}[I])^\perp = Q_1 \cap \cdots \cap Q_r = J.$$

Therefore $\bigcup_e J_d^e = J_d$. Since J_d has finite $\mathbb{C}$-dimension, there must be some e at which stabilization occurs. □

This fact suggests an algorithm for computing J_d from the double truncations, in particular for each value of $e \geq 0$ compute J_d^e until some $J_d^e \subseteq J$. A naive stopping criterion for this procedure might be when $J_d^e = J_d^{e+1}$ for some e, but this will not work as the following example illustrates.

Example 7.3.6. Let $I = \langle x^k + y, y^k \rangle \subset R = \mathbb{C}[x, y, z]$, a positive-dimensional primary

ideal. The reader may check that

$$I_1^1 = y$$

$$I_1^2 = y$$

$$\ldots$$

$$I_1^k = I_1 = 0$$

This example shows that equality of two subsequent I_d^e and I_d^{e+1} is not a valid stopping criterion. Also, note that $I_1^e \not\subset I$ for $e < k$.

Instead we require an method to check if $J_d^e \subseteq J$. First note that for any finite dimensional $\mathbb{C}$-vector subspace V and any subspace W, a generic vector $v \in V$ is in W if and only if $V \subseteq W$. Therefore it is sufficient for our purposes to check if a randomly chosen polynomial $g \in J_d^e$ is contained in J. Such a membership test was described in Algorithm 6.2.4 when generators for the ideal were known, but in this case we do not know generators of J, only for I, so the algorithm must be modified.

Proposition 7.3.7. *Let $I = Q_0 \cap Q_1 \cap \cdots \cap Q_r$ be an irredundant primary decomposition with $\mathbb{V}(Q_i) \ni 0$ for all i and $\dim Q_0 = 0$. Let $J = Q_1 \cap \cdots \cap Q_r$.*

Then $g \in J$ if and only if $I : \langle g \rangle$ is a zero-dimensional ideal.

Proof. If $g \notin J$, then $g \notin Q_i$ for some $i > 0$, so $I : g \subset P_i$ where P_i is the prime associated to Q_i. Since P_i has positive dimension, so does $I : \langle g \rangle$. Conversely if $I : \langle g \rangle$ is positive-dimensional, it is contained in some positive-dimensional prime P. Then I has a primary component Q_i with $Q_i \subset P$ and $g \notin Q_i$. Since $Q_i \subset P$, it has positive dimension so $g \notin J$. □

To check that this condition holds we use the dual space of $\langle F^h \rangle : \langle g^h \rangle$, where $I = \langle F \rangle$, to find g-corners of $I : \langle g \rangle$, just as in Algorithm 6.2.4. $I : \langle g \rangle$ is zero-dimensional if and only if for every variable x_i there is a g-corner of $I : \langle g \rangle$ of the form x_i^a.

We do not know a method to show when $I : \langle x \rangle$ is not zero-dimensional. As a result, our algorithm to determine if $g \in J$ will stop at some cutoff degree c, return true if it can certify that $g \in J$, and return false if the cutoff value is reached.

Algorithm 7.3.8. $B = \text{IsWitnessPolynomial}(F, g, c)$

Require: $I = \langle F \rangle$, an ideal of R;

g, a polynomial in R;

c, a degree cutoff.

Ensure: $B = false$ if $g \notin J$ and $true$ if $g \in J$ and c sufficiently large.

(Here J and I differ by a component at the origin as in Proposition 7.3.7.)

$e \leftarrow \deg g^h$

$d \leftarrow 0$

$G \leftarrow \{\}$ (the g-corners of $I : \langle g \rangle$)

repeat

$C \leftarrow$ new g-corners of $I : \langle g \rangle$ computed from $g^h \cdot D_0^{d+e}[\langle F^h \rangle]$

append C to G

if $x_i^{a_i} \in G$ for all $i = 1, \ldots, n$ and any a_i **then**

return $true$

end if

$d \leftarrow d + 1$

until $d > c$

return $false$

Equipped with this algorithm for checking if a polynomial g is in J, and the double truncation algorithm above, we can now compute J_d as follows.

Algorithm 7.3.9. $J_d = \text{IdealTruncation}(F, d)$

Require: $I = \langle F \rangle$, an ideal of R;

$d \in \mathbb{N}_0$.

$e \leftarrow 0$

loop

$J_d^e \leftarrow$ TruncatedTruncation$(\mathbf{O}_J, d, e)$

$g \leftarrow$ random polynomial chosen from J_d^e

if IsWitnessPolynomial(F, g, e) **then**

return $J_d = J_d^e$

end if

$e \leftarrow e + 1$

end loop

Proof of correctness and termination. If IsWitnessPolynomial(F, g, e) returns true then g must be in J_d. By Proposition 7.3.5 $J_d^e \supseteq J_d$, so randomly chosen g from J_d^e has $g \in J_d$ if and only if $J_d^e = J_d$ almost surely. This proves correctness.

To prove termination, first note that there is e_0 such that $J_d^e = J_d$ for all $e \geq e_0$ by Proposition 7.3.5. It remains to show that IsWitnessPolynomial(F, g, e) will return true for some $e \geq e_0$.

For any $g \in J_d$, let $c(g)$ denote the minimum cutoff value c such that IsWitnessPolynomial(F, g, c) returns true. Let $\{b_1, \ldots, b_s\}$ be a $\mathbb{C}$-basis for J_d, so we can express $g \in J_d$ as $g = \sum_{i=1}^{s} a_i b_i$. For any given value of c, the set of polynomials

$$W_c = \{g \in J_d \mid c(g) = c\}$$

can be described by a finite set of algebraic conditions on $a_1, \ldots, a_s$, so W_c is a constructible set. In particular, there is some c_0 such that W_{c_0} is Zariski open, so IsWitnessPolynomial(F, g, c_0) will return true for generic $g \in J_d$. For $e \geq \max\{e_0, c_0\}$, a generic polynomial g sampled from J_d^e will be a in J_d, and IsWitnessPolynomial(F, g, e) will certify this fact. □

This completes Algorithm 7.3.1 for determining if the origin is a zero-dimensional embedded component of ideal I.

Example 7.3.10. We again consider the cyclic4 system as in Example 7.2.5, but apply the algorithm for varieties of general dimension.

Computing `numericalIrreducibleDecomposition` of the first-order deflated variety $X^{(1)} = \mathbb{V}(I^{(1)})$ we obtain witness sets representing isolated components of $X^{(1)}$ that project to

- two irreducible curves, isolated components that are visible and can be discovered by `numericalIrreducibleDecomposition` of $X = \mathbb{V}(I)$, and
- eight points, approximations to $\{(a, b, -a, -b) \mid a \in \{\pm 1, \pm i\},\ b = \pm a\}$ which are *suspect* components.

For an approximation of the point $(i, -i, -i, i)$, `isPointEmbedded` produces a witness polynomial,

```
witness poly: (d',d) = (1, 4)
(.586169+.361093*ii)*x_1+(.776351+.36685*ii)*x_2+
(.586169+.361093*ii)*x_3+(.776351+.36685*ii)*x_4
```

showing that this point is an embedded component. Same conclusion holds for all suspect points.

The associated primes (computed over $\mathbb{Q}$ with a symbolic *Macaulay2* routine) are

$$\begin{aligned}\mathrm{Ass}(R/I) = \{\ & (x_2 + x_4, x_1 + x_3, x_3x_4 + 1),\\ & (x_2 + x_4, x_1 + x_3, x_3x_4 - 1),\\ & (x_4 - 1, x_3 + 1, x_2 + 1, x_1 - 1),\\ & (x_4 - 1, x_3 - 1, x_2 + 1, x_1 + 1),\\ & (x_4 + 1, x_3 + 1, x_2 - 1, x_1 - 1),\\ & (x_4 + 1, x_3 - 1, x_2 - 1, x_1 + 1),\\ & (x_3 + x_4, x_2 + x_4, x_1 - x_4, x_4^2 + 1),\\ & (x_3 - x_4, x_2 + x_4, x_1 + x_4, x_4^2 + 1)\ \ \}\end{aligned}$$

confirming the numerical results.

7.4 Suspect component of positive dimension

Let P_0 be the vanishing (prime) ideal of suspect component V_0; let $d_0 = \dim V_0 > 0$.

We would like to deduce and rely on a Bertini-type theorem (Theorem 7.4.4) that, roughly, says that given an ideal $I \subset R$ with $\min_{P \in \mathrm{Ass}(R/I)} \dim P \geq d_0$ we have a correspondence between $\mathrm{Ass}(R/I)$ and $\mathrm{Ass}(R/(I+L))$ where L is a generic affine plane of codimension d_0. This correspondence is one-to-one for components of dimension d_0+1; there could be multiple 0-dimensional components in $\mathrm{Ass}(R/(I+L))$ "witnessing" components of dimension d_0 in $\mathrm{Ass}(R/I)$.

Lemma 7.4.1. *Let I be an ideal and f be an element of R. Then for a generic (affine) linear function $h \in R$*

$$(I+H) : F = (I : F) + H, \text{ where } F = \langle f \rangle, H = \langle h \rangle.$$

Proof. (The proof follows closely the argument at `mathoverflow.net/questions/143076` given by Hailong Dao.)

If $I+F = R$ then $I : F = I$ and $(I+H) : F = I+H$; therefore, assume $I+F \neq R$. The set of associated primes $A = \mathrm{Ass}(R/(I+F))$ is finite, hence, a generic h would be a non-zerodivisor on $R/(I+F)$. To see that it is enough to notice that the set of zerodivisors is exactly $\bigcup_{P \in A} P$ and that $n+1$ generic linear functions generate R.

Consider the exact sequence

$$0 \to R/(I : F) \to R/I \to R/(I+F) \to 0$$

with first map being the multiplication by f. Tensoring with R/H we get another exact sequence,

$$0 \to R/(I : F+H) \to R/(I+H) \to R/(I+F+H) \to 0,$$

coming from a long exact sequence for $\mathrm{Tor}^R(\cdot, R/H)$ and the fact that $\mathrm{Tor}_1^R(R/(I+F), R/H) = 0$ as H is a non-zerodivisor on $R/(I+H)$.

On the other hand, the first exact sequence with I replaced by $I + H$ says that the leftmost term in the second sequence should be isomorphic to $R/((I + H) : F)$, which proves the Lemma. □

Lemma 7.4.2. *In the notation of the previous proposition, if I defines a scheme with no embedded components, then so does $I + H$ for a generic H.*

Proof. See [24, Example 3.4.2(6)]: the condition of "having no embedded components" satisfies the Generic Principle [24, Theorem 3.3.10]. □

Lemma 7.4.3. *Let $I = Q_1 \cap ... \cap Q_r$ be a primary decomposition. Then for a generic hyperplane H the natural injection $R/I \hookrightarrow \bigoplus_i (R/Q_i)$ induces an injection*

$$R/(I + H) \hookrightarrow \bigoplus_i (R/(Q_i + H)).$$

In particular, $\mathrm{Ass}(R/(I + H)) \subset \{P + H \mid P \in \mathrm{Ass}(R/I)\}$.

Proof. Consider the short exact sequence

$$0 \to R/I \to \bigoplus_i (R/Q_i) \to C \to 0.$$

As in the proof of Lemma 7.4.1 we see that $\mathrm{Tor}_1(C, R/H) = 0$ for a generic hyperplane H. Indeed, this follows from a generic H being a non-zerodivisor due to the finiteness of $\mathrm{Ass}\, C$. □

Theorem 7.4.4. *Let I be an ideal of $R = \mathbb{C}[x_1, \ldots, x_n]$ and let L be the vanishing ideal for a generic affine $(n - k)$-plane. Then*

$$\mathrm{Ass}(R/I + L) = \{P + L \mid P \in \mathrm{Ass}(R/I),\ \dim(P) > k\} \cup \bigcup_{\substack{P \in \mathrm{Ass}(R/I) \\ \dim(P) = k}} \mathrm{Ass}(R/(P + L)).$$

Proof. Lemma 7.4.2 says, in particular, that for a primary ideal Q the ideal $Q + L$ has no embedded components; therefore, $Q + L$ is either primary or 0-dimensional (in case $\dim(Q) = \mathrm{codim}(L)$).

Now, on one hand, Lemma 7.4.3 says that $I + L$ has no extraneous associated primes: all components have to come from $Q + L$ where Q is an ideal in a primary decomposition of I. On the other hand, Lemma 7.4.1 implies that every $P \in \mathrm{Ass}(R/I)$ is witnessed by $\mathrm{Ass}(R/(P + L))$, since one can arrange an $f \in R$ so that $\mathrm{Ass}(R/(I : f)) = \{P\}$.

Finally, $\mathrm{Ass}(R/(P + L))$ contains one element $P + L$ when $\dim(P) > k$, is empty when $\dim(P) < k$, and is a finite set of maximal ideals when $\dim(P) = k$. □

Using this theorem we can reduce the case of a component of positive dimension to the embedded component test in the 0-dimensional case, i.e., the algorithms in previous subsections of this section. Indeed, for a suspect component V of dimension k one can intersect the scheme with a random affine plane $\mathbb{V}(L)$ of codimension k and ask whether a point of $V \cap \mathbb{V}(L)$ is an embedded component of that intersection.

Example 7.4.5. The radical ideal

$$I = \langle x, z\rangle \cap \langle x^2 - y^2, y + z\rangle \cap \langle x^2 - z^2, x + 2y\rangle \cap \langle (x - 1)y\rangle$$

describes a union of 5 lines and 2 planes.

A *Macaulay2* script that takes a set of generators of I proceeds to construct the first deflation ideal $I^{(1)}$ discovering 13 isolated components of $\mathbb{V}(I^{(1)})$ that project to suspect components in $\mathbb{C}^3$. Its summary reads

```
total: 13 suspect components
true components: {0, 3, 6, 9, 10, 11, 12}
```

displaying the correct list of 7 true components and correctly discarding all pseudocomponents.

This example is built primarily to test various scenarios for pseudocomponents: there is a positive-dimensional pseudocomponent – the intersection of two isolated planes – and several 0-dimensional pseudocomponents. For the former, Theorem 7.4.4

is utilized to reduce to the 0-dimensional case. One of the latter – the origin – has a non-empty set of s-corners, which engages non-trivially one of the termination modes of Algorithm 7.3.1. Here is the corresponding excerpt:

```
               2
-- s-corners: {y z}
                              3   2      2   3   2           2   ...
-- LM(dual of colon ideal): {x , x y, x*y , y , x z, x*y*z, y z, ...
V(z, y, x), contained in 6 other components, is a PSEUDO-component
```

The output can be interpreted to say that $\partial_y^2 \partial_z$ belongs to $\ell \cdot D_0^4[I]$, for a generic linear form ℓ, hence the conclusion.

REFERENCES

[1] Aoki, S. and Takemura, A., "Markov chain Monte Carlo exact tests for incomplete two-way contingency table," *Journal of Statistical Computation and Simulation*, vol. 75, no. 10, pp. 787–812, 2005.

[2] Arsuaga, J., Heskia, I., Hosten, S., and Maskalevich, T., "Uncovering proximity of chromosome territories using classical algebraic statistics," *arXiv preprint arXiv:1406.0148*, 2014.

[3] Aschenbrenner, M. and Hillar, C. J., "Finite generation of symmetric ideals," *Trans. Amer. Math. Soc.*, vol. 359, pp. 5171–5192, 2007.

[4] Aschenbrenner, M. and Hillar, C. J., "Finite generation of symmetric ideals," *Trans. Am. Math. Soc.*, vol. 359, no. 11, pp. 5171–5192, 2007.

[5] Atiyah, M. F. and Macdonald, I. G., *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[6] Bates, D. J., Hauenstein, J. D., Peterson, C., and Sommese, A. J., "A numerical local dimensions test for points on the solution set of a system of polynomial equations," *SIAM J. Numer. Anal.*, vol. 47, no. 5, pp. 3608–3623, 2009.

[7] Brouwer, A. and Draisma, J., "Equivariant Gröbner bases and the Gaussian two-factor model," *Mathematics of Computation*, vol. 80, no. 274, pp. 1123–1133, 2011.

[8] Church, T., Ellenberg, J. S., and Farb, B., "FI-modules: a new approach to stability for S_n-representations," *arXiv preprint arXiv:1204.4533*, 2012.

[9] Church, T., Ellenberg, J. S., Farb, B., and Nagpal, R., "Fi-modules over noetherian rings," *arXiv preprint arXiv:1210.1854*, 2012.

[10] Cohen, D. E., "On the laws of a metabelian variety," *Journal of Algebra*, vol. 5, no. 3, pp. 267–273, 1967.

[11] Cohen, D. E., "Closure relations, Buchberger's algorithm, and polynomials in infinitely many variables," in *Computation theory and logic*, vol. 270 of *Lect. Notes Comput. Sci.*, pp. 78–87, 1987.

[12] Dayton, B. H. and Zeng, Z., "Computing the multiplicity structure in solving polynomial systems," in *International Symposium on Symbolic and Algebraic Computation*, pp. 116–123, ACM, 2005.

[13] De Loera, J. A., Hemmecke, R., Onn, S., and Weismantel, R., "N-fold integer programming," *Discrete Optimization*, vol. 5, no. 2, pp. 231–241, 2008.

[14] De Loera, J. A. and Onn, S., "Markov bases of three-way tables are arbitrarily complicated," *Journal of Symbolic Computation*, vol. 41, pp. 173–181, 2006.

[15] De Loera, J. A., Sturmfels, B., and Thomas, R. R., "Gröbner bases and triangulations of the second hypersimplex," *Combinatorica*, vol. 15, no. 3, pp. 409–424, 1995.

[16] de Loera, J. A., Sturmfels, B., and Thomas, R. R., "Gröbner bases and triangulations of the second hypersimplex," *Combinatorica*, vol. 15, pp. 409–424, 1995.

[17] Decker, W., Greuel, G.-M., and Pfister, G., "Primary decomposition: algorithms and comparisons," in *Algorithmic algebra and number theory (Heidelberg, 1997)*, pp. 187–220, Berlin: Springer, 1999.

[18] Diaconis, P. and Sturmfels, B., "Algebraic algorithms for sampling from conditional distributions," *The Annals of statistics*, vol. 26, no. 1, pp. 363–397, 1998.

[19] Draisma, J., Eggermont, R. H., Krone, R., and Leykin, A., "Noetherianity for infinite-dimensional toric varieties," *arXiv preprint arXiv:1306.0828*, 2013.

[20] Draisma, J., Kuttler, J., and others, "Bounded-rank tensors are defined in bounded degree," *Duke Mathematical Journal*, vol. 163, no. 1, pp. 35–63, 2014.

[21] Drton, M., Sturmfels, B., and Sullivant, S., *Lectures on Algebraic Statistics*, vol. 39 of *Oberwolfach Seminars*. Springer, Berlin, 2009. A Birkhäuser book.

[22] Edel, Y., "Extensions of generalized product caps," *Designs, Codes and Cryptography*, vol. 31, no. 1, pp. 5–14, 2004.

[23] Fink, A. and Moci, L., "Matroids over a ring," *to appear in J. Europ. Math. Soc., arXiv:1209.6571*, 2012.

[24] Flenner, H., O'Carroll, L., and Vogel, W., *Joins and intersections*. Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[25] Gardner, M., "Mathematical games.," *Scientific American*, vol. 243, no. 6, pp. 18–28, 1980.

[26] Greuel, G.-M. and Pfister, G., *A* **Singular** *introduction to commutative algebra*. Berlin: Springer, extended ed., 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh and UNIX).

[27] Griffin, Z. A., Hauenstein, J. D., Peterson, C., and Sommese, A. J., "Numerical computation of the hilbert function of a zero-scheme," *Springer Proceedings in Mathematics & Statistics*, 2011.

[28] Hara, H., Takemura, A., and Yoshida, R., "Markov bases for two-way subtable sum problems," *Journal of Pure and Applied Algebra*, vol. 213, no. 8, pp. 1507–1521, 2009.

[29] Hauenstein, J. D., "A counter example to an ideal membership test," *Advances in Geometry*, vol. 10, pp. 557–559, 2010.

[30] Hauenstein, J. D., "Algebraic computations using Macaulay dual spaces," 2011. Preprint available at `www.math.ncsu.edu/~jdhauens/preprints/hAlgComputations.pdf`.

[31] Hauenstein, J. D. and Wampler, C. W., "Isosingular sets and deflation," *Found. Comput. Math.*, vol. 13, no. 3, pp. 371–403, 2013.

[32] Higman, G., "Ordering by divisibility in abstract algebras," *Proc. Lond. Math. Soc., III. Ser.*, vol. 2, pp. 326–336, 1952.

[33] Hillar, C. J. and del Campo, A. M., "Finiteness theorems and algorithms for permutation invariant chains of Laurent lattice ideals," *J. Symb. Comput.*, vol. 50, pp. 314–334, 2013.

[34] Hillar, C. J. and Sullivant, S., "Finite Gröbner bases in infinite dimensional polynomial rings and applications," *Advances in Mathematics*, vol. 221, pp. 1–25, 2012.

[35] Hillar, C. J. and Sullivant, S., "Finite groebner bases in infinite dimensional polynomial rings and applications," *Advances in Mathematics*, vol. 229, no. 1, pp. 1–25, 2012.

[36] Iarrobino, A. and Kanev, V., *Power sums, Gorenstein algebras, and determinantal loci*. Springer Science & Business Media, 1999.

[37] Kahle, T., Krone, R., and Leykin, A., "Equivariant lattice generators and Markov bases," in *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, pp. 264–271, ACM, 2014.

[38] Krone, R., "Numerical algorithms for dual bases of positive-dimensional ideals," *Journal of Algebra and Its Applications*, vol. 12, no. 06, p. 1350018, 2013.

[39] Krone, R. and Leykin, A., "Embedded Component Tests for Macaulay2." Available at `people.math.gatech.edu/~rkrone3/embedded-component-test/`.

[40] Krone, R. and Leykin, A., "Eliminating dual spaces," *arXiv preprint arXiv:1503.02038*, 2015.

[41] Krone, R., Leykin, A., and Hauenstein, J., "Numerical algorithms for detecting embedded components," *arXiv preprint arXiv:1405.7871*, 2014.

[42] Kruskal, J. B., "The theory of well-quasi-ordering: A frequently discovered concept," *Journal of Combinatorial Theory, Series A*, vol. 13, no. 3, pp. 297–305, 1972.

[43] Lecerf, G., "Quadratic Newton iteration for systems with multiplicity," *Found. Comput. Math.*, vol. 2, pp. 247–293, 2002.

[44] Leykin, A., "Numerical primary decomposition," in *International Symposium on Symbolic and Algebraic Computation*, pp. 165–172, ACM, 2008.

[45] Leykin, A., Verschelde, J., and Zhao, A., "Newton's method with deflation for isolated singularities of polynomial systems," *Theoretical Computer Science*, vol. 359, no. 1-3, pp. 111–122, 2006.

[46] Leykin, A., Verschelde, J., and Zhao, A., "Higher-order deflation for polynomial systems with isolated singular solutions," in *Algorithms in algebraic geometry*, vol. 146 of *IMA Vol. Math. Appl.*, pp. 79–97, New York: Springer, 2008.

[47] Macaulay, F. S., *The algebraic theory of modular systems*. Cambridge University Press, 1916.

[48] Marinari, M., Möller, H., and Mora, T., "On multiplicities in polynomial system solving," *Transactions of the American Mathematical Society*, vol. 348, no. 8, pp. 3283–3321, 1996.

[49] Mourrain, B., "Isolated points, duality and residues," *J. Pure Appl. Algebra*, vol. 117/118, pp. 469–493, 1997. Algorithms for algebra (Eindhoven, 1996).

[50] Nash-Williams, C., "On well-quasi-ordering finite trees," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 59, no. 04, pp. 833–835, 1963.

[51] Ohsugi, H. and Hibi, T., "Convex polytopes all of whose reverse lexicographic initial ideals are squarefree.," *Proc. Am. Math. Soc.*, vol. 129, no. 9, pp. 2541–2546, 2001.

[52] Room, T. G., *The geometry of determinantal loci*. Cambridge University Press, Cambridge, UK, 1938.

[53] Schrijver, A., *Combinatorial optimization: polyhedra and efficiency*, vol. 24. Springer Verlag, 2003.

[54] Snowden, A. and others, "Syzygies of Segre embeddings and δ-modules," *Duke Mathematical Journal*, vol. 162, no. 2, pp. 225–277, 2013.

[55] Sommese, A., Verschelde, J., and Wampler, C., "Numerical decomposition of the solution sets of polynomial systems into irreducible components," *SIAM J. Numer. Anal.*, vol. 38, no. 6, pp. 2022–2046, 2001.

[56] Sommese, A., Verschelde, J., and Wampler, C., "Introduction to numerical algebraic geometry," in *Solving polynomial equations* (Dickenstein, A. and Emiris, I., eds.), pp. 301–338, Springer-Verlag, 2005.

[57] Sommese, A. J. and Wampler, II, C. W., *The numerical solution of systems of polynomials*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.

[58] Sullivant, S., "Compressed polytopes and statistical disclosure limitation.," *Tohoku Math. J. (2)*, vol. 58, no. 3, pp. 433–445, 2006.

[59] Yamaguchi, T., Ogawa, M., and Takemura, A., "Markov degree of the Birkhoff model.," *J. Algebr. Comb.*, vol. 40, no. 1, pp. 293–311, 2014.