Solving Polynomial Systems With Special Structure

by

Christopher Jacques Hillar

B.S. (Yale University) 2000

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA, BERKELEY

Committee in charge:

Professor Bernd Sturmfels, Chair
Professor Mark Haiman
Professor Yuval Peres

Spring 2005

The dissertation of Christopher Jacques Hillar is approved:

Chair Date

Date

Date

University of California, Berkeley

Spring 2005

Solving Polynomial Systems With Special Structure

Abstract

Solving Polynomial Systems With Special Structure

by

Christopher Jacques Hillar
Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Bernd Sturmfels, Chair

We solve a collection of problems that give rise to structured systems of polynomial equations. Our tools are diverse, involving the theory of Gröbner bases, quasi-well-orderings, algebraic combinatorics, group algebras, and Brouwer degree theory. Nonetheless, a consistent theme pervades: exploit the underlying combinatorial structure in novel ways.

The first of these questions involves invariant ideals. Let A be a commutative Noetherian ring, and let $R = A[X]$ be the polynomial ring in an infinite collection X of indeterminates over A. Let $\mathfrak{S}_X$ be the permutation group of X. The group $\mathfrak{S}_X$ acts on R in a natural way, and this in turn gives R the structure of a left module over the group ring $R[\mathfrak{S}_X]$. We prove that all ideals of R invariant under the action of $\mathfrak{S}_X$ are finitely generated as $R[\mathfrak{S}_X]$-modules. The proof involves introducing a certain partial order on monomials and showing that it is a well-quasi-ordering. We also consider the concept of an invariant chain of ideals for finite-dimensional polynomial rings and relate it to the finite generation result mentioned above. Finally, a motivating question from chemistry is presented, with the above framework providing a suitable context in which to study it.

We next study a problem involving a special sequence of resultants, stemming from a question in dynamics. The m-th cyclic resultant of a univariate polynomial

$f \in \mathbb{C}[x]$ is

$$r_m = \operatorname{Res}(f, x^m - 1).$$

We characterize polynomials having the same set of nonzero cyclic resultants. Generically, for a polynomial f of degree d, there are 2^{d-1} distinct degree d polynomials with the same set of cyclic resultants as f. However, in the generic monic case, degree d polynomials are uniquely determined by their cyclic resultants. Moreover, two reciprocal ("palindromic") polynomials giving rise to the same set of nonzero r_m are equal. In the process, we also prove a unique factorization result in group algebras involving products of binomials. Finally, we discuss how our results yield algorithms for explicit reconstruction of polynomials from their cyclic resultants.

Our third system of equations arises in an unexpected manner from a recent problem in differential field theory. Given ordinary differential fields $K \subseteq E$ of characteristic zero, it is known that if $y \in E$ and $1/y$ satisfy linear differential equations with coefficients in K, then y'/y is algebraic over K. We present a new short proof of this fact using Gröbner basis techniques and give a direct method for finding a polynomial over K that y'/y satisfies. Moreover, our techniques provide explicit degree bounds. The chapter concludes with an application of our method to a class of nonlinear differential equations.

For our final topic, we investigate the existence of solutions to certain matrix equations, tangentially related to a long-standing (1975) open problem in quantum mechanics. Let $S(X, B)$ be a symmetric ("palindromic") word in two letters X and B. A theorem due to the author and Johnson states that for each pair of positive definite matrices B and P, there is a positive definite solution X to the word equation $S(X, B) = P$. We also conjectured that these solutions are unique. In this chapter, we resolve this conjecture (negatively). Furthermore, we prove that, generically, the number of solutions is odd (and thus finite) in the real case. Our approach utilizes the theory of Brouwer degree and also provides a second proof of existence of such solutions in the real case.

Professor Bernd Sturmfels
Dissertation Committee Chair

To my sister Annie and my parental units Marian and Janett

Contents

Acknowledgements

First of all, warm thanks go to my Ph.D. advisor Bernd Sturmfels for his constant dedication, insight, and interest. I would not be where I am now if it were not for his influence and assistance.

Other thanks go out to my various coauthors from whom I have learned a great deal. I would like to especially thank the following people: Scott Armstrong, Matthias Aschenbrenner, Charles R. Johnson, Lionel Levine, Elchannan Mossel, Yuval Peres, Darren Rhea, and Ilya Spitkovsky.

The mathematics department at the University of California, Berkeley deserves special thanks as does the National Science Foundation for believing in me enough to provide much needed funding. In addition, the comforting melodies of Belle and Sebastian will not be forgotten.

Finally, I would like to thank my parents for their unending support and love.

Notation

Most of the notation we use is standard. Our definitions will be *italicized* and we shall mottle the exposition with them; those that we feel are most important, and need special emphasis, will be given their own paragraphs. A field will usually be denoted by the letter K, and the algebraic closure of K is written $\overline{K}$. The nonnegative integers will be denoted by $\mathbb{N}$, while the positive integers are $\mathbb{Z}_+$. Additionally, positive real numbers are indicated by $\mathbb{R}_+$. Vectors, such as $\boldsymbol{x} = (x_1, \ldots, x_m) \in \mathbb{R}^m$, are typically displayed using a **boldface** font.

When there is no ambiguity in context, a matrix all of whose entries are zero will be simply written as 0. The conjugate transpose of a complex matrix A is denoted A^*. A *principal submatrix* of an $n \times n$ matrix A is gotten by selecting a submatrix with the same row and column selectors. A *leading principal submatrix* of A is a principal submatrix gotten by choosing row and column selectors that are contiguous and start with row and column 1. Given a product of matrices $P = A_1 \cdots A_k$ and an invertible matrix S, a *uniform similarity* of a product P (with respect to the A_i) is a rewriting, $SPS^{-1} = B_1 \cdots B_k$, in which each $B_i = SA_iS^{-1}$.

Let G be a group and R a ring. The (left) *group ring* of G over R will be denoted by $R[G]$, although sometimes it will be more notationally convenient to write this ring as RG.

Foreward

Mathematics first netted me with the lure of its problems. I soon learned, however, that significant progress is nearly impossible without piggybacking on the great discoveries of generations of mathematicians. Even so, I have always felt that the most interesting and beautiful questions are those that can be stated simply, offer an intellectual challenge, and whose implications can be held in one's own hand by way of examples.

Moreover, as isolated as mathematics is from the other realms of academic endeavor, it is made even more inscrutable by the fractious nature of its various disciplines. One must therefore form a compromise between depth of study and breadth of study. Of course, this is not to say that the first boundary engenders difficulty whereas the second, triviality.

In this regard, the reader will find, I feel, that I have chosen a happy medium. The mathematical background necessary to read this entire work is very modest, and it will, hopefully, appeal to a number of mathematicians, graduate students, and even upper-level undergraduates. At the same time, the problems we study are rich and complex, arising from disparate areas of mathematics.

Each chapter is essentially self-contained and can be read independently of any other. The reader is invited to skip around and find those problems that intrigue him or her the most. For the benefit of exposition, each chapter contains a section summarizing the requisite mathematical background.

The results of the first chapter represent joint research with Matthias Aschenbrenner [4]. The second and third chapters consist of work published in [25] and [24], respectively. Finally, chapter 4 is the result of collaboration with Scott Armstrong [3].

Chapter 1

Finite Generation of Symmetric Ideals

1.1 Introduction

A pervasive theme in invariant theory is that of finite generation. A fundamental example is a theorem of Hilbert stating that the invariant subrings of finite-dimensional polynomial algebras over finite groups are finitely generated [12, Corollary 1.5]. In this chapter, we study invariant ideals of infinite-dimensional polynomial rings. Of course, when the number of indeterminates is finite, Hilbert's basis theorem tells us that any ideal (invariant or not) is finitely generated.

Our setup is as follows. Let X be an infinite collection of indeterminates, and let $\mathfrak{S}_X$ be the group of permutations of X. Fix a commutative Noetherian ring A and let $R = A[X]$ be the polynomial ring in the indeterminates X. The group $\mathfrak{S}_X$ acts naturally on R: if $\sigma \in \mathfrak{S}_X$ and $f \in A[x_1, \ldots, x_n]$ where $x_i \in X$, then

$$\sigma f(x_1, x_2, \ldots, x_n) = f(\sigma x_1, \sigma x_2, \ldots, \sigma x_n) \in R.$$

This in turn gives R the structure of a left module over the (non-commutative) left group ring $R[\mathfrak{S}_X]$. An ideal $I \subseteq R$ is called *invariant under* $\mathfrak{S}_X$ (or simply *invariant*) if

$$\mathfrak{S}_X I := \{\sigma f : \sigma \in \mathfrak{S}_X, f \in I\} \subseteq I.$$

Notice that invariant ideals are simply the $R[\mathfrak{S}_X]$-submodules of R. We may now state our main result.

Theorem 1.1.1. *Every ideal of $R = A[X]$ invariant under $\mathfrak{S}_X$ is finitely generated as an $R[\mathfrak{S}_X]$-module.* (*Stated more succinctly, R is a Noetherian $R[\mathfrak{S}_X]$-module.*)

For the purposes of this work, we will use the following notation. Let B be a ring and let G be a subset of a B-module M. Then $\langle f : f \in G \rangle_B$ will denote the B-submodule of M generated by elements of G.

Example 1.1.2. *Suppose that $X = \{x_1, x_2, \dots\}$. The invariant ideal $I = \langle x_1, x_2, \dots \rangle_R$ is clearly not finitely generated over R, however, it does have the compact representation $I = \langle x_1 \rangle_{R[\mathfrak{S}_X]}$.*

The outline of this chapter is as follows. In Section 1.2, we define a partial order on monomials and show that it can be used to obtain a well-quasi-ordering of the monomials in R. Section 1.3 then goes on to detail our proof of Theorem 1.1.1, using the main result of Section 1.2 in a fundamental way. In the penultimate section, we discuss a relationship between invariant ideals of R and chains of increasing ideals in finite-dimensional polynomial rings. The notions introduced there provide a suitable framework for studying a problem arising from chemistry, the subject of the final section of this chapter.

1.2 The Symmetric Cancellation Ordering

We begin this section by briefly recalling some basic order-theoretic notions. We also discuss some fundamental results due to Higman and Nash-Williams and some of their consequences. We define the ordering mentioned in the section heading, and give a sufficient condition for it to be a well-quasi-ordering; this is needed in the proof of Theorem 1.1.1.

1.2.1 Preliminaries

A *quasi-ordering* on a set S is a binary relation $\leq$ on S which is reflexive and transitive. A *quasi-ordered set* is a pair $(S, \leq)$ consisting of a set S and a quasi-ordering $\leq$ on S.

When there is no confusion, we will omit $\leq$ from the notation, and simply call S a quasi-ordered set. If in addition the relation $\leq$ is *anti-symmetric* ($s \leq t \ \wedge \ t \leq s \Rightarrow s = t$, for all $s, t \in S$), then $\leq$ is called an *ordering* (sometimes also called a *partial ordering*) on the set S. The *trivial* ordering on S is given by $s \leq t \iff s = t$ for all $s, t \in S$. A quasi-ordering $\leq$ on a set S induces an ordering on the set $S/{\sim} = \{s/{\sim} : s \in S\}$ of equivalence classes of the equivalence relation $s \sim t \iff s \leq t \ \wedge \ t \leq s$ on S. If s and t are elements of a quasi-ordered set, we write as usual $s \leq t$ also as $t \geq s$, and we write $s < t$ if $s \leq t$ and $t \not\leq s$.

A map $\varphi \colon S \to T$ between quasi-ordered sets S and T is called *increasing* if $s \leq t \Rightarrow \varphi(s) \leq \varphi(t)$ for all $s, t \in S$, and *strictly increasing* if $s < t \Rightarrow \varphi(s) < \varphi(t)$ for all $s, t \in S$. We also say that $\varphi \colon S \to T$ is a *quasi-embedding* if $\varphi(s) \leq \varphi(t) \Rightarrow s \leq t$ for all $s, t \in S$.

An *antichain* of S is a subset $A \subseteq S$ such that $s \not\leq t$ and $t \not\leq s$ for all $s \not\sim t$ in A. A *final segment* of a quasi-ordered set $(S, \leq)$ is a subset $F \subseteq S$ which is closed upwards: $s \leq t \ \wedge \ s \in F \Rightarrow t \in F$, for all $s, t \in S$. We can view the set $\mathcal{F}(S)$ of final segments of S as an ordered set, with the ordering given by reverse inclusion. Given a subset M of S, the set $\bigl\{t \in S : \exists s \in M \text{ with } s \leq t\bigr\}$ is a final segment of S, the final segment *generated by M*. An *initial segment* of S is a subset of S whose complement is a final segment. An initial segment I of S is *proper* if $I \neq S$. For $a \in S$ we denote by $S^{\leq a}$ the initial segment consisting of all $s \in S$ with $s \leq a$.

A quasi-ordered set S is said to be *well-founded* if there is no infinite strictly decreasing sequence $s_1 > s_2 > \cdots$ in S, and *well-quasi-ordered* if in addition every antichain of S is finite. The following characterization of well-quasi-orderings is classical (see, for example, [38]). An infinite sequence $s_1, s_2, \ldots$ in S is called *good* if $s_i \leq s_j$ for some indices $i < j$, and *bad* otherwise.

Proposition 1.2.1. *The following are equivalent, for a quasi-ordered set S:*

(1) *S is well-quasi-ordered.*

(2) *Every infinite sequence in S is good.*

(3) *Every infinite sequence in S contains an infinite increasing subsequence.*

(4) *Any final segment of S is finitely generated.*

(5) $\big(\mathcal{F}(S),\supseteq\big)$ *is well-founded (i.e., the ascending chain condition holds for final segments of S).* □

Let $(S,\leq_S)$ and $(T,\leq_T)$ be quasi-ordered sets. If there exists an increasing surjection $S\to T$ and S is well-quasi-ordered, then T is well-quasi-ordered, and if there exists a quasi-embedding $S\to T$ and T is well-quasi-ordered, then so is S. Moreover, the cartesian product $S\times T$ can be turned into a quasi-orderd set by using the cartesian product of $\leq_S$ and $\leq_T$:

$$(s,t)\leq(s',t') \quad :\Longleftrightarrow \quad s\leq_S s'\wedge t\leq_T t', \qquad \text{for } s,s'\in S,\ t,t'\in T.$$

Using Proposition 1.2.1 we see that the cartesian product of two well-quasi-ordered sets is again well-quasi-ordered.

Of course, a total ordering $\leq$ is well-quasi-ordered if and only if it is well-founded; in this case $\leq$ is called a *well-ordering*. Every well-ordered set is isomorphic to a unique ordinal number, called its *order type*. The order type of $\mathbb{N}=\{0,1,2,\dots\}$ with its usual ordering is ω.

1.2.2 A lemma of Higman

Given a set X, we let X^* denote the set of all finite sequences of elements of X (including the empty sequence). We may think of the elements of X^* as *non-commutative words* $x_1\cdots x_m$ with letters $x_1,\dots,x_m$ coming from the alphabet X. With the concatenation of such words as operation, X^* is the free monoid generated by X. A quasi-ordering $\leq$ on X yields a quasi-ordering $\leq_{\mathrm{H}}$ (the *Higman quasi-ordering*) on X^* as follows:

$$x_1\cdots x_m\leq_{\mathrm{H}} y_1\cdots y_n \quad :\Longleftrightarrow \quad \left\{\begin{array}{l}\text{there exists a strictly increasing func-}\\ \text{tion } \varphi\colon\{1,\dots,m\}\to\{1,\dots,n\} \text{ such}\\ \text{that } x_i\leq y_{\varphi(i)} \text{ for all } 1\leq i\leq m.\end{array}\right.$$

If $\leq$ is an ordering on X, then $\leq_{\mathrm{H}}$ is an ordering on X^*. The following fact was shown by Higman [23] (with an ingenious proof due to Nash-Williams [49]):

Lemma 1.2.2. *If $\leq$ is a well-quasi-ordering on X, then $\leq_{\mathrm{H}}$ is a well-quasi-ordering on X^*.* □

It follows that if $\leq$ is a well-quasi-ordering on X, then the quasi-ordering $\leq^*$ on X^* defined by

$$x_1 \cdots x_m \leq^* y_1 \cdots y_n \quad :\Longleftrightarrow \quad \begin{cases} \text{there exists an injective} \\ \text{function } \varphi\colon \{1,\dots,m\} \to \\ \{1,\dots,n\} \text{ such that } x_i \leq y_{\varphi(i)} \\ \text{for all } 1 \leq i \leq m \end{cases}$$

is also a well-quasi-ordering. (Since $\leq^*$ extends $\leq_{\mathrm{H}}$.)

We also let $X^\diamond$ be the set of *commutative words* in the alphabet X, that is, the free commutative monoid generated by X (with identity element denoted by 1). We sometimes also refer to the elements of $X^\diamond$ as *monomials* (in the set of indeterminates X). We have a natural surjective monoid homomorphism $\pi\colon X^* \to X^\diamond$ given by simply "making the indeterminates commute" (i.e., interpreting a non-commutative word from X^* as a commutative word in $X^\diamond$). Unlike $\leq_{\mathrm{H}}$, the quasi-ordering $\leq^*$ is compatible with π in the sense that $v \leq^* w \Rightarrow v' \leq^* w'$ for all $v, v', w, w' \in X^*$ with $\pi(v) = \pi(v')$ and $\pi(w) = \pi(w')$. Hence $\pi(v) \leq^\diamond \pi(w) :\Longleftrightarrow v \leq^* w$ defines a quasi-ordering $\leq^\diamond$ on $X^\diamond = \pi(X^*)$ making π an increasing map. The quasi-ordering $\leq^\diamond$ extends the divisibility relation in the monoid $X^\diamond$:

$$v|w \quad :\Longleftrightarrow \quad uv = w \text{ for some } u \in X^\diamond.$$

If we take for $\leq$ the trivial ordering on X, then $\leq^\diamond$ corresponds exactly to divisibility in $X^\diamond$, and this ordering is a well-quasi-ordering if and only if X is finite. In general we have, as an immediate consequence of Higman's lemma (since π is a surjection):

Corollary 1.2.3. *If $\leq$ is a well-quasi-ordering on the set X, then $\leq^\diamond$ is a well-quasi-ordering on $X^\diamond$.* □

1.2.3 A theorem of Nash-Williams

Given a totally ordered set S and a quasi-ordered set X, we denote by $\mathrm{Fin}(S, X)$ the set of all functions $f\colon I \to X$, where I is a proper initial segment of S, whose range $f(I)$ is *finite.* We define a quasi-ordering $\leq_{\mathrm{H}}$ on $\mathrm{Fin}(S, X)$ as follows: for $f\colon I \to X$ and

$g\colon J \to X$ from $\mathrm{Fin}(S,X)$ put

$$f \leq_{\mathrm{H}} g \quad :\Longleftrightarrow \quad \begin{cases} \text{there exists a strictly increasing function} \\ \varphi\colon I \to J \text{ such that } f(i) \leq g(\varphi(i)) \text{ for all } i \in I. \end{cases}$$

We may think of an element of $\mathrm{Fin}(S,X)$ as a sequence of elements of X indexed by indices in some proper intial segment of S. So for $S = \mathbb{N}$ with its usual ordering, we can identify elements of $\mathrm{Fin}(\mathbb{N},X)$ with words in X^*, and then $\leq_{\mathrm{H}}$ for $\mathrm{Fin}(\mathbb{N},X)$ agrees with $\leq_{\mathrm{H}}$ on X^* as defined above. We will have occasion to use a far-reaching generalization of Lemma 1.2.2:

Theorem 1.2.4. *If X is well-quasi-ordered and S is well-ordered, then* $\mathrm{Fin}(S,X)$ *is well-quasi-ordered.* □

This theorem was proved by Nash-Williams [50]; special cases were shown earlier in [13, 48, 53].

1.2.4 Term orderings

A *term ordering* of $X^\diamond$ is a well-ordering $\leq$ of $X^\diamond$ such that

(1) $1 \leq x$ for all $x \in X$, and

(2) $v \leq w \Rightarrow xv \leq xw$ for all $v, w \in X^\diamond$ and $x \in X$.

Every ordering $\leq$ of $X^\diamond$ satisfying (1) and (2) extends the ordering $\leq^\diamond$ obtained from the restriction of $\leq$ to X. In particular, $\leq$ extends the divisibility ordering on $X^\diamond$. By Corollary 1.2.3 above, a total ordering $\leq$ of $X^\diamond$ which satisfies (1) and (2) is a term ordering if and only if its restriction to X is a well-ordering.

Example 1.2.5. *Let $\leq$ be a total ordering of X. We define the induced* lexicographic ordering $\leq_{\mathrm{lex}}$ *of monomials as follows: given $v, w \in X^\diamond$ we can write $v = x_1^{a_1} \cdots x_n^{a_n}$ and $w = x_1^{b_1} \cdots x_n^{b_n}$ with $x_1 < \cdots < x_n$ in X and all $a_i, b_i \in \mathbb{N}$; then*

$$v \leq_{lex} w \quad :\Longleftrightarrow \quad (a_n, \dots, a_1) \leq (b_n, \dots, b_1) \text{ lexicographically (from the left).}$$

The ordering $\leq_{\mathrm{lex}}$ is total and satisfies (1), (2); hence if the ordering $\leq$ of X is a well-ordering, then $\leq_{\mathrm{lex}}$ is a term ordering of $X^\diamond$.

Remark 1.2.6. Let $\leq$ be a total ordering of X. For $w \in X^\diamond$, $w \neq 1$, we let

$$|w| := \max\{x \in X : x|w\} \quad \text{(with respect to } \leq\text{)}.$$

We also put $|1| := -\infty$ where we set $-\infty < x$ for all $x \in X$. One of the perks of using the lexicographic ordering as a term ordering on $X^\diamond$ is that if v and w are monomials with $v \leq_{\text{lex}} w$, then $|v| \leq |w|$. Below, we often use this observation.

The previous example shows that for every set X there exists a term ordering of $X^\diamond$, since every set can be well-ordered by the Axiom of Choice. In fact, every set X can be equipped with a well-ordering every proper initial segment of which has strictly smaller cardinality than X; in other words, the order type of this ordering (a certain ordinal number) is a cardinal number. We shall call such an ordering of X a *cardinal well-ordering* of X.

Lemma 1.2.7. *Let X be a set equipped with a cardinal well-ordering, and let I be a proper initial segment of X. Then every injective function $I \to X$ can be extended to a permutation of X.*

Proof. Since this is clear if X is finite, suppose that X is infinite. Let $\varphi\colon I \to X$ be injective. Since I has cardinality $|I| < |X|$ and X is infinite, we have $|X| = \max\{|X \setminus I|, |I|\} = |X \setminus I|$. Similarly, since $|\varphi(I)| = |I| < |X|$, we also have $|X \setminus \varphi(I)| = |X|$. Hence there exists a bijection $\psi\colon X \setminus I \to X \setminus \varphi(I)$. Combining φ and ψ yields a permutation of X as desired. □

1.2.5 A new ordering of monomials

Let G be a permutation group on a set X, that is, a group G together with a faithful action $(\sigma, x) \mapsto \sigma x\colon G \times X \to X$ of G on X. The action of G on X extends in a natural way to a faithful action of G on $X^\diamond$: $\sigma w = \sigma x_1 \cdots \sigma x_n$ for $\sigma \in G$, $w = x_1 \cdots x_n \in X^\diamond$. Given a term ordering $\leq$ of $X^\diamond$, we define a new relation on $X^\diamond$ as follows:

Definition 1.2.8. (The symmetric cancellation ordering corresponding to G and $\leq$.)

$$v \preceq w \quad :\Longleftrightarrow \quad \begin{cases} v \leq w \text{ and there exist } \sigma \in G \text{ and a mono-} \\ \text{mial } u \in X^\diamond \text{ such that } w = u\sigma v \text{ and for} \\ \text{all } v' \leq v, \text{ we have } u\sigma v' \leq w. \end{cases}$$

Remark 1.2.9. Every term ordering $\leq$ is *linear*: $v \leq w \iff uv \leq uw$ for all monomials u, v, w. Hence the condition above may be rewritten as: $v \leq w$ and there exists $\sigma \in G$ such that $\sigma v | w$ and $\sigma v' \leq \sigma v$ for all $v' \leq v$. (We say that "σ witnesses $v \preceq w$.")

Example 1.2.10. *Let $X = \{x_1, x_2, \ldots\}$ be a countably infinite set of indeterminates, ordered such that $x_1 < x_2 < \cdots$, and let $\leq \, = \, \leq_{\text{lex}}$ be the corresponding lexicographic ordering of $X^\diamond$. Let also G be the group of permutations of $\{1, 2, 3, \ldots\}$, acting on X via $\sigma x_i = x_{\sigma(i)}$. As an example of the relation $\preceq$, consider the following chain:*

$$x_1^2 \preceq x_1 x_2^2 \preceq x_1^3 x_2 x_3^2.$$

To verify the first inequality, notice that $x_1 x_2^2 = x_1 \sigma(x_1^2)$, in which σ is the transposition $(1\,2)$. If $v' = x_1^{a_1} \cdots x_n^{a_n} \leq x_1^2$ with $a_1, \ldots, a_n \in \mathbb{N}$, $a_n > 0$, then it follows that $n = 1$ and $a_1 \leq 2$. In particular, $x_1 \sigma v' = x_1 x_2^{a_1} \leq x_1 x_2^2$. For the second relationship, we have that $x_1^3 x_2 x_3^2 = x_1^3 \tau(x_1 x_2^2)$, in which τ is the cycle $(1\,2\,3)$. Additionally, if $v' = x_1^{a_1} \cdots x_n^{a_n} \leq x_1 x_2^2$ with $a_1, \ldots, a_n \in \mathbb{N}$, $a_n > 0$, then $n \leq 2$, and if $n = 2$, then either $a_2 = 1$ or $a_2 = 2$, $a_1 \leq 1$. In each case we get $x_1^3 \tau v' = x_1^3 x_2^{a_1} x_3^{a_2} \leq x_1^3 x_2 x_3^2$.

Although Definition 1.2.8 appears technical, we will soon present a nice interpretation of it that involves leading term cancellation of polynomials. First we verify that it is indeed an ordering.

Lemma 1.2.11. *The relation $\preceq$ is an ordering on monomials.*

Proof. First notice that $w \preceq w$ since we may take $u = 1$ and σ to be the identity permutation. Next, suppose that $u \preceq v \preceq w$. Then there exist permutations σ, τ in G and monomials u_1, u_2 in $X^\diamond$ such that $v = u_1 \sigma u$, $w = u_2 \tau v$. In particular, $w = u_2(\tau u_1)(\tau\sigma u)$. Additionally, if $v' \leq u$, then $u_1 \sigma v' \leq v$, so that $u_2 \tau(u_1 \sigma v') \leq w$ (since $\leq$ is a term ordering). It follows that $u_2(\tau u_1)(\tau \sigma v') \leq w$. This shows transitivity; anti-symmetry of $\preceq$ follows from anti-symmetry of $\leq$. □

We offer a useful interpretation of this ordering (which motivates its name). We fix a commutative ring A and let $R = A[X]$ be the ring of polynomials with coefficients from A in the collection of commuting indeterminates X. Its elements may be written uniquely in the form

$$f = \sum_{w \in X^\diamond} a_w w$$

where $a_w \in A$ for all $w \in X^\diamond$, and all but finitely many a_w are zero. We say that a monomial w *occurs* in f if $a_w \neq 0$. Given a nonzero $f \in R$ we define $\mathrm{lm}(f)$, the *leading monomial* of f (with respect to our choice of term ordering $\leq$) to be the largest monomial w (with respect to $\leq$) which occurs in f. If $w = \mathrm{lm}(f)$, then a_w is the *leading coefficient* of f, denoted by $\mathrm{lc}(f)$, and $a_w w$ is the *leading term* of f, denoted by $\mathrm{lt}(f)$. By convention, we set $\mathrm{lm}(0) = \mathrm{lc}(0) = \mathrm{lt}(0) = 0$. We let $R[G]$ be the (left) group ring of G over R (with multiplication given by $f\sigma \cdot g\tau = fg(\sigma\tau)$ for $f, g \in R$, $\sigma, \tau \in G$), and we view R as a left $R[G]$-module in the natural way.

Lemma 1.2.12. *Let $f \in R$, $f \neq 0$, and $u, w \in X^\diamond$. Suppose that $\sigma \in G$ witnesses $\mathrm{lm}(f) \preceq w$, and let $u \in X^\diamond$ with $u\sigma \,\mathrm{lm}(f) = w$. Then $\mathrm{lm}(u\sigma f) = u\sigma \,\mathrm{lm}(f)$.*

Proof. Put $v = \mathrm{lm}(f)$. Every monomial occurring in $u\sigma f$ has the form $u\sigma v'$, where v' occurs in f. Hence $v' \leq v$, and since σ witnesses $v \preceq w$, this yields $u\sigma v' \leq w$. □

Suppose that A is a field, let $v \preceq w$ be in $X^\diamond$, and let f, g be two polynomials in R with leading monomials v, w, respectively. Then, from the definition and the lemma above, there exists a $\sigma \in G$ and a term cu ($c \in A \setminus \{0\}$, $u \in X^\diamond$) such that all monomials occurring in

$$h = g - cu\sigma f$$

are strictly smaller (with respect to $\leq$) than w. For readers familiar with the theory of Gröbner bases, the polynomial h can be viewed as a kind of symmetric version of the S-polynomial (see, for instance, [12, Chapter 15]).

Example 1.2.13. *In the situation of Example 1.2.10 above, let $f = x_1x_2^2 + x_2 + x_1^2$ and $g = x_1^3x_2x_3^2 + x_3^2 + x_1^4x_3$. Set $\sigma = (1\,2\,3)$, and observe that*

$$g - x_1^3\sigma f = x_1^4x_3 + x_3^2 - x_1^3x_3 - x_1^3x_2^2$$

has a smaller leading monomial than g.

We are mostly interested in the case where our term ordering on $X^\diamond$ is $\leq_{\mathrm{lex}}$, and $G = \mathfrak{S}_X$. Under these assumptions we have:

Lemma 1.2.14. *Let $v, w \in X^\diamond$ with $v \preceq w$. Then for every $\sigma \in \mathfrak{S}_X$ witnessing $v \preceq w$ we have $\sigma(X^{\leq |v|}) \subseteq X^{\leq |w|}$. Moreover, if the order type of $(X, \leq)$ is $\leq \omega$, then we can choose such σ with the additional property that $\sigma(x) = x$ for all $x > |w|$.*

Proof. To see the first claim, suppose for a contradiction that $\sigma x > |w|$ for some $x \in X$, $x \leq |v|$. We have $\sigma v | w$, so if $x | v$, then $\sigma x | w$, contradicting $\sigma x > |w|$. In particular $x < |v|$, which yields $x <_{\text{lex}} v$ and thus $\sigma x \leq_{\text{lex}} \sigma v \leq_{\text{lex}} w$, again contradicting $\sigma x > |w|$. Now suppose that the order type of X is $\leq \omega$, and let σ witness $v \preceq w$. Then $|v| \leq |w|$, and $\sigma \restriction X^{\leq |v|}$ can be extended to a permutation σ' of the finite set $X^{\leq |w|}$. We further extend σ' to a permutation of X by setting $\sigma'(x) = x$ for all $x > |w|$. One checks easily that σ' still witnesses $v \preceq w$. □

1.2.6 Lovely orderings

We say that a term ordering $\leq$ of $X^\diamond$ is *lovely* for G if the corresponding symmetric cancellation ordering $\preceq$ on $X^\diamond$ is a well-quasi-ordering. If $\leq$ is lovely for a subgroup of G, then $\leq$ is lovely for G.

Example 1.2.15. *The symmetric cancellation ordering corresponding to $G = \{1\}$ and a given term ordering $\leq$ of $X^\diamond$ is just*

$$v \preceq w \quad \Longleftrightarrow \quad v \leq w \ \wedge \ v | w.$$

Hence a term ordering of $X^\diamond$ is lovely for $G = \{1\}$ if and only if divisibility in $X^\diamond$ has no infinite antichains; that is, exactly if X is finite.

This terminology is inspired by the following definition from [7] (which in turn goes back to an idea in [2]):

Definition 1.2.16. Given an ordering $\leq$ of X, consider the following ordering of X:

$$x \sqsubseteq y \quad :\Longleftrightarrow \quad \begin{cases} x \leq y \text{ and there exists } \sigma \in G \text{ such that} \\ \sigma x = y \text{ and for all } x' \leq x, \text{ we have } \sigma x' \leq y. \end{cases}$$

A well-ordering $\leq$ of X is called *nice* (for G) if $\sqsubseteq$ is a well-quasi-ordering.

In [2] one finds various examples of nice orderings, and in [7] it is shown that if X admits a nice ordering with respect to G, then for every field F, the free F-module

FX with basis X is Noetherian as a module over $F[G]$. It is clear that the restriction to X of a lovely ordering of $X^\diamond$ is nice. However, there do exist permutation groups (G, X) for which X admits a nice ordering, but $X^\diamond$ does not admit a lovely ordering; see Example 1.3.4 and Proposition 1.5.2 below.

Example 1.2.17. *Suppose that X is countable. Then every well-ordering of X of order type ω is nice for $\mathfrak{S}_X$. To see this, we may assume that $X = \mathbb{N}$ with its usual ordering. It is then easy to see that if $x \leq y$ in $\mathbb{N}$, then $x \sqsubseteq y$, witnessed by any extension σ of the strictly increasing map $n \mapsto n + y - x \colon \mathbb{N}^{\leq x} \to \mathbb{N}$ to a permutation of $\mathbb{N}$.*

The following crucial fact (generalizing the last example) is needed for our proof of Theorem 1.1.1:

Theorem 1.2.18. *The lexicographic ordering of $X^\diamond$ corresponding to a cardinal well-ordering of a set X is lovely for the full symmetric group $\mathfrak{S}_X$ of X.*

For the proof, let as above $\operatorname{Fin}(X, \mathbb{N})$ be the set of all sequences in $\mathbb{N}$ indexed by elements in some proper initial segment of X which have finite range, quasi-ordered by $\leq_{\mathrm{H}}$. For a monomial $w \neq 1$ we define $w^* \colon X^{\leq |w|} \to \mathbb{N}$ by

$$w^*(x) := \max\{a \in \mathbb{N} : x^a | w\}.$$

Then clearly $w^* \in \operatorname{Fin}(X, \mathbb{N})$, in fact, $w^*(x) = 0$ for all but finitely many $x \in X^{\leq |w|}$. We also let $1^* :=$ the empty sequence $\emptyset \to \mathbb{N}$ (the unique smallest element of $\operatorname{Fin}(X, \mathbb{N})$). We now quasi-order $X^\diamond \times \operatorname{Fin}(X, \mathbb{N})$ by the cartesian product of the ordering $\leq_{\mathrm{lex}}$ on $X^\diamond$ and the quasi-ordering $\leq_{\mathrm{H}}$ on $\operatorname{Fin}(X, \mathbb{N})$. By Corollary 1.2.3, Theorem 1.2.4, and the remark following Proposition 1.2.1, $X^\diamond \times \operatorname{Fin}(X, \mathbb{N})$ is well-quasi-ordered. Therefore, in order to finish the proof of Theorem 1.2.18, it suffices to show:

Lemma 1.2.19. *The map*

$$w \mapsto (w, w^*) \colon X^\diamond \to X^\diamond \times \operatorname{Fin}(X, \mathbb{N})$$

is a quasi-embedding with respect to the symmetric cancellation ordering on $X^\diamond$ and the quasi-ordering on $X^\diamond \times \operatorname{Fin}(X, \mathbb{N})$.

Proof. Suppose that v, w are monomials with $v \leq_{\mathrm{lex}} w$ and $v^* \leq_{\mathrm{H}} w^*$; we need to show that $v \preceq w$. For this we may assume that $v, w \neq 1$. So there exists a strictly increasing function $\varphi\colon X^{\leq |v|} \to X^{\leq |w|}$ such that

$$v^*(x) \leq w^*(\varphi(x)) \qquad \text{for all } x \in X \text{ with } x \leq |v|. \tag{1.2.1}$$

By Lemma 1.2.7 there exists $\sigma \in \mathfrak{S}_X$ such that $\sigma \restriction X^{\leq |v|} = \varphi \restriction X^{\leq |v|}$. Then clearly $\sigma v | w$ by (1.2.1). Now let $v' \leq_{\mathrm{lex}} v$; we claim that $\sigma v' \leq_{\mathrm{lex}} \sigma v$. Again we may assume $v' \neq 1$. Then $|v'| \leq |v|$, hence we may write

$$v' = x_1^{a_1} \cdots x_n^{a_n}, \quad v = x_1^{b_1} \cdots x_n^{b_n}$$

with $x_1 < \cdots < x_n \leq |v|$ in X and $a_i, b_j \in \mathbb{N}$. Put $y_1 := \varphi(x_1), \dots, y_n := \varphi(x_n)$. Then $y_1 < \cdots < y_n$ and

$$\sigma v' = y_1^{a_1} \cdots y_n^{a_n}, \quad \sigma v = y_1^{b_1} \cdots y_n^{b_n},$$

and therefore $\sigma v' \leq_{\mathrm{lex}} \sigma v$ as required. □

1.2.7 The case of countable X

In Section 4 we will apply Theorem 1.2.18 in the case where X is countable. Then the order type of X is at most ω, and in the proof of the theorem given above we only need to appeal to a special instance (Higman's Lemma) of Theorem 1.2.4. We finish this section by giving a self-contained proof of this important special case of Theorem 1.2.18, avoiding Theorem 1.2.4. Let $\mathfrak{S}_{(X)}$ denote the subgroup of $\mathfrak{S}_X$ consisting of all $\sigma \in \mathfrak{S}_X$ with the property that $\sigma(x) = x$ for all but finitely many letters $x \in X$.

Theorem 1.2.20. *The lexicographic ordering of $X^\diamond$ corresponding to a cardinal well-ordering of a countable set X is lovely for $\mathfrak{S}_{(X)}$.*

Let X be countable and let $\leq$ be a cardinal well-ordering of X. Enumerate the elements of X as $x_1 < x_2 < \cdots$. We assume that X is infinite; this is not a restriction, since by Lemma 1.2.14 we have:

Lemma 1.2.21. *If the lexicographic ordering of $X^\diamond$ is lovely for $\mathfrak{S}_{(X)}$, then for any n and $X_n := \{x_1, \dots, x_n\}$, the lexicographic ordering of $(X_n)^\diamond$ is lovely for $\mathfrak{S}_{X_n}$.* □

We begin with some preliminary lemmas. Here, $\preceq$ is the symmetric cancellation ordering corresponding to $\mathfrak{S}_{(X)}$ and $\leq_{\text{lex}}$. We identifty $\mathfrak{S}_{(X)}$ and $\mathfrak{S}_\infty := \mathfrak{S}_{(\mathbb{N})}$ in the natural way, and for every n we regard $\mathfrak{S}_n$, the group of permutations of $\{1, 2, \ldots, n\}$, as a subgroup of $\mathfrak{S}_\infty$; then $\mathfrak{S}_n \leq \mathfrak{S}_{n+1}$ for each n, and $\mathfrak{S}_\infty = \bigcup_n \mathfrak{S}_n$.

Lemma 1.2.22. *Suppose that $x_1^{a_1} \cdots x_n^{a_n} \preceq x_1^{b_1} \cdots x_n^{b_n}$ where $a_i, b_j \in \mathbb{N}$, $b_n > 0$. Then for any $c \in \mathbb{N}$ we have $x_1^{a_1} \cdots x_n^{a_n} \preceq x_1^c x_2^{b_1} \cdots x_{n+1}^{b_n}$.*

Proof. Let $v := x_1^{a_1} \cdots x_n^{a_n}$, $w := x_1^{b_1} \cdots x_n^{b_n}$. We may assume $v \neq 1$. Clearly $v \leq_{\text{lex}} w$ and $b_n > 0$ yield $x_1^{a_1} \cdots x_n^{a_n} \leq_{\text{lex}} x_1^c x_2^{b_1} \cdots x_{n+1}^{b_n}$. Let now $\sigma \in \mathfrak{S}_\infty$ witness $v \preceq w$. Let τ be the cyclic permutation $\tau = (1\,2\,3 \cdots (n+1))$ and set $\hat{\sigma} := \tau\sigma$. Then $\sigma v | w$ yields $\hat{\sigma} v | \tau w$, hence $\hat{\sigma} v | x_1^c \tau w = x_1^c x_2^{b_1} \cdots x_{n+1}^{b_n}$. Next, suppose that $v' \leq_{\text{lex}} v$; then $\sigma v' \leq_{\text{lex}} \sigma v$. By Lemma 1.2.14 and the nature of τ, the map $\tau \restriction \sigma(\{1, \ldots, |v|\})$ is strictly increasing, which gives $\hat{\sigma} v' = \tau\sigma v' \leq_{\text{lex}} \tau\sigma v = \hat{\sigma} v$. Therefore, $\hat{\sigma}$ witnesses $x_1^{a_1} \cdots x_n^{a_n} \preceq x_1^c x_2^{b_1} \cdots x_{n+1}^{b_n}$. □

Lemma 1.2.23. *If $x_1^{a_1} \cdots x_n^{a_n} \preceq x_1^{b_1} \cdots x_n^{b_n}$, where $a_i, b_j \in \mathbb{N}$, $b_n > 0$, and $a, b \in \mathbb{N}$ are such that $a \leq b$, then $x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n} \preceq x_1^b x_2^{b_1} \cdots x_{n+1}^{b_{n+1}}$.*

Proof. As before let $v := x_1^{a_1} \cdots x_n^{a_n}$, $w := x_1^{b_1} \cdots x_n^{b_n}$. Once again, we may assume $v \neq 1$, and it is clear that $x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n} \leq_{\text{lex}} x_1^b x_2^{b_1} \cdots x_{n+1}^{b_{n+1}}$. Let $\sigma \in \mathfrak{S}_\infty$ witness $v \preceq w$. By Lemma 1.2.14 we may assume that $\sigma(x_i) = x_i$ for all $i > n$. Let τ be the cyclic permutation $\tau = (1\,2 \cdots (n+1))$. Setting $\hat{\sigma} = \tau\sigma\tau^{-1}$, we have $\hat{\sigma} x_1 = x_1$, and hence

$$\hat{\sigma}(x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n}) = \hat{\sigma}(x_1^a)\hat{\sigma}(x_2^{a_1} \cdots x_{n+1}^{a_n}) = x_1^a \tau\sigma v. \tag{1.2.2}$$

Since $\sigma v | w$, this last expression divides $x_1^b \tau w = x_1^b x_2^{b_1} \cdots x_{n+1}^{b_n}$. Suppose that $v' = x_1^{c_1} \cdots x_{n+1}^{c_{n+1}} \leq_{\text{lex}} x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n}$, where $c_i \in \mathbb{N}$. Then, since we are using lexicographic order, we have

$$x_2^{c_2} \cdots x_{n+1}^{c_{n+1}} \leq_{\text{lex}} x_2^{a_1} \cdots x_{n+1}^{a_n}$$

and therefore

$$\tau^{-1}(x_2^{c_2} \cdots x_{n+1}^{c_{n+1}}) = x_1^{c_2} \cdots x_n^{c_{n+1}} \leq_{\text{lex}} \tau^{-1}(x_2^{a_1} \cdots x_{n+1}^{a_n}) = v.$$

By assumption, this implies that $\sigma\tau^{-1}(x_2^{c_2} \cdots x_{n+1}^{c_{n+1}}) \leq_{\text{lex}} \sigma v$ and thus by (1.2.2)

$$\hat{\sigma}(x_2^{c_2} \cdots x_{n+1}^{c_{n+1}}) \leq_{\text{lex}} \tau\sigma v = \hat{\sigma}(x_2^{a_1} \cdots x_{n+1}^{a_n}).$$

If this inequality is strict, then since $1 \notin \hat{\sigma}\big(\{2, \ldots, n+1\}\big)$, clearly

$$\hat{\sigma} v' = x_1^{c_1} \hat{\sigma}(x_2^{c_2} \cdots x_{n+1}^{c_{n+1}}) <_{\text{lex}} x_1^a \tau \sigma v = \hat{\sigma}(x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n}).$$

Otherwise, we have $x_2^{c_2} \cdots x_{n+1}^{c_{n+1}} = x_2^{a_1} \cdots x_{n+1}^{a_n}$ so that $c_1 \leq a$. In this case we still have $\hat{\sigma} v' \leq_{\text{lex}} \hat{\sigma}(x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n})$. It follows that $\hat{\sigma}$ witnesses $x_1^a x_2^{a_1} \cdots x_{n+1}^{a_n} \preceq x_1^b x_2^{b_1} \cdots x_{n+1}^{b_{n+1}}$. This completes the proof. □

We now have enough to show Theorem 1.2.20. The proof uses the basic idea from Nash-Williams' proof [50] of Higman's lemma. Assume for the sake of contradiction that there exists a bad sequence

$$w^{(1)}, w^{(2)}, \ldots, w^{(n)}, \ldots \qquad \text{in } X^\diamond.$$

For $w \in X^\diamond \setminus \{1\}$ let $j(w)$ be the index $j \geq 1$ with $|w| = x_j$, and put $j(1) := 0$. We may assume that the bad sequence is chosen in such a way that for every n, $j(w^{(n)})$ is *minimal* among the $j(w)$, where w ranges over all elements of $X^\diamond$ with the property that $w^{(1)}, w^{(2)}, \ldots, w^{(n-1)}, w$ can be continued to a bad sequence in $X^\diamond$. Because $1 \leq_{\text{lex}} w$ for all $w \in X^\diamond$, we have $j(w^{(n)}) > 0$ for all n. For every $n > 0$, write $w^{(n)} = x_1^{a^{(n)}} v^{(n)}$ with $a^{(n)} \in \mathbb{N}$ and $v^{(n)} \in X^\diamond$ not divisible by x_1. Since $\mathbb{N}$ is well-ordered, there is an infinite sequence $1 \leq i_1 < i_2 < \cdots$ of indices such that $a^{(i_1)} \leq a^{(i_2)} \leq \cdots$. Consider the monoid homomorphism $\alpha \colon X^\diamond \to X^\diamond$ given by $\alpha(x_{i+1}) = x_i$ for all $i > 1$. Then $j(\alpha(w)) = j(w) - 1$ if $w \neq 1$. Hence by minimality of $w^{(1)}, w^{(2)}, \ldots$, the sequence

$$w^{(1)}, w^{(2)}, \ldots, w^{(i_1 - 1)}, \alpha(v^{(i_1)}), \alpha(v^{(i_2)}), \ldots, \alpha(v^{(i_n)}), \ldots$$

is good; that is, there exist $j < i_1$ and k with $w^{(j)} \preceq \alpha(v^{(i_k)})$, or there exist $k < l$ with $\alpha(v^{(i_k)}) \preceq \alpha(v^{(i_l)})$. In the first case we have $w^{(j)} \preceq w^{(i_k)}$ by Lemma 1.2.22; and in the second case, $w^{(i_k)} \preceq w^{(i_l)}$ by Lemma 1.2.23. This contradicts the badness of our sequence $w^{(1)}, w^{(2)}, \ldots$, finishing the proof.

Question 1.2.24. Careful inspection of the proof of Theorem 1.2.18 (in particular Lemma 1.2.7) shows that in the statement of the theorem, we can replace $\mathfrak{S}_X$ by its subgroup consisting of all σ with the property that the set of $x \in X$ with $\sigma(x) \neq x$ has cardinality $< |X|$. In Theorem 1.2.18, can one always replace $\mathfrak{S}_X$ by $\mathfrak{S}_{(X)}$?

1.3 Proof of the Finiteness Theorem

We now come to the proof our main result. Throughout this section we let A be a commutative Noetherian ring, X an arbitrary set, $R = A[X]$, and we let G be a permutation group on X. An $R[G]$-submodule of R will be called a *G-invariant ideal* of R, or simply an *invariant ideal*, if G is understood. We will show:

Theorem 1.3.1. *If $X^\diamond$ admits a lovely term ordering for G, then R is Noetherian as an $R[G]$-module.*

For $G = \{1\}$ and X finite, this theorem reduces to Hilbert's basis theorem, by Example 1.2.15. We also obtain Theorem 1.1.1:

Corollary 1.3.2. *The $R[\mathfrak{S}_X]$-module R is Noetherian.*

Proof. Choose a cardinal well-ordering of X. Then the corresponding lexicographic ordering of $X^\diamond$ is lovely for $\mathfrak{S}_X$, by Theorem 1.2.18. Apply Theorem 1.3.1. □

Remark 1.3.3. It is possible to replace the use of Theorem 1.2.18 in the proof of the corollary above by the more elementary Theorem 1.2.20. This is because if the $R[\mathfrak{S}_X]$-module R was not Noetherian, then one could find a *countably generated* $R[\mathfrak{S}_X]$-submodule of R which is not finitely generated, and hence a countable subset X' of X such that $R' = A[X']$ is not a Noetherian $R'[\mathfrak{S}_{X'}]$-module.

The following example shows how the conclusion of Theorem 1.3.1 may fail:

Example 1.3.4. *Suppose that G has a cyclic subgroup H which acts freely and transitively on X. Then X has a nice ordering (see [2]), but $R = \mathbb{Q}[X^\diamond]$ is not Noetherian. To see this let σ be a generator for H, and let $x \in X$ be arbitrary. Then the $R[G]$-submodule of $R = \mathbb{Q}[X^\diamond]$ generated by the elements $\sigma^n x \sigma^{-n} x$ ($n \in \mathbb{N}$) is not finitely generated. So by Theorem 1.3.1, $X^\diamond$ does not admit a lovely term ordering for G.*

For the proof of Theorem 1.3.1 we develop a bit of Gröbner basis theory for the $R[G]$-module R. For the time being, we fix an arbitrary term ordering $\leq$ (not necessarily lovely for G) of $X^\diamond$.

1.3.1 Reduction of polynomials

Let $f \in R$, $f \neq 0$, and let B be a set of nonzero polynomials in R. We say that f is *reducible by* B if there exist pairwise distinct $g_1, \dots, g_m \in B$, $m \geq 1$, such that for each i we have $\operatorname{lm}(g_i) \preceq \operatorname{lm}(f)$, witnessed by some $\sigma_i \in G$, and

$$\operatorname{lt}(f) = a_1 w_1 \sigma_1 \operatorname{lt}(g_1) + \cdots + a_m w_m \sigma_m \operatorname{lt}(g_m)$$

for nonzero $a_i \in A$ and monomials $w_i \in X^\diamond$ such that $w_i \sigma_i \operatorname{lm}(g_i) = \operatorname{lm}(f)$. In this case we write $f \xrightarrow[B]{} h$, where

$$h = f - \bigl(a_1 w_1 \sigma_1 g_1 + \cdots + a_m w_m \sigma_m g_m\bigr),$$

and we say that f *reduces to* h by B. We say that f is *reduced* with respect to B if f is not reducible by B. By convention, the zero polynomial is reduced with respect to B. Trivially, every element of B reduces to 0.

Example 1.3.5. *Suppose that A is a field. Then f is reducible by B if and only if there exists some $g \in B$ such that $\operatorname{lm}(g) \preceq \operatorname{lm}(f)$.*

Example 1.3.6. *Suppose that f is reducible by B as defined (for finite X) in, say, [1, Chapter 4], that is: there exist $g_1, \dots, g_m \in B$ and $a_1, \dots, a_m \in A$ ($m \geq 1$) such that $\operatorname{lm}(g_i) | \operatorname{lm}(f)$ for all i and*

$$\operatorname{lc}(f) = a_1 \operatorname{lc}(g_1) + \cdots + a_m \operatorname{lc}(g_m).$$

Then f is reducible by B in the sense defined above. (Taking $\sigma_i = 1$ for all i.)

Remark 1.3.7. Suppose that $G = \mathfrak{S}_X$, the term ordering $\leq$ of $X^\diamond$ is $\leq_{\text{lex}}$, and the order type of $(X, \leq)$ is $\leq \omega$. Then in the definition of reducibility by B above, we may require that the σ_i satisfy $\sigma_i(x) = x$ for all $1 \leq i \leq m$ and $x > |\operatorname{lm}(f)|$. (By Lemma 1.2.14.)

The smallest quasi-ordering on R extending the relation $\xrightarrow[B]{}$ is denoted by $\xrightarrow[B]{*}$. If $f, h \neq 0$ and $f \xrightarrow[B]{} h$, then $\operatorname{lm}(h) < \operatorname{lm}(f)$, by Lemma 1.2.12. In particular, every chain

$$h_0 \xrightarrow[B]{} h_1 \xrightarrow[B]{} h_2 \xrightarrow[B]{} \cdots$$

with all $h_i \in R \setminus \{0\}$ is finite. (Since the term ordering $\leq$ is well-founded.) Hence there exists $r \in R$ such that $f \xrightarrow[B]{*} r$ and r is reduced with respect to B; we call such an r a *normal form* of f with respect to B.

Lemma 1.3.8. *Suppose that* $f \xrightarrow[B]{*} r$. *Then there exist* $g_1, \dots, g_n \in B$, $\sigma_1, \dots, \sigma_n \in G$ *and* $h_1, \dots, h_n \in R$ *such that*

$$f = r + \sum_{i=1}^{n} h_i \sigma_i g_i \quad \textit{and} \quad \operatorname{lm}(f) \geq \max_{1 \leq i \leq n} \operatorname{lm}(h_i \sigma_i g_i).$$

(*In particular,* $f - r \in \langle B \rangle_{R[G]}$.)

Proof. This is clear if $f = r$. Otherwise we have $f \xrightarrow[B]{} h \xrightarrow[B]{*} r$ for some $h \in R$. Inductively we may assume that there exist $g_1, \dots, g_n \in B$, $\sigma_1, \dots, \sigma_n \in G$ and $h_1, \dots, h_n \in R$ such that

$$h = r + \sum_{i=1}^{n} h_i \sigma_i g_i \quad \text{and} \quad \operatorname{lm}(h) \geq \max_{1 \leq i \leq n} \operatorname{lm}(h_i \sigma_i g_i).$$

There are also $g_{n+1}, \dots, g_{n+m} \in B$, $\sigma_{n+1}, \dots, \sigma_{n+m} \in G$, $a_{n+1}, \dots, a_{n+m} \in A$ and $w_{n+1}, \dots, w_{n+m} \in X^\diamond$ such that $\operatorname{lm}(w_{n+i}\sigma_{n+i}g_{n+i}) = \operatorname{lm}(f)$ for all i and

$$\operatorname{lt}(f) = \sum_{i=1}^{m} a_{n+i} w_{n+i} \sigma_{n+i} \operatorname{lt}(g_{n+i}), \qquad f = h + \sum_{i=1}^{m} a_{n+i} w_{n+i} \sigma_{n+i} g_{n+i}.$$

Hence putting $h_{n+i} := a_{n+i} w_{n+i}$ for $i = 1, \dots, m$ we have $f = r + \sum_{j=1}^{n+m} h_j \sigma_j g_j$ and $\operatorname{lm}(f) > \operatorname{lm}(h) \geq \operatorname{lm}(h_j \sigma_j g_j)$ if $1 \leq j \leq n$, $\operatorname{lm}(f) = \operatorname{lm}(h_j \sigma_j g_j)$ if $n < j \leq n + m$. □

Remark 1.3.9. Suppose that $G = \mathfrak{S}_X$, $\leq\, = \,\leq_{\text{lex}}$, and X has order type $\leq \omega$. Then in the previous lemma we can choose the σ_i such that in addition $\sigma_i(x) = x$ for all i and all $x > |\operatorname{lm}(f)|$. (By Remark 1.3.7.)

1.3.2 Gröbner bases

Let B be a subset of R. We let

$$\operatorname{lt}(B) := \big\langle \operatorname{lc}(g)w : 0 \neq g \in B,\ \operatorname{lm}(g) \preceq w \big\rangle_A$$

be the A-submodule of R generated by all elements of the form $\operatorname{lc}(g)w$, where $g \in B$ is nonzero and w is a monomial with $\operatorname{lm}(g) \preceq w$. Clearly for nonzero $f \in R$ we have:

$\mathrm{lt}(f) \in \mathrm{lt}(B)$ if and only if f is reducible by B. In particular, $\mathrm{lt}(B)$ contains $\big\{ \mathrm{lt}(g) : g \in B \big\}$, and for an ideal I of R which is G-invariant, we simply have

$$\mathrm{lt}(I) = \big\{ \mathrm{lt}(f) : f \in I \big\}.$$

(Use Lemma 1.2.12.) We say that a subset B of an invariant ideal I of R is a *Gröbner basis* for I (with respect to our choice of term ordering $\leq$) if $\mathrm{lt}(I) = \mathrm{lt}(B)$.

Lemma 1.3.10. *Let I be an invariant ideal of R and B be a set of nonzero elements of I. The following are equivalent:*

(1) *B is a Gröbner basis for I.*

(2) *Every nonzero $f \in I$ is reducible by B.*

(3) *Every $f \in I$ has normal form 0. (In particular, $I = \langle B \rangle_{R[G]}$.)*

(4) *Every $f \in I$ has unique normal form 0.*

Proof. The implications (1) ⇒ (2) ⇒ (3) ⇒ (4) are either obvious or follow from the remarks preceding the lemma. Suppose that (4) holds. Every $f \in I \setminus \{0\}$ with $\mathrm{lt}(f) \notin \mathrm{lt}(B)$ is reduced with respect to B, hence has two distinct normal forms (0 and f), a contradiction. Thus $\mathrm{lt}(I) = \mathrm{lt}(B)$. □

Suppose that B is a Gröbner basis for an ideal I of the polynomial ring $R = A[X^\diamond]$, in the usual sense of the word (as defined, for finite X, in [1, Chapter 4]); if I is invariant, then B is a Gröbner basis for I as defined above (by Example 1.3.6). Moreover, for $G = \{1\}$, the previous lemma reduces to a familiar characterization of Gröbner bases in the usual case of polynomial rings. It is probably possible to also introduce a notion of S-polynomial and to prove a Buchberger-style criterion for Gröbner bases in our setting, leading to a completion procedure for the construction of Gröbner bases. At this point, we will not pursue these issues further, and rather show:

Proposition 1.3.11. *Suppose that the term ordering $\leq$ of $X^\diamond$ is lovely for G. Then every invariant ideal of R has a finite Gröbner basis.*

For a subset B of R let $\operatorname{lm}(B)$ denote the final segment of $X^\diamond$ with respect to $\preceq$ generated by the $\operatorname{lm}(g)$, $g \in B$. If A is a field, then a subset B of an invariant ideal I of R is a Gröbner basis for I if and only if $\operatorname{lm}(B) = \operatorname{lm}(I)$. Hence in this case, the proposition follows immediately from the equivalence of (1) and (4) in Proposition 1.2.1. For the general case we use the following observation:

Lemma 1.3.12. *Let S be a well-quasi-ordered set and T be a well-founded ordered set, and let $\varphi\colon S \to T$ be decreasing: $s \leq t \Rightarrow \varphi(s) \geq \varphi(t)$, for all $s, t \in S$. Then the quasi-ordering $\leq_\varphi$ on S defined by*

$$s \leq_\varphi t \quad :\Longleftrightarrow \quad s \leq t \ \wedge \ \varphi(s) = \varphi(t)$$

is a well-quasi-ordering. □

Proof of Proposition 1.3.11. Suppose now that our term ordering of $X^\diamond$ is lovely for G, and let I be an invariant ideal of R. For $w \in X^\diamond$ consider

$$\operatorname{lc}(I, w) := \big\{ \operatorname{lc}(f) : f \in I, \text{ and } f = 0 \text{ or } \operatorname{lm}(f) = w \big\},$$

an ideal of A. Note that if $v \preceq w$, then $\operatorname{lc}(I, v) \subseteq \operatorname{lc}(I, w)$. We apply the lemma to $S = X^\diamond$, quasi-ordered by $\preceq$, $T =$ the collection of all ideals of A, ordered by reverse inclusion, and φ given by $w \mapsto \operatorname{lc}(I, w)$. Thus by (4) in Proposition 1.2.1, applied to the final segment $X^\diamond$ of the well-quasi-ordering $\leq_\varphi$, we obtain finitely many $w_1, \dots, w_m \in X^\diamond$ with the following property: for every $w \in X^\diamond$ there exists some $i \in \{1, \dots, m\}$ such that $w_i \preceq w$ and $\operatorname{lc}(I, w_i) = \operatorname{lc}(I, w)$. Using Noetherianity of A, for every i we now choose finitely many nonzero elements $g_{i1}, \dots, g_{in_i}$ of I ($n_i \in \mathbb{N}$), each with leading monomial w_i, whose leading coefficients generate the ideal $\operatorname{lc}(I, w_i)$ of A. We claim that

$$B := \{g_{ij} : 1 \leq i \leq m, \ 1 \leq j \leq n_i\}$$

is a Gröbner basis for I. To see this, let $0 \neq f \in I$, and put $w := \operatorname{lm}(f)$. Then there is some i with $w_i \preceq w$ and $\operatorname{lc}(I, w_i) = \operatorname{lc}(I, w)$. This shows that f is reducible by $\{g_{i1}, \dots, g_{i,n_i}\}$, and hence by B. By Lemma 1.3.10, B is a Gröbner basis for I. □

From Proposition 1.3.11 and the implication (1) ⇒ (3) in Lemma 1.3.10 we obtain Theorem 1.3.1.

1.3.3 A partial converse of Theorem 1.3.1

Consider now the quasi-ordering $|_G$ of $X^\diamond$ defined by

$$v|_G w \quad :\Longleftrightarrow \quad \exists \sigma \in G : \sigma v | w,$$

which extends every symmetric cancellation ordering corresponding to a term ordering of $X^\diamond$. If M is a set of monomials from $X^\diamond$ and F the final segment of $(X^\diamond, |_G)$ generated by M, then the invariant ideal $\langle M \rangle_{R[G]}$ of R is finitely generated as an $R[G]$-module if and only if F is generated by a finite subset of M. Hence by the implication (4) ⇒ (1) in Proposition 1.2.1 we get:

Lemma 1.3.13. *If R is Noetherian as an $R[G]$-module, then $|_G$ is a well-quasi-ordering.* □

This will be used in Section 1.5 below.

1.3.4 Connection to a concept due to Michler

Let $\leq$ be a term ordering of $X^\diamond$. For each $\sigma \in G$ we define a term ordering $\leq_\sigma$ on $X^\diamond$ by

$$v \leq_\sigma w \quad \Longleftrightarrow \quad \sigma v \leq \sigma w.$$

We denote the leading monomial of $f \in R$ with respect to $\leq_\sigma$ by $\operatorname{lm}_\sigma(f)$. Clearly we have

$$\sigma \operatorname{lm}(f) = \operatorname{lm}_{\sigma^{-1}}(\sigma f) \qquad \text{for all } \sigma \in G \text{ and } f \in R. \tag{1.3.1}$$

Let I be an invariant ideal of R. Generalizing terminology introduced in [45], let us call a set B of nonzero elements of I a *universal G-Gröbner basis* for I (with respect to $\leq$) if B contains, for every $\sigma \in G$, a Gröbner basis (in the usual sense of the word) for the ideal I with respect to the term ordering $\leq_\sigma$. If the set X of indeterminates is finite, then every invariant ideal of R has a finite universal G-Gröbner basis. By the remark following Lemma 1.3.10, every universal G-Gröbner basis for an invariant ideal I of R is a Gröbner basis for I. We finish this section by observing:

Lemma 1.3.14. *Suppose that A is field. If B is a Gröbner basis for the invariant ideal I of R, then*

$$GB = \{\sigma g : \sigma \in G,\ g \in B\}$$

is a universal G-Gröbner basis for I.

Proof. Let $\sigma \in G$ and $f \in I$, $f \neq 0$. Then $\sigma f \in I$, hence there exists $\tau \in G$ and $g \in B$ such that $w \leq \operatorname{lm}(g) \Rightarrow w \leq_\tau \operatorname{lm}(g)$ for all $w \in X^\diamond$, and $\tau \operatorname{lm}(g) | \operatorname{lm}(\sigma f)$. The first condition implies in particular that $\tau \operatorname{lm}(g) = \operatorname{lm}(\tau g)$, hence $\sigma^{-1}\tau \operatorname{lm}(g) = \operatorname{lm}_\sigma(\sigma^{-1}\tau g)$ and $\sigma^{-1} \operatorname{lm}(\sigma f) = \operatorname{lm}_\sigma(f)$ by (1.3.1). Put $h := \sigma^{-1}\tau g \in GB$. Then $\operatorname{lm}_\sigma(h) | \operatorname{lm}_\sigma(f)$ by the second condition. This shows that GB contains a Gröbner basis for I with respect to $\leq_\sigma$, as required. □

Example 1.3.15. *Suppose that $G = \mathfrak{S}_n$, the group of permutations of $\{1, 2, \ldots, n\}$, acting on $X = \{x_1, \ldots, x_n\}$ via $\sigma x_i = x_{\sigma(i)}$. The invariant ideal $I = \langle x_1, \ldots, x_n \rangle_R$ has Gröbner basis $\{x_1\}$ with respect to the lexicographic ordering; a corresponding (minimal) universal $\mathfrak{S}_n$-Gröbner basis for I is $\{x_1, \ldots, x_n\}$.*

1.4 Invariant Chains of Ideals

In this section we describe a relationship between certain chains of increasing ideals in finite-dimensional polynomials rings and invariant ideals of infinite-dimensional polynomial rings. We begin with an abstract setting that is suitable for placing the motivating problem (described in the next section) in a proper context. Throughout this section, m and n range over the set of positive integers. For each n, let R_n be a commutative ring, and assume that R_n is a subring of R_{n+1}, for each n. Suppose that the symmetric group on n letters $\mathfrak{S}_n$ gives an action (not necessarily faithful) on R_n such that $f \mapsto \sigma f \colon R_n \to R_n$ is a ring homomorphism, for each $\sigma \in \mathfrak{S}_n$. Furthermore, suppose that the natural embedding of $\mathfrak{S}_n$ into $\mathfrak{S}_m$ for $n \leq m$ is compatible with the embedding of rings $R_n \subseteq R_m$; that is, if $\sigma \in \mathfrak{S}_n$ and $\hat{\sigma}$ is the corresponding element in $\mathfrak{S}_m$, then $\hat{\sigma} \restriction R_n = \sigma$. Note that there exists a unique action of $\mathfrak{S}_\infty$ on the ring $R := \bigcup_{n \geq 1} R_n$ which extends the action of each $\mathfrak{S}_n$ on R_n. An ideal of R is *invariant* if $\sigma f \in I$ for all $\sigma \in \mathfrak{S}_\infty$, $f \in I$.

We will need a method for lifting ideals of smaller rings into larger ones, and one such technique is as follows.

Definition 1.4.1. For $m \geq n$, the *m-symmetrization* $L_m(B)$ of a set B of elements of

R_n is the $\mathfrak{S}_m$-invariant ideal of R_m given by

$$L_m(B) = \langle g : g \in B \rangle_{R_m[\mathfrak{S}_m]}$$

In order for us to apply this definition sensibly, we must make sure that the m-symmetrization of an ideal can be defined in terms of generators.

Lemma 1.4.2. *If B is a set of generators for the ideal $I_B = \langle B \rangle_{R_n}$ of R_n, then $L_m(I_B) = L_m(B)$.*

Proof. Suppose that B generates the ideal $I_B \subseteq R_n$. Clearly, $L_m(B) \subseteq L_m(I_B)$. Therefore, it is enough to show the inclusion $L_m(I_B) \subseteq L_m(B)$. Suppose that $h \in L_m(I_B)$ so that $h = \sum_{j=1}^{s} f_j \cdot \sigma_j h_j$ for elements $f_j \in R_m$, $h_j \in I_B$ and $\sigma_j \in \mathfrak{S}_m$. Next express each $h_j = \sum_{i=1}^{r_j} p_{ij} g_{ij}$ for $p_{ij} \in R_n$ and $g_{ij} \in B$. Substitution into the expression above for h gives us

$$h = \sum_{j=1}^{s} \sum_{i=1}^{r_j} f_j \cdot \sigma_j p_{ij} \cdot \sigma_j g_{ij}.$$

This is easily seen to be an element of $L_m(B)$, completing the proof. □

Example 1.4.3. *Let $S = \mathbb{Q}[t_1, t_2]$, $R_n = \mathbb{Q}[x_1, \ldots, x_n]$, and consider the natural action of $\mathfrak{S}_n$ on R_n. Let Q be the kernel of the homomorphism induced by the map $\phi\colon R_3 \to S$ given by $\phi(x_1) = t_1^2$, $\phi(x_2) = t_2^2$, and $\phi(x_3) = t_1 t_2$. Then, $Q = \langle x_1 x_2 - x_3^2 \rangle$, and $L_4(Q) \subseteq R_4$ is generated by the following* 12 *polynomials:*

$$\begin{gathered}
x_1x_2 - x_3^2,\ x_1x_2 - x_4^2,\ x_1x_3 - x_2^2,\ x_1x_3 - x_4^2,\\
x_1x_4 - x_3^2,\ x_1x_4 - x_2^2,\ x_2x_3 - x_1^2,\ x_2x_3 - x_4^2,\\
x_2x_4 - x_1^2,\ x_2x_4 - x_3^2,\ x_3x_4 - x_1^2,\ x_3x_4 - x_2^2.
\end{gathered}$$

We would also like a way to project a set of elements in R_m down to a smaller ring R_n ($n \leq m$).

Definition 1.4.4. Let $B \subseteq R_m$ and $n \leq m$. The *n-projection* $P_n(B)$ of B is the $\mathfrak{S}_n$-invariant ideal of R_n given by

$$P_n(B) = \langle g : g \in B \rangle_{R_m[\mathfrak{S}_m]} \cap R_n.$$

We now consider increasing chains $I_\circ$ of ideals $I_n \subseteq R_n$:

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots,$$

simply called *chains* below. Of course, such chains will usually fail to stabilize since they are ideals in larger and larger rings. However, it is possible for these ideals to stabilize "up to the action of the symmetric group," a concept we make clear below. For the purposes of this work, we will only consider a special class of chains; namely, a *symmetrization invariant chain* (resp. *projection invariant chain*) is one for which $L_m(I_n) \subseteq I_m$ (resp. $P_n(I_m) \subseteq I_n$) for all $n \leq m$. If $I_\circ$ is both a symmetrization and a projection invariant chain, then it will be simply called an *invariant chain*. We will encounter some concrete invariant chains in the next section. The stabilization definition alluded to above is as follows.

Definition 1.4.5. A symmetrization invariant chain of ideals $I_\circ$ as above *stabilizes modulo the symmetric group* (or simply *stabilizes*) if there exists a positive integer N such that

$$L_m(I_n) = I_m \qquad \text{for all } m \geq n > N.$$

To put it another way, accounting for the natural action of the symmetric group, the ideals I_n are the same for large enough n. Let us remark that if for a symmetrization invariant chain $I_\circ$, there is some integer N such that $L_m(I_N) = I_m$ for all $m > N$, then $I_\circ$ stabilizes. This follows from the inclusions

$$I_m = L_m(I_N) \subseteq L_m(I_n) \subseteq I_m, \quad n > N.$$

Any chain $I_\circ$ naturally gives rise to an ideal $\mathcal{I}(I_\circ)$ of $R = \bigcup_{n\geq 1} R_n$ by way of

$$\mathcal{I}(I_\circ) := \bigcup_{n\geq 1} I_n.$$

Conversely, if I is an ideal of R, then

$$I_n = \mathcal{J}_n(I) := I \cap R_n$$

defines the components of a chain $\mathcal{J}(I) := I_\circ$. Clearly, for any ideal $I \subseteq R$, we have $\mathcal{I} \circ \mathcal{J}(I) = I$, but, as is easily seen, it is not true in general that $\mathcal{J} \circ \mathcal{I}(I_\circ) = I_\circ$. However, for invariant chains, this relationship does hold, as the following straightforward lemma describes.

Lemma 1.4.6. *There is a one-to-one, inclusion-preserving correspondence between invariant chains $I_\circ$ and invariant ideals I of R given by the maps $\mathcal{I}$ and $\mathcal{J}$.* □

For the remainder of this section we consider the case where, for a commutative Noetherian ring A, we have $R_n = A[x_1, \dots, x_n]$ for each n, endowed with the natural action of $\mathfrak{S}_n$ on the indeterminates $x_1, \dots, x_n$. Then $R = A[X^\diamond]$ where $X = \{x_1, x_2, \dots\}$. We use the results of the previous section to demonstrate the following.

Theorem 1.4.7. *Every symmetrization invariant chain stabilizes modulo the symmetric group.*

Proof. Given a symmetrization invariant chain, construct the invariant ideal $I = \mathcal{I}(I_\circ)$ of R. One would now like to apply Theorem 1.1.1, however, more care is needed to prove stabilization. Let $\leq$ be a well-ordering of X of order type ω, and let B be a finite Gröbner basis for I with respect to the corresponding term ordering $\leq_{\text{lex}}$ of $X^\diamond$. (Theorem 1.2.20 and Proposition 1.3.11.) Choose a positive integer N such that $B \subseteq I_N$; we claim that $I_m = L_m(I_N)$ for all $m \geq N$. Let $f \in I_m$, $f \neq 0$. By the equivalence of (1) and (3) in Lemma 1.3.10 we have $f \xrightarrow[B]{*} 0$. Hence by Lemma 1.3.8 there are $g_1, \dots, g_n \in B$, $h_1, \dots, h_n \in R$, as well as $\sigma_1, \dots, \sigma_n \in \mathfrak{S}_\infty$, such that

$$f = h_1\sigma_1 g_1 + \cdots + h_n\sigma_n g_n \quad \text{and} \quad \operatorname{lm}(f) = \max_i \operatorname{lm}(h_i\sigma_i g_i).$$

By Remark 1.3.9 we may assume that in fact $\sigma_i \in \mathfrak{S}_m$ for each i. Moreover $\operatorname{lm}(h_i) \leq_{\text{lex}} \operatorname{lm}(f)$, hence $|\operatorname{lm}(h_i)| \leq |\operatorname{lm}(f)| \leq m$, for each i. Therefore $h_i \in R_m$ for each i. This shows that $f \in L_m(B) \subseteq L_m(I_N)$ as desired. □

1.5 A Chemistry Motivation

We can now discuss the details of the basic problem that is of interest to us. It was brought to our attention by Bernd Sturmfels, who, in turn, learned about it from Andreas Dress.

Fix a natural number $k \geq 1$. Given a set S we denote by $\langle S\rangle^k$ the set of all ordered k-element subsets of S, that is, $\langle S\rangle^k$ is the set of all k-tuples $\boldsymbol{u} = (u_1, \ldots, u_k) \in S^k$ with pairwise distinct $u_1, \ldots, u_k$. We also just write $\langle n\rangle^k$ instead of $\langle\{1, \ldots, n\}\rangle^k$. Let K be a field, and for $n \geq k$ consider the polynomial ring

$$R_n = K\big[\{x_{\boldsymbol{u}}\}_{\boldsymbol{u}\in\langle n\rangle^k}\big].$$

We let $\mathfrak{S}_n$ act on $\langle n\rangle^k$ by

$$\sigma(u_1, \ldots, u_k) = \big(\sigma(u_1), \ldots, \sigma(u_k)\big).$$

This induces an action $(\sigma, x_{\boldsymbol{u}}) \mapsto \sigma x_{\boldsymbol{u}} = x_{\sigma\boldsymbol{u}}$ of $\mathfrak{S}_n$ on the indeterminates $x_{\boldsymbol{u}}$, which we extend to an action of $\mathfrak{S}_n$ on R_n in the natural way. We also put $R = \bigcup_{n\geq k} R_n$. Note that

$$R = K\big[\{x_{\boldsymbol{u}}\}_{\boldsymbol{u}\in\langle\Omega\rangle^k}\big],$$

where $\Omega = \{1, 2, 3, \ldots\}$ is the set of positive integers, and that the actions of $\mathfrak{S}_n$ on R_n combine uniquely to an action of $\mathfrak{S}_\infty$ on R. Let now $f(y_1, \ldots, y_k) \in K[y_1, \ldots, y_k]$, let $t_1, t_2, \ldots$ be an infinite sequence of pairwise distinct indeterminates over K, and for $n \geq k$ consider the K-algebra homomorphism

$$\phi_n \colon R_n \to K[t_1, \ldots, t_n], \qquad x_{(u_1,\ldots,u_k)} \mapsto f(t_{u_1}, \ldots, t_{u_k}).$$

The ideal

$$Q_n = \ker \phi_n$$

of R_n determined by such a map is the prime ideal of algebraic relations between the quantities $f(t_{u_1}, \ldots, t_{u_k})$. Such ideals arise in chemistry [44, 54, 55]; of specific interest there is when f is a Vandermonde polynomial $\prod_{i<j}(y_i - y_j)$. In this case, the ideals Q_n correspond to relations among a series of experimental measurements. One would then like to understand the limiting behavior of such relations, and in particular, to see that they stabilize up to the action of the symmetric group.

Example 1.5.1. *The permutation $\sigma = (1\,2\,3) \in \mathfrak{S}_3$ acts on the elements*

$$(1, 2),\ (2, 1),\ (1, 3),\ (3, 1),\ (2, 3),\ (3, 2)$$

of $\langle 3\rangle^2$ *to give*

$$(2,3),\ (3,2),\ (2,1),\ (1,2),\ (3,1),\ (1,3),$$

respectively. Let $f(t_1,t_2) = t_1^2 t_2$*. Then the action of* σ *on the valid relation* $x_{12}^2 x_{31} - x_{13}^2 x_{21} \in Q_3$ *gives us another relation* $x_{23}^2 x_{12} - x_{21}^2 x_{32} \in Q_3$*.*

It is easy to see that by construction, the chain $Q_\circ$ of ideals

$$Q_k \subseteq Q_{k+1} \subseteq \cdots \subseteq Q_n \subseteq \cdots$$

(which we call the chain of ideals *induced by the polynomial* f) is an invariant chain. As in the proof of Theorem 1.4.7, we would like to form the ideal $Q = \bigcup_{n\geq k} Q_n$ of the infinite-dimensional polynomial ring $R = \bigcup_{n\geq k} R_n$, and then apply a finiteness theorem to conclude that $Q_\circ$ stabilizes in the sense mentioned above (Definition 1.4.5). For $k = 1$, Theorem 1.4.7 indeed does the job. Unfortunately however, this simple-minded approach fails for $k \geq 2$:

Proposition 1.5.2. *For* $k \geq 2$*, the* $R[\mathfrak{S}_\infty]$*-module* R *is not Noetherian.*

Proof. Let us make the dependence on k explicit and denote R by $R^{(k)}$. Then

$$x_{(u_1,\ldots,u_k,u_{k+1})} \mapsto x_{(u_1,\ldots,u_k)}$$

defines a surjective K-algebra homomomorphism $\pi_k \colon R^{(k+1)} \to R^{(k)}$ with invariant kernel. Hence if $R^{(k+1)}$ is Noetherian as an $R[\mathfrak{S}_\infty]$-module, then so is $R^{(k)}$; thus it suffices to prove the proposition in the case $k = 2$. Suppose therefore that $k = 2$. By Lemma 1.3.13 it is enough to produce an infinite bad sequence for the quasi-ordering $|_{\mathfrak{S}_\infty}$ of $X^\diamond$, where $X = \{x_{\boldsymbol{i}} : \boldsymbol{i} \in \langle\Omega\rangle^2\}$. For this, consider the sequence of monomials

$$\begin{aligned}
s_3 &= x_{(1,2)}x_{(3,2)}x_{(3,4)} \\
s_4 &= x_{(1,2)}x_{(3,2)}x_{(4,3)}x_{(4,5)} \\
s_5 &= x_{(1,2)}x_{(3,2)}x_{(4,3)}x_{(5,4)}x_{(6,7)} \\
&\ \vdots \\
s_n &= x_{(1,2)}x_{(3,2)}x_{(4,3)}\cdots x_{(n,n-1)}x_{(n,n+1)} \qquad (n = 3,4,\ldots) \\
&\ \vdots
\end{aligned}$$

Now for $n < m$ and any $\sigma \in \mathfrak{S}_\infty$, the monomial σs_n does not divide s_m. To see this, suppose otherwise. Note that $x_{(1,2)}$, $x_{(3,2)}$ is the only pair of indeterminates which divides s_n or s_m and has the form $x_{(i,j)}$, $x_{(l,j)}$ $(i, j, l \in \Omega)$. Therefore $\sigma(2) = 2$, and either $\sigma(1) = 1$, $\sigma(3) = 3$, or $\sigma(1) = 3$, $\sigma(3) = 1$. But since 1 does not appear as the second component j of a factor $x_{(i,j)}$ of s_m, we have $\sigma(1) = 1$, $\sigma(3) = 3$. Since $x_{(4,3)}$ is the only indeterminate dividing s_n or s_m of the form $x_{(i,3)}$ with $i \in \Omega$, we get $\sigma(4) = 4$; since $x_{(5,4)}$ is the only indeterminate dividing s_n or s_m of the form $x_{(i,4)}$ with $i \in \Omega$, we get $\sigma(5) = 5$; etc. Ultimately this yields $\sigma(i) = i$ for all $i = 1, \dots, n$. But the only indeterminate dividing s_m of the form $x_{(n,j)}$ with $j \in \Omega$ is $x_{(n,n-1)}$, hence the factor $\sigma x_{(n,n+1)} = x_{(n,\sigma(n+1))}$ of σs_n does not divide s_m. This shows that $s_3, s_4, \dots$ is a bad sequence for the quasi-ordering $|_{\mathfrak{S}_\infty}$, as claimed. □

Remark 1.5.3. The construction of the infinite bad sequence $s_3, s_4, \dots$ in the proof of the previous proposition was inspired by an example in [36].

1.5.1 A criterion for stabilization

Our next goal is to give a condition for the chain $Q_\circ$ to stabilize. Given $g \in R$, we define the *variable size* of g to be the number of distinct indeterminates $x_{\boldsymbol{u}}$ that appear in g. For example, $g = x_{12}^5 + x_{45}x_{23} + x_{45}$ has variable size 3.

Lemma 1.5.4. *A chain of ideals $Q_\circ$ induced by a polynomial $f \in K[y_1, \dots, y_k]$ stabilizes modulo the symmetric group if and only if there exist integers M and N such that for all $n > N$, there are generators for Q_n with variable sizes at most M. Moreover, in this case a bound for stabilization is given by* $\max(N, kM)$.

Proof. Suppose M and N are integers with the stated property. To see that $Q_\circ$ stabilizes, since $Q_\circ$ is an invariant chain, we need only verify that $N' = \max(N, kM)$ is such that $Q_m \subseteq L_m(Q_n)$ for $m \geq n > N'$. For this inclusion, it suffices that each generator in a generating set for the ideal Q_m of R_m is in $L_m(Q_n)$. Since $m > N$, there are generators B for Q_m with variable sizes at most M. If $g \in B$, then there are at most kM different integers appearing as subscripts of indeterminates in g. We can form a permutation $\sigma \in \mathfrak{S}_m$ such that $\sigma g \in R_{N'}$ and thus in R_n. But then $\sigma g \in P_n(Q_m) \subseteq Q_n$ so that $g = \sigma^{-1}\sigma g \in L_m(Q_n)$ as desired.

Conversely, suppose that $Q_\circ$ stabilizes. Then there exists an N such that $Q_m = L_m(Q_N)$ for all $m > N$. Let B be any finite generating set for Q_N. Then for all $m > N$, $Q_m = L_m(B)$ is generated by elements of bounded variable size, by Lemma 1.4.2. □

Although this condition is a very simple one, it will prove useful. Below we will apply it together with a preliminary reduction to the case that each indeterminate $y_1, \ldots, y_k$ actually occurs in the polynomial f, which we explain next. For this we let $\pi_k \colon R^{(k+1)} \to R^{(k)}$ be the surjective K-algebra homomorphism defined in the proof of Proposition 1.5.2. We write $Q^{(k)}$ for Q, and considering $f \in K[y_1, \ldots, y_k]$ as an element of $K[y_1, \ldots, y_k, y_{k+1}]$, we also let $Q^{(k+1)}$ be the kernel of the K-algebra homomorphsm

$$R^{(k+1)} \to K[t_1, t_2, \ldots], \qquad x_{(u_1,\ldots,u_k,u_{k+1})} \mapsto f(t_{u_1}, \ldots, t_{u_k}, t_{u_{k+1}})$$
$$(= f(t_{u_1}, \ldots, t_{u_k})).$$

Note that $\pi_k(Q^{(k+1)}) = Q^{(k)}$, and the ideal $\ker \pi_k$ of $R^{(k+1)}$ is generated by the elements

$$x_{(u_1,\ldots,u_k,i)} - x_{(u_1,\ldots,u_k,j)} \qquad (i, j \in \Omega),$$

in particular $\ker \pi_k \subseteq Q^{(k+1)}$. It is easy to see that as an $R^{(k+1)}[\mathfrak{S}_\infty]$-module, $\ker \pi_k$ is generated by the single element $x_{(1,\ldots,k,k+1)} - x_{(1,\ldots,k,k+2)}$. These observations now yield:

Lemma 1.5.5. *Suppose that the invariant ideal $Q^{(k)}$ of $R^{(k)}$ is finitely generated as an $R^{(k)}[\mathfrak{S}_\infty]$-module. Then the invariant ideal $Q^{(k+1)}$ of $R^{(k+1)}$ is finitely generated as an $R^{(k+1)}[\mathfrak{S}_\infty]$-module.* □

We let $\mathfrak{S}_k$ act on $\langle\Omega\rangle^k$ by

$$\tau(u_1, \ldots, u_k) = (u_{\tau(1)}, \ldots, u_{\tau(k)}) \qquad \text{for } \tau \in \mathfrak{S}_k,\ (u_1, \ldots, u_k) \in \langle\Omega\rangle^k.$$

This action gives rise to an action of $\mathfrak{S}_k$ on $\{x_{\boldsymbol{u}}\}_{\boldsymbol{u} \in \langle\Omega\rangle^k}$ by $\tau x_{\boldsymbol{u}} = x_{\tau\boldsymbol{u}}$, which we extend to an action of $\mathfrak{S}_k$ on R in the natural way. We also let $\mathfrak{S}_k$ act on $K[y_1, \ldots, y_k]$ by $\tau f(y_1, \ldots, y_k) = f(y_{\tau(1)}, \ldots, y_{\tau(k)})$. Note that

$$\tau Q_k \subseteq \tau Q_{k+1} \subseteq \cdots \subseteq \tau Q_n \subseteq \cdots$$

is the chain induced by τf. Using the lemma above we obtain:

Corollary 1.5.6. *Let $f \in K[y_1, \ldots, y_k]$. There are $i \in \{0, \ldots, k\}$ and $\tau \in \mathfrak{S}_k$ such that $\tau f \in K[y_1, \ldots, y_i]$ and each of the indeterminates $y_1, \ldots, y_i$ occurs in τf. If the chain of ideals induced by the polynomial τf stabilizes, then so does the chain of ideals induced by f.* □

1.5.2 Chains induced by monomials

If the given polynomial f is a monomial, then the homomorphism ϕ_n from above produces a (homogeneous) toric kernel Q_n. In particular, there is a finite set of binomials that generate Q_n (see [64]). Although a proof for the general toric case eludes us, we do have the following.

Theorem 1.5.7. *Let $f \in K[y_1, \ldots, y_k]$ be a square-free monomial. Then, the sequence of kernels induced by f stabilizes modulo the symmetric group. Moreover, a bound for when stabilization occurs is $N = 4k$.*

To prepare for the proof of this result, we discuss in detail the toric encoding associated to our problem (see [64, Chapter 14] for more details). By Corollary 1.5.6, we may assume that $f = y_1 \cdots y_k$. Then $g - \tau g \in Q$ for all $g \in R$. We say that $\boldsymbol{u} = (u_1, \ldots, u_k) \in \langle \Omega \rangle^k$ is *sorted* if $u_1 < \cdots < u_k$, and *unsorted* otherwise; similarly we say that $x_{\boldsymbol{u}}$ is sorted (unsorted) if $\boldsymbol{u}$ is sorted (unsorted, respectively). For example, x_{135} is a sorted indeterminate, whereas x_{315} is not. Consider the set of vectors

$$\mathcal{A}_n = \big\{(i_1, \ldots, i_n) \in \mathbb{Z}^n : i_1 + \cdots + i_n = k,\ 0 \leq i_1, \ldots, i_n \leq 1\big\}.$$

View $\mathcal{A}_n$ as an n-by-$\binom{n}{k}$ matrix entries with 0 and 1, whose with columns are indexed by sorted indeterminates $x_{\boldsymbol{u}}$ and whose rows are indexed by t_i ($i = 1, \ldots, n$). (See Example 1.5.9 below.) Let $\operatorname{sort}(\,\cdot\,)$ denote the operator which takes any word in $\{1, \ldots, n\}^*$ and sorts it in increasing order. By [64, Remark 14.1], the toric ideal $I_{\mathcal{A}_n}$ associated to $\mathcal{A}_n$ is generated (as K-vector space) by the binomials $x_{\boldsymbol{u}_1} \cdots x_{\boldsymbol{u}_r} - x_{\boldsymbol{v}_1} \cdots x_{\boldsymbol{v}_r}$, where $r \in \mathbb{N}$ and the $\boldsymbol{u}_i$, $\boldsymbol{v}_j$ are sorted elements of $\langle n \rangle^k$ such that $\operatorname{sort}(\boldsymbol{u}_1 \cdots \boldsymbol{u}_r) = \operatorname{sort}(\boldsymbol{v}_1 \cdots \boldsymbol{v}_r)$. In particular, we have $I_{\mathcal{A}_n} \subseteq Q_n$. Let B be any set of generators for the ideal $I_{\mathcal{A}_n}$.

Lemma 1.5.8. *A generating set for the ideal Q_n of R_n is given by*

$$S = B \cup \{x_{\boldsymbol{u}} - x_{\tau \boldsymbol{u}} :\ \tau \in \mathfrak{S}_k,\ \boldsymbol{u} \text{ is sorted}\}.$$

Proof. Elements of Q_n are of the form $g = x_{\boldsymbol{u}_1} \cdots x_{\boldsymbol{u}_r} - x_{\boldsymbol{v}_1} \cdots x_{\boldsymbol{v}_r}$, in which the $\boldsymbol{u}_i$ and $\boldsymbol{v}_j$ are ordered k-element subsets of $\{1, \ldots, n\}$ such that $\mathrm{sort}(\boldsymbol{u}_1 \cdots \boldsymbol{u}_r) = \mathrm{sort}(\boldsymbol{v}_1 \cdots \boldsymbol{v}_r)$. We induct on the number t of $\boldsymbol{u}_i$ and $\boldsymbol{v}_j$ that are not sorted. If $t = 0$, then $g \in I_{\mathcal{A}_n}$, and we are done. Suppose now that $t > 0$ and assume without loss of generality that $\boldsymbol{u}_1$ is not sorted. Let $\tau \in \mathfrak{S}_k$ be such that $\tau \boldsymbol{u}_1$ is sorted, and consider the element $h = x_{\tau \boldsymbol{u}_1} x_{\boldsymbol{u}_2} \cdots x_{\boldsymbol{u}_r} - x_{\boldsymbol{v}_1} \cdots x_{\boldsymbol{v}_r}$ of Q_n. This binomial involves $t-1$ unsorted indeterminates, and therefore, inductively, can be expressed in terms of S. But then

$$g = h - (x_{\tau \boldsymbol{u}_1} - x_{\boldsymbol{u}_1}) x_{\boldsymbol{u}_2} \cdots x_{\boldsymbol{u}_r}$$

can as well, completing the proof. □

Example 1.5.9. *Let $k = 2$ and $n = 4$. Then*

$$\begin{array}{ccccccc}
 & x_{12} & x_{13} & x_{14} & x_{23} & x_{24} & x_{34} \\
t_1 & 1 & 1 & 1 & 0 & 0 & 0 \\
t_2 & 1 & 0 & 0 & 1 & 1 & 0 \\
t_3 & 0 & 1 & 0 & 1 & 0 & 1 \\
t_4 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}$$

represents the matrix associated to $\mathcal{A}_4$. The ideal $I_{\mathcal{A}_4}$ is generated by the two binomials $x_{13}x_{24} - x_{12}x_{34}$ and $x_{14}x_{23} - x_{12}x_{34}$. Hence Q_4 is generated by these two elements along with

$$\{x_{12} - x_{21}, x_{13} - x_{31}, x_{14} - x_{41}, x_{23} - x_{32}, x_{24} - x_{42}, x_{34} - x_{43}\}.$$

We are now in a position to prove Theorem 1.5.7.

Proof of Theorem 1.5.7. By Lemma 1.5.4, we need only show that there exist generators for Q_n which have bounded variable sizes. Using [64, Theorem 14.2], it follows that $I_{\mathcal{A}_n}$ has a quadratic (binomial) Gröbner basis for each n (with respect to some term ordering of R_n). By Lemma 1.5.8, there is a set of generators for Q_n with variable sizes at most 4. This proves the theorem. □

We close this chapter with a conjecture that generalizes Theorem 1.5.7.

Conjecture 1.5.10. *The sequence of kernels induced by a monomial f stabilizes modulo the symmetric group.*

Chapter 2

Cyclic Resultants

2.1 Introduction

The m-th cyclic resultant of a univariate polynomial $f \in \mathbb{C}[x]$ is

$$r_m = \mathrm{Res}(f, x^m - 1).$$

We are primarily interested here in the fibers of the map $r : \mathbb{C}[x] \to \mathbb{C}^{\mathbb{N}}$ given by $f \mapsto (r_m)_{m=0}^{\infty}$. In particular, what are the conditions for two polynomials to give rise to the same set of cyclic resultants? For technical reasons, we will only consider polynomials f that do not have a root of unity as a zero. With this restriction, a polynomial will map to a set of all nonzero cyclic resultants. Our main result gives a complete answer to this question.

Theorem 2.1.1. *Let f and g be polynomials in $\mathbb{C}[x]$. Then, f and g generate the same sequence of nonzero cyclic resultants if and only if there exist $u, v \in \mathbb{C}[x]$ with $u(0) \neq 0$ and nonnegative integers l_1, l_2 such that $\deg(u) \equiv l_2 - l_1 \pmod 2$, and*

$$\begin{aligned} f(x) &= (-1)^{l_2 - l_1} x^{l_1} v(x) u(x^{-1}) x^{\deg(u)} \\ g(x) &= x^{l_2} v(x) u(x). \end{aligned}$$

Remark 2.1.2. All our results involving $\mathbb{C}$ hold over any algebraically closed field of characteristic zero.

Although the theorem statement appears somewhat technical, we present a natural interpretation of the result. Suppose that $g(x) = x^{l_2}v(x)u(x)$ is a factorization as above of a polynomial g with nonzero cyclic resultants. Then, another polynomial f giving rise to this same sequence of resultants is obtained from v by multiplication with the reversal $u(x^{-1})x^{\deg(u)}$ of u and a factor $(-1)^{\deg(u)}x^{l_1}$ in which $l_1 \equiv l_2 - \deg(u) \pmod 2$. In other words, $f(x) = (-1)^{\deg(u)}x^{l_1}v(x)u(x^{-1})x^{\deg(u)}$, and all such f must arise in this manner.

Example 2.1.3. *One can check that the polynomials*

$$f(x) = x^3 - 10\,x^2 + 31\,x - 30$$
$$g(x) = 15\,x^5 - 38\,x^4 + 17\,x^3 - 2\,x^2$$

both generate the same cyclic resultants. This follows from the factorizations

$$f(x) = (x-2)\left(15x^2 - 8x + 1\right)$$
$$g(x) = x^2(x-2)\left(x^2 - 8x + 15\right). \quad \square$$

One motivation for the study of cyclic resultants comes from the theory of dynamical systems. Sequences of the form r_m arise as the cardinalities of sets of periodic points for toral endomorphisms. Let A be a $d \times d$ integer matrix and let $X = \mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$ denote the d-dimensional additive torus. Then, the matrix A acts on X by multiplication mod 1; that is, it defines a map $T : X \to X$ given by

$$T(\boldsymbol{x}) = A\boldsymbol{x} \mod \mathbb{Z}^d.$$

Let $\mathrm{Per}_m(T) = \{\boldsymbol{x} \in \mathbb{T}^d : T^m(\boldsymbol{x}) = \boldsymbol{x}\}$ be the set of points fixed under the map T^m. Under the ergodicity condition that no eigenvalue of A is a root of unity, it follows (see [14]) that

$$|r_m(f)| = |\mathrm{Per}_m(T)| = |\det(A^m - I)|,$$

in which I is the $d \times d$ identity matrix, and f is the characteristic polynomial of A. As a consequence of our results, we characterize when the sequence $|\mathrm{Per}_m(T)|$ determines the spectrum of the linear map A lifting T (see Corollary 2.1.13).

In connection with number theory, cyclic resultants were also studied by Pierce and Lehmer [14] in the hope of using them to produce large primes. As a simple example, the Mersenne numbers $M_m = 2^m - 1$ arise as cyclic resultants of the polynomial

$f(x) = x - 2$. Indeed, the map $T(x) = 2x \mod 1$ has precisely M_m points of period m. Further motivation comes from knot theory [63], Lagrangian mechanics [20, 35], and, more recently, in the study of amoebas of varieties [52] and quantum computing [37].

The principal result in the direction of our main characterization theorem was discovered by Fried [17] although certain implications of Fried's result were known to Stark [11]. Given a polynomial $f = a_0x^d + a_1x^{d-1} + \cdots + a_d$ of degree d, the *reversal* of f is the polynomial $x^d f(1/x)$. Additionally, f is called *reciprocal* if $a_i = a_{d-i}$ for $0 \leq i \leq d$ (sometimes such a polynomial is called *palindromic*). Alternatively, f is reciprocal if it is equal to its own reversal. Fried's result may be stated as follows. It will be a corollary of Theorem 2.1.8 below (the real version of Theorem 2.1.1).

Corollary 2.1.4 (Fried). *Let $p(x) = a_0x^d + \cdots + a_{d-1}x + a_d \in \mathbb{R}[x]$ be a real reciprocal polynomial of even degree d with $a_0 > 0$, and let r_m be the m-th cyclic resultants of p. Then, $|r_m|$ uniquely determine this polynomial of degree d as long as the r_m are never 0.*

The following is a direct corollary of our main theorem to the generic case.

Corollary 2.1.5. *Let g be a generic polynomial in $\mathbb{C}[x]$ of degree d. Then, there are exactly 2^{d-1} degree d polynomials with the same set of cyclic resultants as g.*

Proof. If g is generic, then g will not have a root of unity as a zero nor will $g(0) = 0$. Theorem 2.1.1, therefore, implies that any other degree d polynomial $f \in \mathbb{C}[x]$ giving rise to the same set of cyclic resultants is determined by choosing an even cardinality subset of the roots of g. Such polynomials will be distinct since g is generic. Since there are 2^d subsets of the roots of g and half of them have even cardinality, the theorem follows. □

Example 2.1.6. *Let $g(x) = (x-2)(x-3)(x-5) = x^3 - 10\,x^2 + 31\,x - 30$. Then, there are $2^{3-1} - 1 = 3$ other degree 3 polynomials with the same set of cyclic resultants as g. They are:*

$$15\,x^3 - 38\,x^2 + 17\,x - 2$$

$$10\,x^3 - 37\,x^2 + 22\,x - 3$$

$$6\,x^3 - 35\,x^2 + 26\,x - 5. \quad \square$$

If one is interested in the case of generic monic polynomials, then Theorem 2.1.1 also implies the following uniqueness result.

Corollary 2.1.7. *The set of cyclic resultants determines g for generic monic $g \in \mathbb{C}[x]$ of degree d.*

Proof. Again, since g is generic, it will not have a root of unity as a zero nor will $g(0) = 0$. Theorem 2.1.1 forces a constraint on the roots of g for there to be a different monic polynomial f with the same set of cyclic resultants as g. Namely, a subset of the roots of g has product 1, a non-generic situation. □

As to be expected, there are analogs of Theorem 2.1.1 and Corollary 2.1.7 to the real case involving absolute values.

Theorem 2.1.8. *Let f and g be polynomials in $\mathbb{R}[x]$. If f and g generate the same sequence of nonzero cyclic resultant absolute values, then there exist $u, v \in \mathbb{C}[x]$ with $u(0) \neq 0$ and nonnegative integers l_1, l_2 such that*

$$\begin{aligned} f(x) &= \pm\, x^{l_1} v(x) u(x^{-1}) x^{\deg(u)} \\ g(x) &= x^{l_2} v(x) u(x). \end{aligned}$$

Corollary 2.1.9. *The set of cyclic resultant absolute values determines g for generic monic $g \in \mathbb{R}[x]$ of degree d.*

The generic real case without the monic assumption is more subtle than that of Corollary 2.1.5. The difficulty is that we are restricted to polynomials in $\mathbb{R}[x]$. However, there is the following

Corollary 2.1.10. *Let g be a generic polynomial in the set of degree d elements of $\mathbb{R}[x]$ with at most one real root. Then there are exactly $2^{\lceil d/2 \rceil + 1}$ degree d polynomials in $\mathbb{R}[x]$ with the same set of cyclic resultant absolute values as g.*

Proof. If d is even, then the hypothesis implies that all of the roots of g are nonreal. In particular, it follows from Theorem 2.1.8 (and genericity) that any other degree d polynomial $f \in \mathbb{R}[x]$ giving rise to the same set of cyclic resultant absolute values is determined by choosing a subset of the $d/2$ pairs of conjugate roots of g and a sign. This gives us a count of $2^{d/2+1}$ distinct real polynomials. When d is odd, g has exactly one real root, and a similar counting argument gives us $2^{\lceil d/2 \rceil+1}$ for the number of distinct real polynomials in this case. This proves the corollary. □

A surprising consequence of this result is that the number of polynomials with equal sets of cyclic resultant absolute values can be significantly smaller than the number predicted by Corollary 2.1.5.

Example 2.1.11. *Let $g(x) = (x-2)(x+i+2)(x-i+2) = x^3+2\,x^2-3\,x-10$. Then, there are $2^{\lceil 3/2 \rceil+1} - 1 = 7$ other degree 3 real polynomials with the same set of cyclic resultant absolute values as g. They are:*

$$-x^3-2\,x^2+3\,x+10,\ \pm(-2\,x^3-7\,x^2-6\,x+5),$$

$$\pm(5\,x^3-6\,x^2-7\,x-2),\ \pm(-10\,x^3-3\,x^2+2\,x+1).$$

It is important to realize that while

$$\begin{aligned} f(x) &= (1-2x)(1+(i+2)x)(x-i+2) \\ &= (-4-2\,i)\,x^3-(10-i)\,x^2+(2+2\,i)\,x+2-i \end{aligned}$$

has the same set of actual cyclic resultants (by Theorem 2.1.1), it does not appear in the count above since it is not in $\mathbb{R}[x]$. □

As an illustration of the usefulness of Theorem 2.1.1, we prove a uniqueness result involving cyclic resultants of reciprocal polynomials. Fried's result also follows in the same way using Theorem 2.1.8 in place of Theorem 2.1.1.

Corollary 2.1.12. *Let f and g be reciprocal polynomials with equal sets of nonzero cyclic resultants. Then, $f = g$.*

Proof. Let f and g be as in the statement of the corollary. Applying Theorem 2.1.1, it follows that $d = \deg(f) = \deg(g)$ and that

$$\begin{aligned} f(x) &= v(x)u(x^{-1})x^{\deg(u)} \\ g(x) &= v(x)u(x) \end{aligned}$$

($l_1 = l_2 = 0$ since $f(0), g(0) \neq 0$). But then,

$$\begin{aligned}\frac{u(x^{-1})}{u(x)} x^{\deg(u)} &= \frac{f(x)}{g(x)} \\ &= \frac{x^d f(x^{-1})}{x^d g(x^{-1})} \\ &= \frac{u(x)}{u(x^{-1})} x^{-\deg(u)}.\end{aligned}$$

In particular, $u(x) = \pm u(x^{-1}) x^{\deg(u)}$. If $u(x) = u(x^{-1}) x^{\deg(u)}$, then $f = g$ as desired. In the other case, it follows that $f = -g$. But then $\mathrm{Res}(f,x-1) = \mathrm{Res}(g,x-1) = -\mathrm{Res}(f,x-1)$ is a contradiction to f having all nonzero cyclic resultants. This completes the proof. □

We now state the application to toral endomorphims discussed in the introduction.

Corollary 2.1.13. *Let T be an ergodic, toral endomorphism induced by a $d \times d$ integer matrix A. If there is no subset of the eigenvalues of A with product ± 1, then the sequence $|\mathrm{Per}_m(T)|$ determines the spectrum of the linear map that defines T.*

Proof. Suppose that T' is another toral endomorphism induced by an integral $d \times d$ matrix B such that

$$|\mathrm{Per}_m(T)| = |\mathrm{Per}_m(T')|.$$

Let f and g be the characteristic polynomials of A and B, respectively. From the hypothesis of the corollary and the statement of Theorem 2.1.8, it follows that f and g must be equal. In particular, the eigenvalues of the matrices A and B coincide, completing the proof. □

Remark 2.1.14. We note that a more complete characterization is possible using the results of Theorem 2.1.8, however, the statement is more technical and not very enlightening.

When a degree d polynomial is uniquely determined by its sequence of cyclic resultants, it is natural to ask for an algorithm that performs the reconstruction. In several applications, moreover, explicit inversion using small numbers of resultants is desired (see, for instance, [35, 37]). In Section 2.5, we describe a method that inverts the map r using the first 2^{d+1} cyclic resultants. Empirically, however, only $d+1$ resultants suffice, and a conjecture by Sturmfels and Zworski would imply that this is always the case. As evidence for this conjecture, we provide explicit reconstructions for several small examples.

The rest of this chapter is organized as follows. In Section 2.2, we make a digression into the theory of semigroup algebras and binomial factorizations. The unique factorization result discussed there (Theorem 2.2.10) will form a crucial component in the proof of Theorem 2.1.1. The subsequent chapter deals with algebraic properties of cyclic resultants, and Section 2.5 concludes with proofs of our main cyclic resultant characterization theorems. Finally, in the last section, we discuss algorithms for reconstruction.

2.2 Binomial Factorizations

We now switch to the seemingly unrelated topic of binomial factorizations in group algebras. The relationship to cyclic resultants will become clear later. We begin with a very general situation. Let G be a group and let $\mathbb{Z}G$ be the group algebra over $\mathbb{Z}$. In the following definition (which appears to be new), we view $\mathbb{R}$ as a group under addition.

Definition 2.2.1. Let G be group and let $S \subset G$. The set S is called *nonderogatory* if for each finitely generated subgroup H containing a subset $\{g_1, \ldots, g_n\} \subset S$, there is a group homomorphism $\phi : H \to \mathbb{R}$ such that $\phi(g_i) \neq 0$ for all i.

Obviously, not every set of group elements has this property – for instance, if any of the elements of S have torsion. Less trivial non-examples can be found by taking triples $g, h, ghg^{-1}h^{-1}$ of torsion-free elements in a group G. Nevertheless, nonderogatory sets are relatively easy to find. For a simple example, consider $G = GL_n(\mathbb{C})$. There is a natural homomorphism $\phi : G \to \mathbb{R}$ given by

$$\phi(A) = \log|\det(A)|. \tag{2.2.1}$$

We then have the following

Example 2.2.2. *The set of elements of $GL_n(\mathbb{C})$ with determinants outside the unit circle (in the complex plane) is nonderogatory.*

More examples can be generated using the following lemma. Intuitively, it says that these objects are closed under taking a conjugate closure.

Lemma 2.2.3. *Let S be a nonderogatory set for a group G and let $T \subset G$. Then,*

$$\{tst^{-1} : t \in T, s \in S\}$$

is a nonderogatory subset of G.

Proof. Let S be as in the lemma and let $t_i \in T, s_i \in S$ for $i = 1, \ldots, n$. For a finitely generated subgroup H that contains $\{t_1 s_1 t_1^{-1}, \ldots, t_n s_n t_n^{-1}\}$, we must exhibit a homomorphism $\phi : H \to \mathbb{R}$ with $\phi(t_i s_i t_i^{-1}) \neq 0$ for all i. Consider the finitely generated group,

$$\widetilde{H} = \langle h, s_i, t_i : h \in H,\ i = 1, \ldots, n\rangle.$$

Since S is nonderogatory, there is a homomorphism $\psi : \widetilde{H} \to \mathbb{R}$ with $\psi(s_i) \neq 0$ for all i. Clearly, $H \subseteq \widetilde{H}$, and since $\psi(t_i s_i t_i^{-1}) = \psi(s_i)$, it follows that ψ restricted to H satisfies our requirements. This completes the proof. □

Later, we shall be able to give a complete characterization of nonderogatory subsets in the Abelian case (Proposition 2.2.9). We now give the factorization motivation for our definition.

Recall that two elements $x, y \in G$ are called *conjugate* (denoted $x \sim y$) if there exists $z \in G$ such that $x = zyz^{-1}$. The following definition explains what we shall mean by unique factorization of binomials.

Definition 2.2.4. A subset S of a group G has the *unique binomial factorization* property if the existence of a factorization

$$a \prod_{i=1}^{m} (g_i - h_i) = b \prod_{i=1}^{n} (u_i - v_i), \quad a, b \in \mathbb{Z},\ g_i^{-1} h_i, u_i^{-1} v_i \in S$$

in $\mathbb{Z}G$ implies that $a = \pm b$, $m = n$, and that up to permutation, for each i, there are elements $c_i \in G$ such that $(g_i - h_i) \sim \pm c_i (u_i - v_i)$.

Example 2.2.5. *To illustrate the need for conjugation in the definition, consider the identity*

$$(u-v)(w-x)(y-z) = (uwy - vwy)(1 - y^{-1}w^{-1}xy)(1 - y^{-1}z),$$

which holds in any group algebra. One can then check that

$$\begin{aligned}(u-v) &= wy(y^{-1}w^{-1})(uwy - vwy)y^{-1}w^{-1}\\ (w-x) &= y(y^{-1}wy)(1 - y^{-1}w^{-1}xy)y^{-1}\\ (y-z) &= y(1 - y^{-1}z). \quad \square\end{aligned}$$

The main conjecture of this section would provide a sufficient condition for unique factorizations of binomials in a group algebra.

Conjecture 2.2.6. *Nonderogatory subsets of a group G have the unique binomial factorization property.*

The following unique factorization result would be a direct consequence of Theorem 3.1.3.

Conjecture 2.2.7. *The set of elements of $GL_n(\mathbb{C})$ with determinants outside the unit circle (in the complex plane) have the unique factorization property.*

We should remark that there are obstructions to unique factorization that make necessary some kind of supplemental hypothesis. For example, when $G = \mathbb{Z}/2\mathbb{Z}$, we have $\mathbb{Z}G \cong \mathbb{Z}[s]/\langle s^2 - 1\rangle$, and it is easily verified that

$$(1-s)(1-s) = 2(1-s).$$

One might also wonder what happens when the binomials are not of the form $g - h$. The following example exhibits some of the difficulty in formulating a general statement.

Example 2.2.8. *Let $G = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ so that $\mathbb{Z}G \cong \mathbb{Z}[s,t,t^{-1}]/\langle s^2 - 1\rangle$. Then,*

$$(1-t^4) = (1-t^2)(1+t^2) = (1-st^2)(1+st^2)$$

are three different binomial factorizations of the same element. $\square$

We now proceed to give a proof of Conjecture 2.2.6 in the Abelian case, essentially by giving a characterization of nonderogatory sets.

Let A be a finitely generated abelian group and let $a_1, \ldots, a_n$ be distinguished generators of A. Let Q be the semigroup generated by $a_1, \ldots, a_n$. The *semigroup algebra* $\mathbb{Z}[Q]$ is the $\mathbb{Z}$-algebra with $\mathbb{Z}$-basis $\{\mathbf{s}^a : a \in Q\}$ and multiplication defined by $\mathbf{s}^a \cdot \mathbf{s}^b = \mathbf{s}^{a+b}$. Let L denote the kernel of the homomorphism $\mathbb{Z}^n$ onto A. The *lattice ideal* associated with L is the following ideal in $S = \mathbb{Z}[x_1, \ldots, x_n]$:

$$I_L = \langle x^{\boldsymbol{u}} - x^{\boldsymbol{v}} \ : \ \boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}^n \text{ with } \boldsymbol{u} - \boldsymbol{v} \in L \rangle.$$

It is well-known that $\mathbb{Z}[Q] \cong S/I_L$ (e.g. see [46]). Our main theorems are the following.

Theorem 2.2.9. *For a subset S of an Abelian group G the following are equivalent:*

(1) *S is nonderogatory*

(2) *S consists only of torsion-free elements*

Theorem 2.2.10. *Nonderogatory subsets of Abelian groups have the unique binomial factorization property.*

To prove our main results, we will pass to the group algebra $\mathbb{Q}[A]$. As above, we represent elements $\tau \in \mathbb{Q}[A]$ as $\tau = \sum_{i=1}^{m} \alpha_i \mathbf{s}^{g_i}$, in which $\alpha_i \in \mathbb{Q}$ and $g_i \in A$. The following lemma is quite well-known.

Lemma 2.2.11. *If $0 \neq \alpha \in \mathbb{Q}$ and $g \in A$ has infinite order, then $1 - \alpha \boldsymbol{s}^g \in \mathbb{Q}[A]$ is not a zero-divisor.*

Proof. Let $0 \neq \alpha \in \mathbb{Q}, g \in A$ and $\tau = \sum_{i=1}^{m} \alpha_i \mathbf{s}^{g_i} \neq 0$ be such that

$$\tau = \alpha \mathbf{s}^g \tau = \alpha^2 \mathbf{s}^{2g} \tau = \alpha^3 \mathbf{s}^{3g} \tau = \cdots .$$

Suppose that $\alpha_1 \neq 0$. Then, the elements $\mathbf{s}^{g_1}, \mathbf{s}^{g_1+g}, \mathbf{s}^{g_1+2g}, \ldots$ appear in τ with nonzero coefficient, and since g has infinite order, these elements are all distinct. It follows, therefore, that τ cannot be a finite sum, and this contradiction finishes the proof. □

Since the proof of the main theorem involves multiple steps, we record several facts that will be useful later. The first result is a verification of the factorization theorem for a special case.

Lemma 2.2.12. *Fix an abelian group C. Let $\mathbb{Q}[C]$ be the group algebra with $\mathbb{Q}$-basis given by $\{\boldsymbol{s}^c : c \in C\}$ and set $R = \mathbb{Q}[C][t, t^{-1}]$. Suppose that $c_i, d_i, b \in C$, m_i, n_i are nonzero integers, $q \in \mathbb{Z}$, and $z \in \mathbb{Q}$ are such that*

$$\prod_{i=1}^{e} (1 - \boldsymbol{s}^{c_i} t^{m_i}) = z \boldsymbol{s}^b t^q \prod_{i=1}^{f} (1 - \boldsymbol{s}^{d_i} t^{n_i})$$

holds in R. Then, $e = f$ and after a permutation, for each i, either $\boldsymbol{s}^{c_i} t^{m_i} = \boldsymbol{s}^{d_i} t^{n_i}$ or $\boldsymbol{s}^{c_i} t^{m_i} = \boldsymbol{s}^{-d_i} t^{-n_i}$.

Proof. Let $\operatorname{sgn} : \mathbb{Z} \setminus \{0\} \to \{-1, 1\}$ denote the standard sign map $\operatorname{sgn}(n) = n/|n|$ and set $\gamma = z \mathbf{s}^b t^q$. Rewrite the left-hand side of the given equality as:

$$\prod_{i=1}^{e} (1 - \mathbf{s}^{c_i} t^{m_i}) = \prod_{\operatorname{sgn}(m_i) = -1} -\mathbf{s}^{c_i} t^{m_i} \prod_{i=1}^{e} \left(1 - \mathbf{s}^{\operatorname{sgn}(m_i) c_i} t^{|m_i|}\right).$$

Similarly for the right-hand side, we have:

$$\prod_{i=1}^{f} \left(1 - \mathbf{s}^{d_i} t^{n_i}\right) = \prod_{\operatorname{sgn}(n_i) = -1} -\mathbf{s}^{d_i} t^{n_i} \prod_{i=1}^{f} \left(1 - \mathbf{s}^{\operatorname{sgn}(n_i) d_i} t^{|n_i|}\right).$$

Next, set

$$\eta = \gamma \prod_{\operatorname{sgn}(m_i) = -1} -\mathbf{s}^{-c_i} t^{-m_i} \prod_{\operatorname{sgn}(n_i) = -1} -\mathbf{s}^{d_i} t^{n_i}$$

so that our original equation may be written as

$$\prod_{i=1}^{e} \left(1 - \mathbf{s}^{\operatorname{sgn}(m_i) c_i} t^{|m_i|}\right) = \eta \prod_{i=1}^{f} \left(1 - \mathbf{s}^{\operatorname{sgn}(n_i) d_i} t^{|n_i|}\right).$$

Comparing the lowest degree term (with respect to t) on both sides, it follows that $\eta = 1$. It is enough, therefore, to prove the claim in the case when

$$\prod_{i=1}^{e} (1 - \mathbf{s}^{c_i} t^{m_i}) = \prod_{i=1}^{f} \left(1 - \mathbf{s}^{d_i} t^{n_i}\right) \tag{2.2.2}$$

and the m_i, n_i are positive. Without loss of generality, suppose the lowest degree non-constant term on both sides of (2.2.2) is t^{m_1} with coefficient $-\mathbf{s}^{c_1} - \cdots - \mathbf{s}^{c_u}$ on the left and $-\mathbf{s}^{d_1} - \cdots - \mathbf{s}^{d_v}$ on the right. Here, u (resp. v) corresponds to the number of m_i (resp. n_i) with $m_i = m_1$ (resp. $n_i = m_1$).

Since the set of distinct monomials $\{\mathbf{s}^c : c \in C\}$ is a $\mathbb{Q}$-basis for the ring $\mathbb{Q}[C]$, equality of the t^{m_1} coefficients above implies that $u = v$ and that up to permutation, $\mathbf{s}^{c_j} = \mathbf{s}^{d_j}$ for $j = 1, \ldots, u$. Lemma 2.2.11 and induction complete the proof. □

Lemma 2.2.13. *Let $P = (p_{ij})$ be a $d \times n$ integer matrix such that every row has at least one nonzero integer. Then, there exists $\boldsymbol{v} \in \mathbb{Z}^n$ such that the vector $P\boldsymbol{v}$ does not contain a zero entry.*

Proof. Let P be a $d \times n$ integer matrix as in the hypothesis of the lemma, and for $h \in \mathbb{Z}$, let $\boldsymbol{v}_h = (1, h, h^2, \ldots, h^{n-1})^T$. Assume, by way of contradiction, that $P\boldsymbol{v}$ contains a zero entry for all $\boldsymbol{v} \in \mathbb{Z}^n$. Then, in particular, this is true for all $\boldsymbol{v}_h$ as above. By the (infinite) pigeon-hole principle, there exists an infinite set of $h \in \mathbb{Z}$ such that (without loss of generality) the first entry of $P\boldsymbol{v}_h$ is zero. But then,

$$f(h) := \sum_{i=1}^{n} p_{1i} h^{i-1} = 0$$

for infinitely many values of h. It follows, therefore, that $f(h)$ is the zero polynomial, contradicting our hypothesis and completing the proof. □

Lemma 2.2.13 will be useful in verifying the following fact.

Lemma 2.2.14. *Let A be a finitely generated abelian group and $a_1, \ldots, a_d$ elements in A of infinite order. Then, there exists a homomorphism $\phi : A \to \mathbb{Z}$ such that $\phi(a_i) \neq 0$ for all i.*

Proof. Write $A = B \oplus C$, in which C is a finite group and B is free of rank n. If $n = 0$, then there are no elements of infinite order; therefore, we may assume that the rank of B is positive. Since $a_1, \ldots, a_d$ have infinite order, their images in the natural projection $\pi : A \to B$ are nonzero. It follows that we may assume that A is free and a_i are nonzero elements of A.

Let $e_1, \ldots, e_n$ be a basis for A, and write

$$a_t = p_{t1} e_1 + \cdots + p_{tn} e_n$$

for (unique) integers $p_{ij} \in \mathbb{Z}$. To determine a homomorphism $\phi : A \to \mathbb{Z}$ as in the lemma, we must find integers $\phi(e_1), \dots, \phi(e_n)$ such that

$$\begin{aligned} 0 &\neq p_{11}\phi(e_1) + \cdots + p_{1n}\phi(e_n) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0 &\neq p_{d1}\phi(e_1) + \cdots + p_{dn}\phi(e_n). \end{aligned} \tag{2.2.3}$$

This, of course, is precisely the consequence of Lemma 2.2.13 applied to the matrix $P = (p_{ij})$, finishing the proof. □

Recall that a *trivial unit* in the group ring $\mathbb{Q}[A]$ is an element of the form $\alpha\mathbf{s}^a$ in which $0 \neq \alpha \in \mathbb{Q}$ and $a \in A$. The main content of Theorem 2.2.9 is contained in the following result. The technique of embedding $\mathbb{Q}[A]$ into a Laurent polynomial ring is also used by Fried in [17].

Lemma 2.2.15. *Let A be an abelian group. Two factorizations in $\mathbb{Q}[A]$,*

$$\prod_{i=1}^{e} (1 - \boldsymbol{s}^{g_i}) = \eta \prod_{i=1}^{f} \left(1 - \boldsymbol{s}^{h_i}\right),$$

in which η is a trivial unit and $g_i, h_i \in A$ all have infinite order are equal if and only if $e = f$ and there is some nonnegative integer p such that, up to permutation,

(1) *$g_i = h_i$ for $i = 1, \dots, p$*

(2) *$g_i = -h_i$ for $i = p+1, \dots, e$*

(3) *$\eta = (-1)^{e-p}\boldsymbol{s}^{g_{p+1}+\cdots+g_e}$.*

Proof. The if-direction of the claim is a straightforward calculation. Therefore, suppose that one has two factorizations as in the lemma. It is clear we may assume that A is finitely generated. By Lemma 2.2.14, there exists a homomorphism $\phi : A \to \mathbb{Z}$ such that $\phi(g_i), \phi(h_i) \neq 0$ for all i. The ring $\mathbb{Q}[A]$ may be embedded into the Laurent ring, $R = \mathbb{Q}[A][t, t^{-1}]$, by way of

$$\psi\left(\sum_{i=1}^{m} \alpha_i \mathbf{s}^{a_i}\right) = \sum_{i=1}^{m} \alpha_i \mathbf{s}^{a_i} t^{\phi(a_i)}.$$

Write $\eta = \alpha \mathbf{s}^b$. Then, applying this homomorphism to the original factorization, we have

$$\prod_{i=1}^{e} \left(1 - \mathbf{s}^{g_i} t^{\phi(g_i)}\right) = \alpha \mathbf{s}^b t^{\phi(b)} \prod_{i=1}^{f} \left(1 - \mathbf{s}^{h_i} t^{\phi(h_i)}\right).$$

Lemma 2.2.12 now applies to give us that $e = f$ and there is an integer p such that up to permutation,

(1) $g_i = h_i$ for $i = 1, \dots, p$

(2) $g_i = -h_i$ for $i = p+1, \dots, e$.

We are therefore left with verifying statement (3) of the lemma. Using Lemma 2.2.11, we may cancel equal terms in our original factorization, leaving us with the following equation:

$$\begin{aligned}\prod_{i=p+1}^{e} (1 - \mathbf{s}^{g_i}) &= \eta \prod_{i=p+1}^{e} (1 - \mathbf{s}^{-g_i}) \\ &= \eta(-1)^{e-p} \prod_{i=p+1}^{e} \mathbf{s}^{-g_i} \prod_{i=p+1}^{e} (1 - \mathbf{s}^{g_i}).\end{aligned}$$

Finally, one more application of Lemma 2.2.11 gives us that $\eta = (-1)^{e-p} \mathbf{s}^{g_{p+1} + \cdots + g_e}$ as desired. This finishes the proof. □

Our main theorems are now immediate from what we have done.

Proof of Theorem 2.2.9. (1) ⇒ (2) is clear from the definition and (2) ⇒ (1) follows directly from Lemma 2.2.14. □

Proof of Theorem 2.2.10. Suppose that

$$\mathbf{s}^a \prod_{i=1}^{e} (\mathbf{s}^{u_i} - \mathbf{s}^{v_i}) = \alpha \mathbf{s}^b \prod_{i=1}^{f} (\mathbf{s}^{x_i} - \mathbf{s}^{y_i})$$

are two factorizations in the ring $\mathbb{Q}[A]$. Factor each element of the form $(\mathbf{s}^u - \mathbf{s}^v)$ as $\mathbf{s}^u (1 - \mathbf{s}^{v-u})$. By assumption and Theorem 2.2.9, each such $v - u$ has infinite order. Now, apply Lemma 2.2.15, giving us that $\alpha = \pm 1$, $e = f$, and that after a permutation, for each i either $\mathbf{s}^{v_i - u_i} = \mathbf{s}^{y_i - x_i}$ or $\mathbf{s}^{v_i - u_i} = \mathbf{s}^{x_i - y_i}$. It easily follows from this that for each i, there are elements $c_i \in A$ such that $(\mathbf{s}^{u_i} - \mathbf{s}^{v_i}) = \pm \mathbf{s}^{c_i} (\mathbf{s}^{x_i} - \mathbf{s}^{y_i})$. This completes the proof of the theorem. □

Finally, to close this section, we offer the following open problem.

Conjecture 2.2.16. *The torsion-free elements of an arbitrary group have the unique binomial factorization property.*

2.3 Cyclic Resultants and Rational Functions

We begin with some preliminaries concerning cyclic resultants. Let $f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_d$ be a degree d polynomial over $\mathbb{C}$, and let the companion matrix for f be given by:

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_d/a_0 \\ 1 & 0 & \cdots & 0 & -a_{d-1}/a_0 \\ 0 & 1 & \cdots & 0 & -a_{d-2}/a_0 \\ 0 & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1/a_0 \end{bmatrix}.$$

Also, let I denote the $d \times d$ identity matrix. Then, we may write [8, p. 77]

$$r_m = a_0^m \det (A^m - I). \tag{2.3.1}$$

This equation can also be expressed as,

$$r_m = a_0^m \prod_{i=1}^{d} (\alpha_i^m - 1), \tag{2.3.2}$$

in which $\alpha_1, \ldots, \alpha_d$ are the roots of $f(x)$.

Let $e_i(y_1, \ldots, y_d)$ be the i-th elementary symmetric function in the variables $y_1, \ldots, y_d$ (we set $e_0 = 1$). Then, we know that $a_i = (-1)^i a_0 e_i(\alpha_1, \ldots, \alpha_d)$ and that

$$r_m = a_0^m \sum_{i=0}^{d} (-1)^i e_{d-i} (\alpha_1^m, \ldots, \alpha_d^m). \tag{2.3.3}$$

We first record an auxiliary result.

Lemma 2.3.1. *Let* $F_k(z) = \prod_{1 \le i_1 < \cdots < i_k \le d} (1 - a_0\alpha_{i_1} \cdots \alpha_{i_k} z)$ *with* $F_0(z) = 1 - a_0 z$. *Then,*

$$\sum_{m=1}^{\infty} a_0^m e_k (\alpha_1^m, \ldots, \alpha_d^m) z^m = -z \cdot \frac{F_k'}{F_k},$$

in which F_k' *denotes* $\frac{dF_k}{dz}$.

Proof. For $k = 0$, the equation is easily verified. When $k > 0$, the calculation is still fairly straightforward:

$$\begin{aligned}
\sum_{m=1}^{\infty} a_0^m e_k\left(\alpha_1^m, \ldots, \alpha_d^m\right) z^m &= \sum_{m=1}^{\infty} \sum_{i_1 < \cdots < i_k} a_0^m \alpha_{i_1}^m \cdots \alpha_{i_k}^m \cdot z^m \\
&= \sum_{i_1 < \cdots < i_k} \sum_{m=1}^{\infty} a_0^m \alpha_{i_1}^m \cdots \alpha_{i_k}^m \cdot z^m \\
&= \sum_{i_1 < \cdots < i_k} \frac{a_0 \alpha_{i_1} \cdots \alpha_{i_k} z}{1 - a_0 \alpha_{i_1} \cdots \alpha_{i_k} z} \\
&= \frac{-z \cdot \frac{d}{dz}\left[\prod_{i_1 < \cdots < i_k} \left(1 - a_0 \alpha_{i_1} \cdots \alpha_{i_k} z\right)\right]}{\prod_{i_1 < \cdots < i_k} \left(1 - a_0 \alpha_{i_1} \cdots \alpha_{i_k} z\right)} \\
&= -z \cdot \frac{F_k'}{F_k}.
\end{aligned}$$

□

We are now ready to state and prove a rationality result for cyclic resultants.

Lemma 2.3.2. *$R_f(z) = \sum_{m=1}^{\infty} r_m z^m$ is a rational function in z.*

Proof. We simply compute that

$$\begin{aligned}
\sum_{m=1}^{\infty} r_m z^m &= \sum_{m=1}^{\infty} \sum_{i=0}^{d} (-1)^i a_0^m e_{d-i}\left(\alpha_1^m, \ldots, \alpha_d^m\right) \cdot z^m \\
&= \sum_{i=0}^{d} (-1)^i \sum_{m=1}^{\infty} a_0^m e_{d-i}\left(\alpha_1^m, \ldots, \alpha_d^m\right) \cdot z^m \\
&= -z \cdot \sum_{i=0}^{d} (-1)^i \cdot \frac{F_{d-i}'}{F_{d-i}}.
\end{aligned}$$

□

Manipulating the expression for $R_f(z)$ occurring in Lemma 2.3.2, we also have the following fact.

Corollary 2.3.3. *If d is even, let $G_d = \frac{F_d F_{d-2} \cdots F_0}{F_{d-1} F_{d-3} \cdots F_1}$ and if d is odd, let $G_d = \frac{F_d F_{d-2} \cdots F_1}{F_{d-1} F_{d-3} \cdots F_0}$. Then,*

$$\sum_{m=1}^{\infty} r_m z^m = -z \frac{G_d'}{G_d}.$$

In particular, it follows that

$$\exp\left(-\sum_{m=1}^{\infty} r_m \frac{z^m}{m} \right) = G_d. \tag{2.3.4}$$

Example 2.3.4. *Let $f(x) = x^2 - 5x + 6 = (x-2)(x-3)$. Then, $r_m = (2^m - 1)(3^m - 1)$ and $F_0(z) = 1 - z$, $F_1(z) = (1-2z)(1-3z)$, $F_2(z) = 1 - 6z$. Thus,*

$$R_f(z) = -z \left(\frac{F_2'}{F_2} - \frac{F_1'}{F_1} + \frac{F_0'}{F_0} \right) = \frac{6z}{1-6z} - \frac{2z}{1-2z} - \frac{3z}{1-3z} + \frac{z}{1-z}$$

and

$$\exp\left(-\sum_{m=1}^{\infty} r_m \frac{z^m}{m} \right) = \frac{(1-6z)(1-z)}{(1-2z)(1-3z)}. \quad \square$$

Following [17], we discuss how to deal with absolute values in the real case. Let $f \in \mathbb{R}[x]$ have degree d such that the r_m as defined above are all nonzero. We examine the sign of r_m using equation (2.3.2). First notice that a complex conjugate pair of roots of f does not affect the sign of r_m. A real root α of f contributes a sign factor of $+1$ if $\alpha > 1$, -1 if $-1 < \alpha < 1$, and $(-1)^m$ if $\alpha < -1$. Let E be the number of zeroes of f in $(-1, 1)$ and let D be the number of zeroes in $(-\infty, -1)$. Also, set $\epsilon = (-1)^E$ and $\delta = (-1)^D$. Then, it follows that

$$\frac{r_m}{|r_m|} = \epsilon \cdot \delta^m. \tag{2.3.5}$$

In particular,

$$|r_m| = \epsilon (\delta a_0)^m \prod_{i=1}^{d} (\alpha_i^m - 1). \tag{2.3.6}$$

In other words, the sequence of $|r_m|$ is obtained by multiplying each cyclic resultant of the polynomial $\tilde{f} := \delta f = \delta a_0 x^d + \delta a_1 x^{d-1} + \cdots + \delta a_d$ by ϵ. Denoting by $\widetilde{G}_d$ the rational function determined by $\tilde{f}$ as in (2.3.3), it follows that

$$\exp\left(-\sum_{m=1}^{\infty} |r_m| \frac{z^m}{m} \right) = \left(\widetilde{G}_d \right)^{\epsilon}. \tag{2.3.7}$$

2.4 Proofs of the Main Theorems

In this section, we discuss how the problem of binomial factorization arises in a natural way from the study of cyclic resultants. Let S denote the ring of sequences over $\mathbb{C}$ under pointwise sum and product, and for $\mu \in \mathbb{C}$, let $e(\mu)$ denote the exponential sequence $e(\mu)_n = \mu^n$ $(n \geq 1)$. With this identification, the infinite number of expressions (2.3.2) (similarly for (2.3.6)) can be represented succinctly by

$$e(a_0) \prod_{i=1}^{d} (e(\alpha_i) - 1) \in S. \tag{2.4.1}$$

Let $G = \mathbb{C}^*$ be the multiplicative group generated by nonzero elements of $\mathbb{C}$. Because of the multiplicative structure of G, we represent $\mathbb{Z}$-basis elements of the group ring $\mathbb{Z}[G]$ as $[\mu]$, $\mu \in G$; multiplication is given by $[\mu] \cdot [\nu] = [\mu\nu]$. The map $e : \mathbb{Z}[G] \to S$ sending $[\mu] \mapsto e(\mu)$ (and extended by linearity) is an embedding of $\mathbb{Z}$-algebras, as the following lemma shows.

Lemma 2.4.1. *The map $e : \mathbb{Z}[G] \to S$ sending $[\mu] \mapsto e(\mu)$ is an injective homomorphism.*

Proof. Since $e(\mu)e(\nu) = e(\mu\nu)$, the map e is an algebra homomorphism. Injectivity follows since the exponential sequences $e(\mu_1)$, …, $e(\mu_m)$ are linearly independent for distinct $\mu_i \in G$ (the determinant $|e(\mu_i)_j|_{i,j=1}^{m}$ is Vandermonde). □

From these remarks, it follows that determining when two polynomials produce equal sequences of cyclic resultants reduces to solving a problem in binomial factorization. We are now ready to complete the proofs of our main characterization theorems for cyclic resultants.

Proof of Theorem 2.1.1. Let f and g be polynomials as in the hypothesis, and suppose that the multiplicity of 0 as a root of f (resp. g) is l_1 (resp. l_2). Then, $f(x) = x^{l_1}(a_0x^{d_1} + \cdots + a_{d_1})$ and $g(x) = x^{l_2}(b_0x^{d_2} + \cdots + b_{d_2})$ in which a_0 and b_0 are not 0. Let $\alpha_1, \ldots, \alpha_{d_1}$ and $\beta_1, \ldots, \beta_{d_2}$ be the nonzero roots of f and g, respectively, and let G be the multiplicative group generated by these elements along with a_0, b_0. Since f and g

both generate the same sequence of cyclic resultants, it follows from (2.4.1) and Lemma 2.4.1 that we have an equality of factorizations

$$(-1)^{d_1+l_1}[a_0]\prod_{i=1}^{d_1}(1-[\alpha_i]) = (-1)^{d_2+l_2}[b_0]\prod_{i=1}^{d_2}(1-[\beta_i]).$$

Since we have assumed that f and g generate a set of nonzero cyclic resultants, neither of them can have a root of unity as a zero. Therefore, Lemma 2.2.15 applies to give us that $d := d_1 = d_2$ and that up to a permutation, there is a nonnegative integer p such that

(1) $\alpha_i = \beta_i$ for $i = 1, \ldots, p$

(2) $\alpha_i = \beta_i^{-1}$ for $i = p+1, \ldots, d$

(3) $(-1)^{d-p} = (-1)^{l_2-l_1}$, $a_0 b_0^{-1} = \beta_{p+1}\cdots\beta_d$.

Set $u(x) = (x-\beta_{p+1})\cdots(x-\beta_d)$ which has $\deg(u) \equiv l_2 - l_1 \pmod 2$, and let $v(x) = b_0(x-\beta_1)\cdots(x-\beta_p)$ (note that if $p = 0$, then $v(x) = b_0$) so that $g(x) = x^{l_2}v(x)u(x)$. Now,

$$u(x^{-1})x^{\deg(u)} = (-1)^{d-p}\beta_{p+1}\cdots\beta_d(x-\beta_{p+1}^{-1})\cdots(x-\beta_d^{-1}),$$

and thus

$$\begin{aligned} f(x) &= x^{l_1}a_0b_0^{-1}v(x)(x-\beta_{p+1}^{-1})\cdots(x-\beta_d^{-1}) \\ &= (-1)^{l_2-l_1}x^{l_1}v(x)u(x^{-1})x^{\deg(u)}. \end{aligned}$$

Finally, the converse is straightforward from (2.3.2), completing the proof of the theorem. □

The proof of Theorem 2.1.8 is similar, employing equation (2.3.6) in place of (2.3.2).

Proof of Theorem 2.1.8. Since multiplication of a real polynomial by a power of x does not change the absolute value of a cyclic resultant, we may assume $f, g \in \mathbb{R}[x]$ have nonzero roots. The result now follows from (2.3.6) and the argument used to prove the if-direction of Theorem 2.1.1. □

2.5 Reconstructing Dynamical Systems From Their Zeta Functions

In the final section of this chapter, we describe how to explicitly reconstruct a polynomial from its cyclic resultants. For an ergodic toral endomorphism as in the introduction, the sequence $|r_m|$ encodes the cardinalities of sets of periodic points. In particular, fixing the *zeta function*,

$$Z(T,z) = \exp\left(-\sum_{m=1}^{\infty} |\mathrm{Per}_m(T)| \frac{z^m}{m} \right),$$

of the dynamical system in question is another way of writing equation (2.3.7).

In many of the applications [11, 35, 37, 63], the defining polynomial is reciprocal, and the techniques discussed here restrict easily to this special case. Furthermore, since reciprocal polynomials are uniquely determined without any genericity assumptions (see Corollary 2.1.4 and Corollary 2.1.12), the computational organization is simpler.

Let $f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_d$ be a degree d polynomial with indeterminate coefficients a_i. We distinguish between two cases. In the first situation, the variable a_0 is replaced by 1 so that f is monic; while in the second, we set $a_i = a_{d-i}$ for $i = 1, \dots, d$ so that f is reciprocal.

Although the results mentioned in this paper only imply that the full sequence of cyclic resultants determine f when it is (generic) monic or reciprocal, a finite number of resultants is sufficient. Specifically, as detailed in forthcoming work [32], it is shown (using the results of this chapter) that 2^{d+1} resultants are enough. Empirical evidence suggests that this is far from tight, and a conjecture of Sturmfels and Zworski asserts the following.

Conjecture 2.5.1. *A generic monic polynomial $f(x) \in \mathbb{C}[x]$ of degree d is determined by its first $d+1$ cyclic resultants. Moreover, if f is (non-monic) reciprocal of even degree d, then the number of resultants needed for inversion is given by $d/2 + 2$.*

A straightforward algorithm for inverting N cyclic resultants is as follows. Its correctness when $N = 2^{d+1}$ follows from [8] and the results of [32].

Algorithm 2.5.2. *(Specific reconstruction of a polynomial from its cyclic resultants)*
Input: Positive integer d and a sequence of $r_1, \ldots, r_N \in \mathbb{C}$.
Output: The coefficients a_i $(i = 0, \ldots, d)$ corresponding to f.

(1) *Compute a lexicographic Gröbner basis $\mathcal{G}$ for the ideal*

$$I = \langle r_1 - \mathit{Res}(f, x-1), \ldots, r_N - \mathit{Res}(f, x^N - 1)\rangle.$$

(2) *Solve the resulting triangular system of equations for a_i using back substitution.*

□

If the data are given in terms of cyclic resultant absolute values (for the real case), then more care must be taken in implementing Algorithm 2.5.2. Examining expression (2.3.5), there are 2 possible sequences of viable r_m that come from a given sequence of (generically generated) cyclic resultant absolute values $|r_m|$; they are $\{|r_m|\}$ and $\{-|r_m|\}$. By the uniqueness in Corollaries 2.1.7 and 2.1.9, however, only one of these sequences can come from a monic polynomial. Therefore, the corresponding modification is to run Algorithm 2.5.2 on both these inputs. For one of these sequences, it will generate the Gröbner basis $\langle 1 \rangle$; while for the other, it will output the desired reconstruction.

Finding "universal" equations expressing the coefficients a_i in terms of the resultants r_i is also possible using a similar strategy.

Algorithm 2.5.3. *(Formal reconstruction of a polynomial from its cyclic resultants)*
Input: Positive integers d and N.
Output: Equations expressing a_i $(i = 0, \ldots, d)$ parameterized by $r_1, \ldots, r_N$.

(1) *Let $R = \mathbb{Q}[a_0, \ldots, a_d, r_1, \ldots, r_N]$ and let $\prec$ be any elimination term order with $\{a_i\} \prec \{r_j\}$.*

(2) *Compute the reduced Gröbner basis $\mathcal{G}$ for the ideal*

$$I = \langle r_1 - \mathit{Res}(f, x-1), \ldots, r_N - \mathit{Res}(f, x^N - 1)\rangle.$$

(3) *Output a triangular system of equations for a_i in terms of the r_i.*

□

A few remarks concerning Algorithm 2.5.3 are in order. If the a_i are indeterminates, a monic polynomial with coefficients a_i will be generic. Therefore, the first $N = 2^{d+1}$ cyclic resultants of f will determine it as a polynomial in x over an algebraic closure of $\mathbb{Q}(a_1, \ldots, a_d)$. It then follows from general theory (for instance, quantifier elimination for ACF, algebraically closed fields) that each a_i can be expressed as a rational function in the r_i ($i = 1, \ldots, N$). The same result holds for reciprocal polynomials with indeterminate coefficients. It is an interesting and difficult problem to determine these rational functions for a given d. As motivation for future work on this problem, we use Algorithm 2.5.3 to find these expressions explicitly for several small cases.

When $f = a_0x + a_1$ is linear, we need only two nonzero cyclic resultants to recover the coefficients a_0, a_1. An inversion is given by the formulae:

$$a_0 = \frac{r_2^2 - r_1}{2r_1},\ a_1 = \frac{-r_1^2 - r_2}{2r_1}.$$

In the quadratic case, a monic $f = x^2 + a_1x + a_2$ is also determined by two nonzero resultants:

$$a_1 = \frac{r_1^2 - r_2}{2r_1},\ a_2 = \frac{r_1^2 - 2r_1 + r_2}{2r_1}.$$

When $f = x^3 + a_1x^2 + a_2x + a_3$ has degree three, four resultants suffice, and inversion is given by:

$$\begin{aligned}
a_1 &= \frac{-12r_2r_1^3 - 12r_1r_2^2 + 3r_2^3 - r_2r_1^4 - 8r_2r_1r_3 + 6r_1^2r_4}{24r_2r_1^2}, \\
a_2 &= \frac{-r_1^2 - 2r_1 + r_2}{2r_1}, \\
a_3 &= \frac{-3r_2^3 + r_2r_1^4 + 8r_2r_1r_3 - 6r_1^2r_4}{24r_1^2r_2}.
\end{aligned}$$

Reconstruction for $d = 4$ is also possible using five resultants, however, the expressions are too cumbersome to list here.

As a final example, we describe the reconstruction of a degree 6 monic, reciprocal polynomial $f = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2x^2 + a_1x + 1$ from its first four cyclic resultants:

$$P = -540\, r_1{}^2 r_2\, r_4 - 13824\, r_1{}^3 r_2 + r_1{}^6 r_2 + 27\, r_2{}^3 r_1{}^2 + 9\, r_1{}^4 r_2{}^2 + 27\, r_2{}^4 - 432\, r_1{}^3 r_2{}^2 -$$

$$648\, r_1\, r_2{}^3 - 72\, r_1{}^5 r_2 - 448\, r_3\, r_1{}^3 r_2 + 192\, r_3\, r_1\, r_2{}^2 + 108\, r_1{}^4 r_4 + 1536\, r_1{}^2 r_2\, r_3 +$$

$$2592\, r_1{}^3 r_4 + 1728\, r_1{}^4 r_2 + 5184\, r_1{}^2 r_2{}^2,$$

$$Q = r_1{}^2 \left(-16\, r_3\, r_2 + 9\, r_4\, r_1\right),$$

$$R = -648\, r_1\, r_2{}^3 + 27\, r_2{}^3 r_1{}^2 + 27\, r_2{}^4 - 576\, r_3\, r_1\, r_2{}^2 + 2592\, r_1{}^3 r_4 + r_1{}^6 r_2 - 72\, r_1{}^5 r_2 +$$

$$9\, r_1{}^4 r_2{}^2 + 1728\, r_1{}^4 r_2 - 432\, r_1{}^3 r_2{}^2 + 320\, r_3\, r_1{}^3 r_2 - 324\, r_1{}^4 r_4 - 13824\, r_1{}^3 r_2 +$$

$$5184\, r_1{}^2 r_2{}^2 + 1536\, r_1{}^2 r_2\, r_3 - 108\, r_1{}^2 r_2\, r_4,$$

$$a_1 = \frac{1}{192}\, P/Q,\ a_2 = \frac{-4\, r_1 + r_1{}^2 + r_2}{4 r_1},\ a_3 = \frac{-1}{96} R/Q.$$

Chapter 3

Logarithmic Derivatives

3.1 Statement of Results

Using Gröbner basis techniques, we provide new constructive proofs of two theorems of Harris and Sibuya [21, 22] (see also, [60, 61] and [62, Problem 6.60]) that give degree bounds and allow for several generalizations. To prepare for the statement of the result, we begin with some preliminary definitions.

Definition 3.1.1. A *differential field* is a field K equipped with a map called a *derivation* $D : K \to K$ that is linear and satisfies the ordinary rule for derivatives; i.e.,

$$D(u+v) = D(u) + D(v), \quad D(uv) = uD(v) + vD(u).$$

When it is more convenient, we sometimes write u', u'', etc. for Du, D^2u, etc. Let F be a differential field extension of K (that is, a field extension that is also a differential field). A *linear homogeneous differential polynomial* $L(Y)$ over K of order m is a mapping from F to itself of form

$$L(Y) = a_m D^m(Y) + a_{m-1} D^{m-1}(Y) + \cdots + a_1 D(Y) + a_0 Y, \quad a_i \in K, a_m \neq 0.$$

We may now state the results of Harris and Sibuya.

Proposition 3.1.2. *Let $N_1, N_2 > 1$ be positive integers and let K be a differential field of characteristic 0. Let F be a (differential) field extension of K and suppose that $L_1(Y)$*

and $L_2(Y)$ are nonzero homogeneous linear differential polynomials (of orders N_1 and N_2 respectively) with coefficients in K. Further, suppose that one of the following holds:

(1) *$y \in F$ has $L_1(y) = L_2(1/y) = 0$, or*

(2) *$N_2 \leq q \in \mathbb{Z}_+$, and $y \in F$ has $L_1(y) = L_2(y^q) = 0$.*

Then, Dy/y is algebraic over K.

In this chapter, we prove the following more refined result.

Theorem 3.1.3. *Let $N_1, N_2 > 1$ be positive integers and let K be a differential field of characteristic 0. Let F be a (differential) field extension of K. Suppose that $L_1(Y)$ and $L_2(Y)$ are nonzero homogeneous linear differential polynomials (of orders N_1 and N_2 respectively) with coefficients in K. Further, suppose that one of the following holds:*

(1) *$y \in F$ has $L_1(y) = L_2(1/y) = 0$, or*

(2) *$N_2 \leq q \in \mathbb{Z}_+$, and $y \in F$ has $L_1(y) = L_2(y^q) = 0$.*

Then, $D^j y/y$ is algebraic over K for all $j \geq 1$. Moreover, the degree of the minimal polynomial for $D^j y/y$ ($j = 1, \ldots, N_1 - 1$) in (1) is at most $\binom{N_2+N_1-2}{N_1-1}$.

Remark 3.1.4. We note that with a more careful analysis, one may use our techniques to get similar results for fields of sufficiently large characteristic.

The first part (algebraicity) of this theorem is proved in Section 3.3, while in Section 3.4, we prove the specified degree bounds. Finally, in Section 3.5, we describe how our technique applies to certain nonlinear differential equations. Recall that a polynomial $f \in K[x]$ is called *separable* if all of its roots are distinct, and a field K is called *perfect* if every irreducible polynomial in $K[x]$ is separable. Examples of perfect fields include finite fields, fields of characteristic zero, and, of course, algebraically closed fields. It is interesting to note that there is a converse to Theorem 3.1.3 for this class of fields.

Proposition 3.1.5. *Let K be a perfect field. If y'/y is algebraic over K, then both y and $1/y$ satisfy linear differential equations over K.*

Proof. Suppose that K is perfect and $u = y'/y$ is algebraic over K. Let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in K[x]$ be the monic, irreducible polynomial for u over K. Since K is perfect, it follows from basic field theory that $\gcd(f, \frac{\partial f}{\partial x}) = 1$. In particular, $\frac{\partial f}{\partial x} \neq 0$. Consider now,

$$0 = f(u)' = u' \left(mu^{m-1} + \sum_{i=1}^{m-1} ia_i u^{i-1} \right) + \sum_{i=0}^{m-1} a_i' u^i.$$

Since $\frac{\partial f}{\partial x} = mx^{m-1} + \sum_{i=1}^{m-1} ia_i x^{i-1}$ is not the zero polynomial, it follows from the irreducibility of f that $mu^{m-1} + \sum_{i=1}^{m-1} ia_i u^{i-1} \neq 0$. Hence, $u' \in K(u)$ and the same holds for higher derivatives.

Next, notice that $(1/y)' = -y'/y^2 = -u/y$ and an easy induction gives us that $(1/y)^{(k)} = p_k(u, u', u'', \ldots)/y$, in which p_k is a polynomial (over K) in u and its derivatives (set $p_0 = 1$). By above, the polynomials $p_k(u, u', \ldots)$ lie in the field $K(u)$. This implies that they satisfy some (non-trivial) linear dependence relation,

$$\sum_{k=0}^{N} h_k p_k = 0,$$

in which $h_k \in K$. Therefore,

$$0 = \sum_{k=0}^{N} h_k p_k / y = \sum_{k=0}^{N} h_k (1/y)^{(k)}$$

as desired. Performing a similar examination on the derivatives of $y' = uy$ produces a linear differential equation for y over K, completing the proof. □

As an application of our main theorem, take F to be the field of complex meromorphic functions on $\mathbb{C}$ and $K = \mathbb{Q}$. Then, the only y such that both y and $1/y$ satisfy linear differential equations over K are the functions, $y = ce^{ux}$, in which u is an algebraic number of degree at most $\min\{N_1, N_2\}$ and $c \in \mathbb{C} \setminus \{0\}$. This simple example shows that it is possible to produce a minimum degree of $\min\{N_1, N_2\}$ for y'/y; however, it is still an open question of whether we can achieve a minimum degree close to the bound given in Theorem 3.1.3.

Theorem 3.1.3 can also be used to show that elements in a differential field F do not satisfy linear differential equations over a subfield K, as the following example demonstrates.

Example 3.1.6. ([62, Problem 6.59]). Let $K = \mathbb{C}(x)$ and $F = \mathbb{C}((x))$. Then, $\sec(x)$ does not satisfy a linear differential equation over K. To see this, suppose otherwise. Then, since $y = \cos(x)$ satisfies a linear differential equation, Theorem 3.1.3 would imply that $y'/y = \cos(x)'/\cos(x) = -\tan(x)$ is algebraic over $\mathbb{C}(x)$, a contradiction.

3.2 Algebraic Preliminaries

We begin by quickly reviewing some standard terminology (some of this material overlaps that of Chapter 1). Let K be a field. A *term order* (or *monomial ordering*) on $\mathbb{N}^n$ is a total order $\prec$ that is a well-ordering and is linear:

$$\boldsymbol{a} \prec \boldsymbol{b} \Rightarrow \boldsymbol{a} + \boldsymbol{c} \prec \boldsymbol{b} + \boldsymbol{c},$$

for $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{N}^n$. This ordering of $\mathbb{N}^n$ gives a corresponding ordering on the monomials of $R = K[x_1, \ldots, x_n]$.

Given a polynomial $f \in R$, the *leading monomial* of f (simply written $\mathrm{lm}_\prec(f)$) is the largest monomial occurring in f with respect to $\prec$. The *initial ideal* of an ideal $I \subseteq R$ is defined to be

$$\mathrm{in}_\prec(I) := \langle \mathrm{lm}_\prec(f) : f \in I \rangle.$$

A Gröbner Basis for an ideal $I \subseteq R$ is a finite subset $G = \{g_1, \ldots, g_m\}$ of I such that:

$$\langle \mathrm{lm}_\prec(g_1), \ldots, \mathrm{lm}_\prec(g_m) \rangle = \mathrm{in}_\prec(I).$$

There is a canonical Gröbner basis for an ideal with respect to a fixed term order called the *reduced Gröbner Basis* of I, and it can be computed algorithmically [9].

Let I be an ideal of a polynomial ring $R = K[x_1, \ldots, x_n]$ over the field K and let $V(I)$ be the corresponding variety (we work over $\overline{K}^n$ to simplify exposition):

$$V(I) := \{(a_1, \ldots, a_n) \in \overline{K}^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}.$$

We call $V(I)$ *zero-dimensional* if it consists of a finite number of points. The following characterization of zero-dimensional varieties can be found in [9, p. 230].

Theorem 3.2.1. *Let $V(I)$ be a variety in $\overline{K}^n$ and fix a term ordering $\prec$ for $K[x_1, \ldots, x_n]$. Then the following statements are equivalent:*

(1) *V is a finite set.*

(2) *For each i, $1 \leq i \leq n$, there is some $m_i \geq 0$ such that $x_i^{m_i} \in \mathrm{in}_{\prec}(I)$.*

(3) *Let G be a Gröbner basis for I. Then for each i, $1 \leq i \leq n$, there is some $m_i \geq 0$ such that $x_i^{m_i} = \mathrm{lm}_{\prec}(g)$ for some $g \in G$.*

The following fact is well-known, but we include a proof for completeness.

Proposition 3.2.2. *If $V(I)$ is a zero-dimensional variety, then the coordinates of every point of $V(I)$ are algebraic over K.*

Proof. Let $(a_1, \dots, a_n)$ be a point in $V(I)$. We prove that a_1 is algebraic over K (the other coordinates are treated similarly). Fix a lexicographic term order $\prec$ on $K[x_1, \dots, x_n]$ such that $x_1 < x_2 < \cdots < x_n$, and let G be a reduced Gröbner basis for I with respect to this term order. Then, it follows from Theorem 3.2.1 that $x_1^m = \mathrm{lm}_{\prec}(g)$ for some $0 \neq g \in G$ and $m \geq 0$. Since G is computed using operations in the field K (the ideal I is defined over K), it follows that $g \in K[x_1, \dots, x_n]$. Moreover, our term order insures that $g(x_1, \dots, x_n) = g(x_1)$ is a univariate polynomial in the variable x_1. Since $g(a_1, \dots, a_n) \in I$, we must have that $g(a_1) = 0$. It follows that a_1 is algebraic over K, completing the proof. □

Proposition 3.2.2 is an important tool in the proof of our main theorem. We now describe another ingredient in the solution of our problem, although its generality should be useful in many other contexts. Give R a grading by assigning to each x_i, a number $w(x_i) = w_i \in \mathbb{N}$, so that

$$w\left(\prod_{i=1}^{n} x_i^{v_i}\right) = \sum_{i=1}^{n} v_i w_i.$$

Then, we have the following extension of a result of Sperber [61]. A proof of a generalization can be found in [57, Lemma 2.2.2]; however, again for completeness we include an argument for our special case.

Lemma 3.2.3. *Let I be the ideal of $R = K[x_1, \dots, x_n]$ generated by a collection of polynomials, $\{f_\beta\}_{\beta \in \Gamma} \subseteq R$. Let $\tilde{f}_\beta$ be the leading homogeneous form of f_β with respect to the above grading, and let J be the ideal generated by $\{\tilde{f}_\beta\}_{\beta \in \Gamma}$. Then, if $V(J)$ is zero-dimensional, so is $V(I)$.*

Proof. Fix a grading $w = (w_1, \dots, w_n) \in \mathbb{N}^n$ and let $\prec$ be a monomial ordering on R. Define a new monomial ordering $\prec_w$ as follows [64, p. 4]: for $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}^n$ we set

$$\boldsymbol{a} \prec_w \boldsymbol{b} \;:\Leftrightarrow\; w \cdot \boldsymbol{a} < w \cdot \boldsymbol{b} \;\text{ or }\; (w \cdot \boldsymbol{a} = w \cdot \boldsymbol{b} \text{ and } \boldsymbol{a} \prec \boldsymbol{b}).$$

Since $V(J)$ is zero-dimensional, as before, Theorem 3.2.1 tells us that for each $i \in \{1, \dots, n\}$ there exist integers $m_i \geq 0$ such that $x_i^{m_i} \in \mathrm{in}_{\prec_w}(J)$. From Dickson's Lemma [9, p. 69], it follows that $\mathrm{in}_{\prec_w}(J)$ can be finitely generated as

$$\langle \mathrm{lm}_{\prec_w}(\tilde{f}_{\beta_1}), \dots, \mathrm{lm}_{\prec_w}(\tilde{f}_{\beta_q}) \rangle$$

for some positive integer q and $\beta_j \in \Gamma$. Thus, we may write

$$x_i^{m_i} = \sum_{j=1}^{q} g_{i,j} \cdot \mathrm{lm}_{\prec_w}(\tilde{f}_{\beta_j})$$

for polynomials $g_{i,j}$. Set $\tilde{g}_{i,j}$ to be the terms in $g_{i,j}$ of weight $m_i w_i - w(\tilde{f}_{\beta_j})$, and also let $\hat{g}_{i,j} = g_{i,j} - \tilde{g}_{i,j}$. Notice that the equation above then implies

$$x_i^{m_i} = \sum_{j=1}^{q} \hat{g}_{i,j} \cdot \mathrm{lm}_{\prec_w}(\tilde{f}_{\beta_j}) + \sum_{j=1}^{q} \tilde{g}_{i,j} \cdot \mathrm{lm}_{\prec_w}(\tilde{f}_{\beta_j}).$$

The first sum on the right above has terms of weight that are different from $m_i w_i$, while the second has terms of only this weight. Since the left-hand-side of the equation has weight $m_i w_i$, we must have that

$$\sum_{j=1}^{q} \hat{g}_{i,j} \cdot \mathrm{lm}_{\prec_w}(\tilde{f}_{\beta_j}) = 0.$$

Finally, define

$$h_i = \sum_{j=1}^{q} \tilde{g}_{i,j} f_{\beta_j} \;\in\; I.$$

It is clear that the leading term (with respect to $\prec_w$) of h_i is $x_i^{m_i}$. But then again using Theorem 3.2.1, we have that $V(I)$ is a finite set, completing the proof. □

In other words, this lemma says that in many instances information about an ideal I can be uncovered by passing to a simpler ideal involving leading forms. This fundamental concept is an important component in Gröbner deformation theory.

3.3 Proofs of The Main Theorems

Before embarking on proofs of the theorems stated in Section 3.1, we present a simple example to illustrate our technique. Let $y_1, y_2, \dots$ be variables. We will view $y_j = D^j y/y$ as solutions to a system of polynomial equations over $K[\{y_j\}_{j=1}^{\infty}]$. For example, consider the system $(N_1 = 3, N_2 = 2)$:

$$y''' + a_2 y'' + a_1 y' + a_0 y = 0,$$
$$(1/y)'' + b_1 (1/y)' + b_0 (1/y) = 0$$

in which $a_2, a_1, a_0, b_1, b_0 \in K$. Dividing the first equation by y and expanding the second one gives us the more suggestive equations:

$$y_3 + a_2 y_2 + a_1 y_1 + a_0 = 0,$$
$$(2y_1^2 - y_2) - b_1 y_1 + b_0 = 0.$$

Also, differentiating the original equation for $1/y$ and expanding, we have that

$$-6y_1^3 + 6y_1 y_2 - y_3 + b_1(2y_1^2 - y_2) - y_1(b_1' + b_0) + b_0' = 0.$$

Thus, we may view $(y'/y, y''/y, y'''/y) = (y_1, y_2, y_3)$ as a solution to a system of three polynomial equations in three unknowns.

Let $w(y_i) = i$ define a grading of $K[y_1, y_2, y_3]$, and notice that the system of leading forms, $\{y_3 = 0, 2y_1^2 - y_2 = 0, -6y_1^3 + 6y_1 y_2 - y_3 = 0\}$, has only the trivial solution $(y_1, y_2, y_3) = (0, 0, 0)$. In light of Lemma 3.2.3, it follows that the equations above define a zero-dimensional variety. Therefore, appealing to Proposition 3.2.2, we have established the algebraicity component of Theorem 3.1.3 (1) for this example $(N_1 = 3, N_2 = 2)$.

In general, we will construct a system of $N_1 - 1$ equations in $N_1 - 1$ unknowns satisfied by the y_i. These equations will define a zero-dimensional variety, and thus, standard elimination techniques (see, for instance, [8]) give us a direct method of computing, for each i, a nonzero polynomial (over K) satisfied by y_i.

Let us first examine what happens when we compute $f_n = D^n(1/y)$. Notice that

$$\begin{aligned} f_0 &= 1/y \\ f_1 &= -y^{-2}Dy = -y_1/y \\ f_2 &= 2y^{-3}(Dy)^2 - y^{-2}D^2y = 2y_1^2/y - y_2/y \\ f_3 &= -6y_1^3/y + 6y_1y_2/y - y_3/y. \end{aligned}$$

In general, these functions f_n can be expressed in the form $f_n = (1/y)p_n(y_1, \ldots, y_n)$ for polynomials $p_n \in \mathbb{Z}[y_1, \ldots, y_n]$. Moreover, with respect to the grading $w(y_i) = i$, these p_n are homogeneous of degree n. These facts are easily deduced from the following lemma.

Lemma 3.3.1. *Let $m \in \mathbb{Z}_+$. Then,*

$$\frac{p_m}{m!} = -\sum_{j=1}^{m-1} \frac{p_{m-j}}{(m-j)!}\frac{y_j}{j!} - \frac{y_m}{m!}.$$

Proof. Consider the following well-known identity (Leibniz' rule),

$$\sum_{j=0}^{m} \binom{m}{j} \left(D^j h\right) \left(D^{m-j} g\right) = D^m(hg).$$

Setting $h = y$ and $g = 1/y$, it follows that

$$\sum_{j=0}^{m} \frac{D^j y}{j!} \frac{D^{m-j}(1/y)}{(m-j)!} = 0.$$

Multiplying the numerator and denominator by y and rewriting this expression gives us

$$\frac{p_m}{m!} = -\frac{p_{m-1}}{(m-1)!}\frac{y_1}{1!} - \frac{p_{m-2}}{(m-2)!}\frac{y_2}{2!} - \cdots - \frac{p_1}{1!}\frac{y_{m-1}}{(m-1)!} - \frac{y_m}{m!}.$$

□

We are now ready to prove Theorem 3.1.3 (1).

Proof of Theorem 3.1.3 (1). With N_1, N_2 as in Theorem 3.1.3, we suppose $N_1 = n$, $N_2 = m$. Dividing through by y in the first differential equation for y gives us

$$y_n = -a_{n-1}y_{n-1} - \cdots - a_1y_1 - a_0, \qquad a_i \in K \tag{3.3.1}$$

while multiplying the second one for $1/y$ by y produces the equation

$$p_m + b_{m-1}p_{m-1} + \cdots + b_0 = 0, \qquad b_i \in K.$$

Differentiating k times the original linear differential equation for y, we will arrive at linear equations $y_{n+k} = L_k(y_1, \ldots, y_{n-1})$ in terms (over K) of $y_1, \ldots, y_{n-1}$ like (3.3.1) above (by repeated substitution of the previous linear equations). If we also differentiate the equation for $1/y$ k times, we will produce another equation for the variables y_i. More formally, we have that

$$D^{m+k}(1/y) + D^k(b_{m-1}D^{m-1}(1/y)) + \cdots + D^k(b_0/y) = 0$$

produces the equation (by Leibniz' rule)

$$D^{m+k}(1/y) + \sum_{i=0}^{m-1}\sum_{j=0}^{k}\binom{k}{j}\left(D^j b_i\right)\left(D^{k-j+i}\left(1/y\right)\right) = 0.$$

So finally (after multiplying through by y), it follows that

$$P_{m+k} := p_{m+k} + \sum_{i=0}^{m-1}\sum_{j=0}^{k}\binom{k}{j}\left(D^j b_i\right)p_{k-j+i} = 0. \tag{3.3.2}$$

It is clear that the leading homogeneous forms of the P_{m+k} (with respect to the grading above) are p_{m+k}. Consider now the ring homomorphism $\phi : K[\{y_i\}_{i=1}^{\infty}] \to K[y_1, \ldots, y_{n-1}]$ defined by sending $y_j \mapsto 0$ for $j \geq n$ and $y_j \mapsto y_j$ for $j < n$. Let $\tilde{P}_{m+k}$ denote the polynomials produced by substituting the linear forms L_i for the variables y_{n+i} $(i = 0, 1, \ldots)$ into the polynomials, P_{m+k}. The leading homogeneous forms of the $\tilde{P}_{m+k}$ will just be $\tilde{p}_{m+k} := \phi(p_{m+k})$ because we are substituting linear polynomials with strictly smaller degree (corresponding to the grading). In light of Lemma 3.2.3, we verify that the $n-1$ equations (in the $n-1$ variables),

$$\tilde{p}_m = 0,\ \tilde{p}_{m+1} = 0,\ \ldots,\ \tilde{p}_{m+n-2} = 0, \tag{3.3.3}$$

are only satisfied by the point $(0, \ldots, 0)$ to prove the claim.

Suppose that $(y_1, \ldots, y_{n-1}) \neq (0, \ldots, 0)$ is a zero of the system in (3.3.3); we will derive a contradiction. Let $r \in \{1, \ldots, n-1\}$ be the largest integer such that $y_r \neq 0$, and choose $t \in \{0, \ldots, m-1\}$ maximal such that $\tilde{p}_{m-t} = 0$, $\tilde{p}_{m-t+1} = 0$, ..., $\tilde{p}_m = 0$. If $t = m-1$, then $\tilde{p}_1 = -y_1 = 0$, and so the recurrence in Lemma 3.3.1 and (3.3.3) give us that $y_i = 0$ for $i \in \{1, \ldots, n-1\}$, a contradiction. Thus, $t \leq m-2$. Using Lemma 3.3.1 with ϕ (and the maximality of r), we have the following identity:

$$\frac{\tilde{p}_{m-t+r-1}}{(m-t+r-1)!} = -\frac{\tilde{p}_{m-t+r-2}}{(m-t+r-2)!}\frac{y_1}{1!} - \cdots - \frac{\tilde{p}_{m-t}}{(m-t)!}\frac{y_{r-1}}{(r-1)!} - \frac{\tilde{p}_{m-t-1}}{(m-t-1)!}\frac{y_r}{r!}.$$

From (3.3.3) and the property of t above, it follows that $\frac{\tilde{p}_{m-t-1}}{(m-t-1)!}\frac{y_r}{r!} = 0$. Thus, $y_r = 0$ or $\tilde{p}_{m-(t+1)} = 0$; the first possibility contradicts $y_r \neq 0$, while the second contradicts maximality of t.

This proves that the equations (3.3.3) define a zero-dimensional variety, from which the algebraicity of $D^j y/y$ $(j = 1, \ldots, n-1)$ follows using Proposition 3.2.2. With repeated differentiation of (3.3.1), we also see that $D^j y/y$ is algebraic for all $j \geq n$. The proof of the degree bounds will be postponed until Section 3.4. □

The proof for Theorem 3.1.3 (2) is similar to the one above, however, the recurrences as in Lemma 3.3.1 are somewhat more complicated. Let $n \in \mathbb{N}$, $q \in \mathbb{Z}_+$ and examine $f_{n,q} = D^n(y^q)$. It turns out that $f_{n,q} = y^q p_{n,q}(y_1, \ldots, y_n)$ in which $p_{n,q} \in \mathbb{Z}[y_1, \ldots, y_n]$ is homogeneous of degree n (with respect to the grading $w(y_i) = i$). This follows in a similar manner as before from the following lemma.

Lemma 3.3.2. *Let $p_{n,1} = y_n$ for $n \in \mathbb{N}$ $(y_0 = 1)$. Then, for all $m \in \mathbb{N}, q > 1$,*

$$p_{m,q} = y_m + \sum_{j=0}^{m-1} \binom{m}{j} y_j p_{m-j,q-1}.$$

Proof. Use Leibniz' rule as in Lemma 3.3.1 with $h = y^{q-1}$ and $g = y$. □

The next lemma will be used in the proof of Theorem 3.1.3 (2), and it follows from a straightforward induction on a (using Lemma 3.3.2).

Lemma 3.3.3. *Let ϕ be as in the proof of Theorem 3.1.3 (1) and $n \geq 2$. Then, for all $a \in \mathbb{Z}_+$ and $b \in \mathbb{N}$, we have $\phi\left(p_{(a+1)(n-1)+b,a}\right) = 0$.*

We now prove Theorem 3.1.3 (2).

Proof of Theorem 3.1.3 (2). With N_1, N_2 as in Theorem 3.1.3, we suppose $N_1 = n$, $N_2 = m \leq q$. As before, the first differential equation for y gives us

$$y_n = -a_{n-1}y_{n-1} - \cdots - a_1y_1 - a_0 \quad a_i \in K \tag{3.3.4}$$

while the second one for y^q (after dividing through by y^q) produces the equation

$$p_{m,q} + b_{m-1}p_{m-1,q} + \cdots + b_0 = 0 \quad b_i \in K.$$

Differentiating k times the original linear differential equation for y, produces linear equations $y_{n+k} = L_k(y_1, \ldots, y_{n-1})$ in terms (over K) of $y_1, \ldots, y_{n-1}$ like (3.3.4) above. If we also differentiate the equation for y^q, k times, we will arrive at another equation for the variables y_i:

$$P_{m+k,q} := p_{m+k,q} + \sum_{i=0}^{m-1}\sum_{j=0}^{k}\binom{k}{j}\left(D^jb_i\right)p_{k-j+i,q} = 0.$$

It is clear that the leading homogeneous forms of the $P_{m+k,q}$ (with respect to the grading above) are $p_{m+k,q}$. Let ϕ be as in the proof of Theorem 3.1.3 (1), and let $\tilde{P}_{m+k,q}$ denote the polynomials produced by substituting the linear forms L_i for the variables y_{n+i} $(i = 0, 1, \ldots)$ into the polynomials, $P_{m+k,q}$. If $\tilde{p}_{m+k,q} := \phi(p_{m+k,q}) \neq 0$, then the leading homogeneous form of $\tilde{P}_{m+k,q}$ is $\tilde{p}_{m+k,q}$ because we are substituting linear polynomials with strictly smaller degree (corresponding to the grading).

Consider the following system of equations (recall that $q \geq m$ and $n \geq 2$),

$$\tilde{p}_{m,q} = 0,\ \tilde{p}_{m+1,q} = 0,\ \ldots,\ \tilde{p}_{(q+1)(n-1)-1,q} = 0. \tag{3.3.5}$$

We claim that $(0, \ldots, 0)$ is the only solution to (3.3.5). Suppose, on the contrary, that $(y_1, \ldots, y_{n-1}) \neq (0, \ldots, 0)$ is a solution to (3.3.5), and let $r \in \{1, \ldots, n-1\}$ be the largest integer such that $y_r \neq 0$. Also, choose $t \in \{1, \ldots, q\}$ minimial such that

$$\tilde{p}_{tr,t} = 0,\ \tilde{p}_{tr+1,t} = 0,\ \ldots,\ \tilde{p}_{(t+1)r-1,t} = 0. \tag{3.3.6}$$

Clearly $t \neq 1$, as then $\tilde{p}_{r,1} = y_r = 0$, a contradiction. Applying Lemma 3.3.2 with ϕ (and maximality of r), examine the equation,

$$\tilde{p}_{(t+1)r-1,t} = \tilde{p}_{(t+1)r-1,t-1} + \cdots + \binom{(t+1)r-1}{r}y_r\tilde{p}_{tr-1,t-1}. \tag{3.3.7}$$

Using Lemma 3.3.3 (with $a = t - 1$) and the maximality of r, we have $\tilde{p}_{tr+b,t-1} = 0$ for all $b \in \mathbb{N}$. Consequently, (3.3.7) and (3.3.6) imply that $\tilde{p}_{tr-1,t-1} = 0$. Repeating this examination with $\tilde{p}_{(t+1)r-2,t}, \tilde{p}_{(t+1)r-3,t}, \ldots, \tilde{p}_{tr,t}$ (in that order) in place of $\tilde{p}_{(t+1)r-1,t}$ on the left-hand side of (3.3.7), it follows that $\tilde{p}_{tr-i,t-1} = 0$ for $i = 1, \ldots, r$. This, of course, contradicts the minimality of t and proves the claim.

It now follows from Lemma 3.2.3 that the variety determined by

$$\left\{\tilde{P}_{m,q} = 0, \ldots, \tilde{P}_{(q+1)(n-1)-1,q} = 0\right\}$$

is zero-dimensional. An application of Proposition 3.2.2 completes the proof. □

3.4 The Degree Bounds

In this section, we outline how to obtain the degree bounds in Theorem 3.1.3. We begin by stating a useful theorem that bounds the cardinality of a variety by the product of the degrees of the polynomials defining it (see [59] for more details).

Theorem 3.4.1 (Bezout's theorem). *Let K be an arbitrary field, and let $f_1, \ldots, f_t \in K[y_1, \ldots, y_t]$. If $V(f_1, \ldots, f_t)$ is finite, then*

$$|V(f_1, \ldots, f_t)| \leq \prod_{i=1}^{t} \deg(f_i).$$

We next make the following straightforward observation.

Lemma 3.4.2. *Let K be a perfect field, and let $I \subset K[y_1, \ldots, y_t]$ be such that $V(I)$ is finite. Then, the degree of the minimal polynomial for each component of an element in $V(I)$ is bounded by the number of elements of $V(I)$.*

Proof. Suppose that $g(x) \in K[x]$ is the irreducible polynomial for $y \in \overline{K}$, a component of $(y_1, \ldots, y, \ldots, y_t) \in V(I)$. Since K is perfect, this polynomial has distinct roots. Thus, there are $\deg(g)$ distinct embeddings $\sigma : K(y) \to \overline{K}$ that are the identity on K. Moreover, each of these homomorphisms extends to an embedding $\tilde{\sigma} : \overline{K} \to \overline{K}$ [39, p. 233]. In particular, the $\deg(g)$ points, $(\tilde{\sigma}y_1, \ldots, \tilde{\sigma}y, \ldots, \tilde{\sigma}y_t)$, are all distinct elements of $V(I)$. Thus, we must have

$$\deg(g) \leq |V(I)|.$$

This completes the proof. □

Theorem 3.4.3. *Assuming the hypothesis as in Theorem 3.1.3, the degree of the polynomial for $D^j y/y$ $(j = 1, \ldots, N_1 - 1)$ over K in (1) is at most $\binom{N_2+N_1-2}{N_1-1}$.*

Proof. Let $N_1 = n$, $N_2 = m$ and set $\tilde{P}_{m+k} \in K[y_1, \ldots, y_{n-1}]$ $(k = 0, \ldots, n-2)$ to be the polynomials in (3.3.2) after substitution of the linear forms, $y_{n+i} = L_i(y_1, \ldots, y_{n-1})$. Corresponding to the grading $w(y_j) = j$, the weight of each monomial in $\tilde{P}_{m+k}$ is less than or equal to $m + k$. Let $\tilde{S}$ be the set of all solutions with coordinates in $\overline{K}$ to the system $\{\tilde{P}_{m+k} = 0\}_{k=0}^{n-2}$. Our first goal is to bound the cardinality of $\tilde{S}$ by $\binom{m+n-2}{n-1}$.

Suppose that $\{y_{i,1}, \ldots, y_{i,s}\}$ is the list of all s distinct i-th coordinates of members of $\tilde{S}$. Since K is infinite, there exists $k_i \in K$ such that $y_{i,j} \neq k_i$ for $j = 1, \ldots, s$. Now, let $x_1, \ldots, x_{n-1}$ be variables and consider the new polynomials $F_{m+k} \in K[x_1, \ldots, x_{n-1}]$ produced by the substitution $y_i = x_i^i + k_i$ in the $\tilde{P}_{m+k}$. As the $n-1$ equations $\tilde{P}_{m+k} = 0$ define a zero-dimensional variety, so do the $n-1$ equations $F_{m+k} = 0$.

Let S denote the set of all solutions with coordinates in $\overline{K}$ to the system $\{F_{m+k} = 0\}_{k=0}^{n-2}$. Since the total degree of each F_{m+k} is just $m+k$, we have by Bezout's theorem (Theorem 3.4.1),

$$|S| \leq \frac{(m+n-2)!}{(m-1)!} = (n-1)!\binom{m+n-2}{n-1}.$$

Consider the (set-theoretic) map $\psi : S \to \tilde{S}$ given by

$$(x_1, \ldots, x_{n-1}) \mapsto (x_1 + k_1, \ldots, x_{n-1}^{n-1} + k_{n-1}).$$

It is easy to see that

$$\sum_{s \in \tilde{S}} \left|\psi^{-1}(s)\right| = |S|. \tag{3.4.1}$$

Let $(y_1, \ldots, y_{n-1}) \in \tilde{S}$. By our choice of k_i, the polynomial $h_i(x_i) = x_i^i + k_i - y_i$ has precisely i distinct zeroes. These i roots are distinct since characteristic zero implies that $\gcd(h_i, \frac{\partial h_i}{\partial x}) = 1$. Hence, $\left|\psi^{-1}(s)\right| \geq (n-1)!$ for all $s \in \tilde{S}$, and so from

$$|\tilde{S}|(n-1)! \leq |S| \leq \binom{m+n-2}{n-1}(n-1)!,$$

we arrive at the desired bound on $|\tilde{S}|$.

An application of Lemma 3.4.2 now completes the proof. □

We should also note that the proof above generalizes to bound the number of distinct solutions to certain systems of equations. Specifically, we have the following interesting fact.

Theorem 3.4.4. *Let $w(y_j) = j$ be the grading as above and let K be a field of characteristic zero. Let $m \in \mathbb{Z}_+$ and suppose that $\{F_{m+k}(y_1, \ldots, y_{n-1}) = 0\}_{k=0}^{n-2}$ is a zero-dimensional system of polynomial equations over K such that each monomial in F_{m+k} has weight less than or equal to $m + k$. Then, this system will have at most $\binom{m+n-2}{n-1}$ distinct solutions with coordinates in $\overline{K}$.*

In principle, the number of solutions for a generic system with conditions as in Theorem 3.4.4 can be found by a mixed volume computation and Bernstein's Theorem (see [8], for instance). This approach, however, seems difficult to implement.

3.5 Applications to Nonlinear Differential Equations

In the proof of Theorem 3.1.3, it is clear that the important attributes of the recursions as in (3.3.1) are that they reduce the degree and are polynomial in nature. In particular, it was not necessary that they were linear. For example, the system,

$$yy''' + a(y')^2 + by^2 = 0,$$
$$(1/y)'' + c(1/y)' + d(1/y) = 0$$

gives us the recurrence $y_3 + ay_1^2 + b = 0$ (divide the first equation by y^2), which has y_3 expressible as a polynomial in y_1, y_2 with strictly smaller weight. Repeated differentiation of this equation, preserves this property. In general, let $h \in K[z_1, \ldots, z_n]$ be a homogeneous polynomial (with respect to total degree) such that each monomial $z^\alpha = z_1^{\alpha_1} \cdots z_n^{\alpha_n}$ has

$$\sum_{i=1}^{n} (i-1)\alpha_i < n.$$

If the hypothesis of Theorem 3.1.3 are weakened to allow y to satisfy an equation of the form, $D^n y = h(y, Dy, \ldots, D^{(n-1)}y)$, then the proof applies without change. A generalization along these lines was also considered by Sperber in [61], however, the techniques developed here give us degree bounds just as in Theorem 3.1.3.

Chapter 4

Symmetric Word Equations in Positive Definite Letters

4.1 Introduction

In this chapter, we consider a natural matrix generalization to the elementary scalar equation

$$bx^s = p,$$

in which $b > 0$, $p \geq 0$, $s \in \mathbb{Z}_+$ and x is a nonnegative real indeterminate. One difficulty with an extension is dealing with matrix noncommutativity, while another is determining what should be meant by the words "real" and "nonnegative." Fortunately for us, the latter concerns have already long been addressed: the natural matrix interpretation of the reals are the Hermitian matrices, while nonnegative (resp. positive) numbers correspond to those complex Hermitian matrices with all nonnegative (resp. positive) eigenvalues, the so-called *positive semidefinite* (resp. *positive definite*) matrices. The issue of noncommutativity, however, is of a more subtle nature, and we first introduce some notation before addressing it.

Fix a positive integer k, and let $W = W(X, B_1, \ldots, B_k)$ be a word in the letters X and $B_1, \ldots, B_k$. The *reversal* of W is the word written in reverse order, and it is denoted by W^*. A word is *symmetric* if it is identical to its reversal (in other contexts, the name "palindromic" is also used). As we shall soon see (see Sections 4.2 and 4.3), formulating our generalization requires restriction to a special class of words. For the purposes of this work, an *interlaced* word $W = W(X, B_1, \ldots, B_k)$ in the *interlacing* letter X is a juxtaposition of powers of letters that alternate in X. More precisely, an interlaced word is an expression of the form,

$$W = B_{i_1}^{q_1} \prod_{j=1}^{m} X^{p_j} B_{i_{j+1}}^{q_{j+1}}, \tag{4.1.1}$$

in which the exponents $p_j > 0$, $q_j \geq 0$ are nonnegative integers and $\{i_1, \ldots, i_{m+1}\} \subseteq \{1, \ldots, k\}$. (Here, of course, we consider the zeroth power of a letter to be the empty word, the identity element of the monoid). For example, the word $B_1 X B_3^7 X^2 B_2^3 X^5$ is interlaced, whereas the word $X B_1 B_2 X B_2 B_1 X$ is not. The integer $s = p_1 + \cdots + p_m$ is called the *degree* of the interlaced word W.

The interlacing letter X is distinguished, and is to be viewed as an indeterminate $n \times n$ positive semidefinite matrix, while the letters $B_1, \ldots, B_k$ correspond to fixed $n \times n$ positive definite matrices. For convenience, the letters X and B_i will also represent the substituted matrices (the context will make the distinction clear). When $k = 1$, the set of interlaced words is simply the set of all words in two letters containing at least one X. For notational simplicity, when k is understood, we write $W(X, B_i)$ in place of $W(X, B_1, \ldots, B_k)$.

Returning to our motivating example, notice that there is a unique nonnegative solution to the equation $bx^s = p$ for every pair of positive b and nonnegative p; we would like to generalize this observation. Our introductory remarks prepare us to make the following definition.

Definition 4.1.1. A *symmetric word equation* is an equation, $S(X, B_i) = P$, in which $S(X, B_i)$ is an interlaced symmetric word. If the B_i are positive definite and P is positive semidefinite, then any positive semidefinite matrix X for which the equation holds is called a *solution* to the symmetric word equation.

A symmetric word equation will be called *solvable* if there exists a solution for every positive definite $n \times n$ matrices B_i and $n \times n$ positive semidefinite P. Moreover, if each such B_i and P give rise to a unique solution, the equation will be called *uniquely solvable.*

Theorem 4.1.2 (Hillar and Johnson). *Every symmetric word equation is solvable. Moreover, if the parameters P and B_i are real, then there is a real solution.*

Theorem 4.1.2 first appeared in [29, Theorem 7.1]. Its proof was accomplished using fixed point methods. The authors left open the problem of uniqueness.

Conjecture 4.1.3. *Every symmetric word equation is uniquely solvable.*

Uniquely solvable equations are ubiquitous (see Section 4.5, where we produce a large family of them). Recently, Lawson and Lim [40] have verified Conjecture 4.1.3 in the case that the degree of $S(X, B_i)$ is not greater than five. Their approach utilizes the Riemannian metric on the set of positive definite matrices and Banach's fixed point theorem.

In this chapter, we resolve Conjecture 4.1.3 negatively in the case $n \geq 3$.

Theorem 4.1.4. *There are symmetric word equations of degree* 6 *which have multiple real* 3×3 *positive definite solutions.*

Conjecture 4.1.3 remains open in the case of 2×2 matrices.

Theorem 4.1.4 shows that the result of Lawson and Lim is optimal. Although uniqueness fails in general, our approach allows us to verify that these equations are still well-behaved in the following sense.

Theorem 4.1.5. *Fix an interlaced symmetric word S and real positive definite matrices $B_1, \ldots, B_k$ and P. There is a bounded open subset U of real positive definite matrices such that all real solutions X of the equation $f(X) = S(X, B_i) = P$ lie in U. Moreover, identifying the real symmetric matrices with $\mathbb{R}^m$ we have that*

$$\deg(f, U, P) = 1.$$

Here, $\deg(f, U, P)$ is the Brouwer degree of f at P with respect to U; in a vague sense, it gives a topological measure of the number of solutions inside U to the equation $f(X) = P$. See Example 4.2.5 for a (non-interlaced) symmetric word equation with an unbounded set of solutions. Theorem 4.1.5 implies a special case of Theorem 4.1.2, giving a second proof of existence in the real case.

Corollary 4.1.6. *Every symmetric word equation in real positive definite letters has a real positive semidefinite solution.*

Proof. The result follows from Theorem 4.1.5, Theorem 4.6.2, and Lemma 4.7.1. □

Corollary 4.1.7. *For almost every real positive definite matrix P, the symmetric word equation*

$$S(X, B_i) = P$$

has an odd (and thus finite) number of real solutions X.

Proof. By Theorems 4.1.5 and 4.7.3, at any regular value P of the map $X \mapsto S(X, B_i)$, the equation $S(X, B_i) = P$ has an odd number of solutions X. By Sard's theorem, the set of regular values is a set of full measure, completing the proof. □

The proof of Theorem 4.1.5 is the content of Sections 4.8, 4.9 and 4.10. The arguments in the proof often employ the reductions found in Section 4.6. Some consequences of Theorem 4.1.5 are explored in Section 4.11, including a proof of Theorem 4.1.4. In Sections 4.2 and 4.3 we explain why we restrict our attention to interlaced symmetric words, and Sections 4.4 and 4.5 are devoted to applications and a special class of uniquely solvable words, respectively. In Section 4.7 we review the theory of Brouwer degree.

4.2 A Collection of Examples

The simplest instance of a symmetric word equation arises in the following example ([34, p. 413] and [34, p. 433]); it is the most straightforward generalization of the scalar case.

Example 4.2.1. *Let P be any positive semidefinite matrix and let $S(X)$ be the word X^m, for a positive integer m. Then, there is a unique positive semidefinite solution to the equation $S(X) = P$. In fact, writing $P = UDU^*$ for a unitary matrix U and a nonnegative diagonal matrix D, we have $X = UD^{1/m}U^*$.* □

As another example, we examine a special case of the *algebraic Riccati equation*, which is encountered frequently in control theory [51].

Example 4.2.2. *The equation,* $XBX = P$*, has a unique positive semidefinite solution given positive definite* B *and positive semidefinite* P*. Moreover, it is given by*

$$X = B^{-1/2}(B^{1/2}PB^{1/2})^{1/2}B^{-1/2}.$$

This fact can be deduced from the proof of Proposition 4.5.2, in which a large class of word equations are shown to be uniquely solvable. When P *is invertible, this solution can also be expressed as*

$$X = P^{1/2}(P^{-1/2}B^{-1}P^{-1/2})^{1/2}P^{1/2},$$

even though this expression appears quite different. □

As promised, we now explain why it makes sense to restrict our attention to interlaced symmetric words. A first obstacle in generalizing the scalar case is that most words do not evaluate to positive semidefinite matrices upon substitution. One simple example is the word XB, which does not even have to be Hermitian when X and B are positive definite. Similarly, the unique matrix solution X of the equation $XB = P$ is not in general positive semidefinite. It turns out that the right class of words to consider are the symmetric ones, and this is evidenced by the following discussion.

Recall that two $n \times n$ matrices X and Y are said to be *congruent* if there is an invertible $n \times n$ matrix Z such that $Y = Z^*XZ$ (here, C^* denotes the *conjugate transpose* of a complex matrix C); and that congruence on Hermitian matrices preserves inertia (the ordered triple consisting of the number of positive, negative, and zero eigenvalues) and, thus, positive definiteness [33, p. 223]. A symmetric word evaluated at positive definite matrices is inductively congruent to the "center," positive definite matrix. We conclude that

Lemma 4.2.3. *A symmetric word evaluated at positive definite matrices is positive definite.*

A more careful examination (or a simple continuity argument) also proves the following.

Lemma 4.2.4. *A symmetric word evaluated at positive semidefinite matrices is positive semidefinite.*

Conversely, it may be shown that symmetric words are the only words that are positive definite for all positive definite substitutions (see Section 4.3 for a proof). In light of these facts, restricting our consideration to symmetric words seems appropriate.

Next, we discuss the difficulties that arise when considering non-interlaced symmetric words. As the following examples demonstrate, both uniqueness and existence may fail even when $k = n = 2$ and $s = 3$.

Example 4.2.5. *Let* $S(X, B_1, B_2) = XB_1B_2XB_2B_1X$ *and set*

$$B_1 = \begin{bmatrix} 3 & -1 \\ -1 & 1 \end{bmatrix}, \ B_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \ \textit{and} \ \ P = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Then, as is easily verified, the equation $S(X, B_1, B_2) = P$ *has symmetric solutions*

$$X = \begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix} \ \ \textit{and} \ \ X = \begin{bmatrix} x/5 & -x \\ -x & 5x \end{bmatrix},$$

in which x *is an arbitrary real number. In particular, there are infinitely many positive semidefinite solutions (in two distinct solution classes). Notice also that the kernel of a solution* X *and that of* P *can be different. For interlaced words, this situation cannot occur (see Lemma 4.6.1).* □

Example 4.2.6. *Let* S *and* B_1, B_2 *be as in the previous example, but instead set*

$$P = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Then, there are no positive semidefinite solutions to $S(X, B_1, B_2) = P$*. To verify this, suppose that*

$$X = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

is a complex solution to $S(X, B_1, B_2) = P$*. Computing the ideal generated by the 4 consequent polynomial equations (using Maple or Macaulay 2 to find the reduced Gröbner basis), we find that it is the entire ring* $\mathbb{C}[e, f, g, h]$*. In particular, there are no matrix solutions over* $\mathbb{C}$ *to the given equation, much less positive semidefinite ones.* □

4.3 Relations Between Positive Definite Words

In this section, we explain our restriction to symmetric words. Specifically, we prove that a word $W(A, B)$ in two letters A and B is positive definite for all positive definite substitutions if and only if the word is symmetric.

We begin by illustrating some of the subtlety of the problem. Let B and P be positive definite matrices. In Example (4.2.2) we saw that

$$P^{1/2}\left(P^{-1/2}B^{-1}P^{-1/2}\right)^{1/2}P^{1/2} = B^{-1/2}\left(B^{1/2}PB^{1/2}\right)^{1/2}B^{-1/2},$$

even though both expressions are quite different. In fact, both sides of the above equality are the unique solution X to the symmetric word equation,

$$S(X, B) = XBX = P.$$

Fortunately, such behavior does not occur with words, as the following discussion illustrates.

Let $\mathcal{W}$ be the set of words in two letters A and B, and fix a, b to be two $n \times n$ complex matrices. Consider the *evaluation homomorphism* $Eval_{a,b} : \mathcal{W} \to \mathbb{M}_n(\mathbb{C})$ which sends a word $W(A, B)$ to the matrix $W(a, b)$ produced by substituting the matrices a and b for the letters A and B, respectively. By convention, the empty word is sent to the identity matrix by this map. We describe a pair of positive definite a and b for which this function is injective.

Lemma 4.3.1. *The map $Eval_{a,b}$ is injective when*

$$a = \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}, \ b = \begin{bmatrix} 1 & 1 \\ 1 & 3 \end{bmatrix}.$$

Proof. Let a, b be the matrices in the statement of the lemma, and let W_1 and W_2 be two words for which $W_1(a, b) = W_2(a, b)$; we must show that W_1 and W_2 are the same word. If either W_1 or W_2 is the empty word, then the claim is clear (take a determinant). Furthermore, since a and b are invertible, we may suppose that $W_1 = AU$ and $W_2 = BV$ for some words U and V.

Let x and y be indeterminates. Given a word W, we set

$$\begin{bmatrix} W^x x + W^y y \\ W_x x + W_y y \end{bmatrix} = W(a,b) \begin{bmatrix} x \\ y \end{bmatrix},$$

for natural numbers W^x, W^y, W_x, W_y. Notice that by our choice of a and b, we cannot have both W^x and W^y equal to zero. A direct computation shows that $(AU)^x - (AU)_x = 2U^x$ and that $(BV)^x - (BV)_x = -2V_x$. By assumption, these two numbers are equal so that $U^x + V_x = 0$. Since these two quantities are nonnegative integers, it follows that $U^x = V_x = 0$. Similarly, the equality $(AU)^y - (AU)_y = (BV)^y - (BV)_y$ implies that $U^y = V_y = 0$. This contradiction finishes the proof. □

Corollary 4.3.2. *The following are equivalent for a word W.*

(1) *W is positive definite for all substitutions of positive definite A and B*

(2) *W is Hermitian for all substitutions of positive definite A and B*

(3) *W is Hermitian for all 2×2 substitutions of positive definite A and B*

(4) *W is symmetric ("palindromic")*

In particular, if a word is Hermitian for all 2×2 substitutions of positive definite A and B, then the word is necessarily positive definite for all such substitutions.

Proof. (1) ⇒ (2) ⇒ (3) is clear. If $W(A,B)$ is always Hermitian for 2×2 positive definite A and B, then $W(A,B)^* = W(A,B)$ for all such A and B. But then Lemma 4.3.1 says that W^* and W must be identical as words. It follows that W is symmetric. This proves (3) ⇒ (4). Finally, if W is symmetric, Lemma 4.2.3 says that W will always be positive definite for any positive definite A and B. This completes the proof. □

4.4 Applications

Symmetric word equations were first encountered while studying a trace conjecture [27] involving words in two letters A and B (see also [28, 31]).

Conjecture 4.4.1. *A word in two letters A and B has positive trace for every pair of real positive definite A and B if and only if the word is symmetric or a product (juxtaposition) of 2 symmetric words.*

For each solvable symmetric word equation, one can identify an infinite class of words that admit real positive definite matrices A and B giving those words a negative trace. The following is a brief description of this application. Consider the word $W = BABAAB$, which is not symmetric nor a product of two symmetric words. In light of Conjecture 4.4.1, we would like to verify that there exist real positive definite matrices A and B giving W a negative trace. This is surprisingly difficult, as the methods in [27] show. Resulting A and B that exhibit a negative trace are, for example,

$$A_1 = \begin{bmatrix} 1 & 20 & 210 \\ 20 & 402 & 4240 \\ 210 & 4240 & 44903 \end{bmatrix} \quad \text{and} \quad B_1 = \begin{bmatrix} 36501 & -3820 & 190 \\ -3820 & 401 & -20 \\ 190 & -20 & 1 \end{bmatrix}.$$

Consider now the following extension. Let T be the word given by $T = S_1S_2$, in which S_1 and S_2 are symmetric words in the letters A and B. If the simultaneous word equations

$$S_1(A,B) = B_1,$$
$$S_2(A,B) = A_1$$

may be solved for positive definite A and B given positive definite A_1 and B_1, then the word TTT^* can have negative trace. Specializing to the case that S_2 is the word A, we have the following.

Corollary 4.4.2. *Let $S = S(A,B)$ be any symmetric word with at least one B. Then the word $SASAAS$ admits real positive definite matrices A and B giving it negative trace.*

Proof. The matrix $B_1A_1B_1A_1A_1B_1$ has negative trace. Using Corollary 4.1.6, the equation $S(A_1, X) = B_1$ has a real positive definite solution $X = B_2$. The two matrices $B = B_2$ and $A = A_1$ are then the desired witnesses. □

We should remark that Conjecture 4.4.1, while interesting in its own right, arises from a long-standing problem in statistical physics. In [6], while studying partition functions of quantum mechanical systems, a conjecture was made regarding a positivity property of traces of matrices. If this property holds, explicit error bounds in a sequence of Padé approximants follow. Recently, in [41], and as previously communicated to us [27], the conjecture of [6] was reformulated by Lieb and Seiringer as a question about the traces of certain sums of words in two positive definite matrices.

Conjecture 4.4.3 (Bessis-Moussa-Villani). *The polynomial* $p(t) = \mathrm{Tr}\left[(A + tB)^m\right]$ *has all positive coefficients whenever* A *and* B *are* $n \times n$ *positive definite matrices.*

The coefficient of t^k in $p(t)$ is the trace of $H_{m,k}(A, B)$, the sum of all words of length m in A and B, in which k B's appear. Since its introduction in [6], many partial results and substantial computational experimentation have been given [10, 15, 27, 30, 47], all in favor of the conjecture's validity. However, despite much work, very little is known about the problem, and it has remained unresolved except in very special cases. Until recently, even the case $m = 6$ and $n = 3$ was unknown. In this case, all coefficients, except $\mathrm{Tr}[H_{6,3}(A, B)]$ were known to be positive [27]. The remaining coefficient $\mathrm{Tr}[H_{6,3}(A, B)]$ can be shown to be positive, but the proof requires notably different methods [30]. The difficulty is that some summands of $H_{6,3}(A, B)$ can have negative trace, precisely the types of words such as $BABAAB$ considered above.

A recent advance on the conjecture (see [26]) has been the derivation of a pair of equations satisfied by A and B with Euclidean norm 1 that minimize a coefficient $\mathrm{Tr}[H_{m,k}(A, B)]$:

$$\begin{cases} AH_{m-1,k}(A,B) & = \; A^2\mathrm{Tr}[AH_{m-1,k}(A,B)] \\ BH_{m-1,k-1}(A,B) & = \; B^2\mathrm{Tr}[BH_{m-1,k-1}(A,B)]. \end{cases}$$

It is possible that some of the techniques developed here can be applied to these more general types of word equations.

4.5 A Class of Uniquely Solvable Equations

In this section, we describe a class of words that are uniquely solvable with solutions that can be explicitly constructed. These words generalize those found in Examples 4.2.1 and 4.2.2.

Definition 4.5.1. A symmetric word is called *totally symmetric* if it can be expressed as a composition of maps of the form

(1) $\pi_{m,B_i}(W) = (WB_i)^m W$, m a positive integer

(2) $\varphi_m(W) = W^m$, m a positive integer

(3) $\mathcal{C}_{B_i}(W) = B_i W B_i$

applied to the letter X.

For example, the word $W = B_1X^2B_2X^2B_2X^2B_1$ may be expressed as the composition, $\mathcal{C}_{B_1} \circ \pi_{2,B_2} \circ \varphi_2(X)$. The utility of this definition becomes clear from the following proposition.

Proposition 4.5.2. *For every totally symmetric word $S(X, B_i)$ and every positive definite B_i and positive semidefinite P, the equation $S(X, B_i) = P$ has a unique positive semidefinite solution X.*

Proof. We induct on the number of compositions involved in the word S; the base case $S = X$ being trivial. If $S = \varphi_m(W)$ for some word W, then $W = P^{1/m}$ is a smaller totally symmetric word equation and any solution X to $S(X, B_i) = P$ satisfies it. A similar statement holds when $S = \mathcal{C}_{B_i}(W)$ (using Lemma 4.2.4), leaving us to deal with π_{m,B_i}.

Without loss of generality, we prove the result for the equation $(XB)^mX = P$. Assume that B and P are given and that X is a solution to $(XB)^mX = P$. Set $Y = B^{1/2}XB^{1/2}$, so that $X = B^{-1/2}YB^{-1/2}$. Then,

$$P = (B^{-1/2}YB^{1/2})^m B^{-1/2}YB^{-1/2} = B^{-1/2}Y^{m+1}B^{-1/2}.$$

Therefore, $Y^{m+1} = B^{1/2}PB^{1/2}$, from which it follows that Y is uniquely determined as $(B^{1/2}PB^{1/2})^{1/(m+1)}$. Hence, X must be the positive semidefinite matrix

$$B^{-1/2}(B^{1/2}PB^{1/2})^{1/(m+1)}B^{-1/2}.$$

Finally, substituting this X into the original equation does verify that it is a solution. This completes the proof. □

The shortest symmetric word equation without a known (closed-form) solution, as above, is $XBX^3BX = P$ (although it is uniquely solvable [40]). An exploration of which equations give rise to such explicit solutions is the focus of future work.

4.6 Reductions

The purpose of this section is to make some reductions that simplify the problem. Given the nature of Theorem 4.1.2 and Conjecture 4.1.3, we begin by noticing that we may assume our interlaced symmetric words are of the following form:

$$S = X^{p_1}B_1X^{p_2}B_2\cdots B_2X^{p_2}B_1X^{p_1}, \tag{4.6.1}$$

in which the exponents p_j are positive. This simplification is accomplished by observing first, that powers of positive definite matrices are positive definite; and second, that congruences of positive semidefinite P are positive semidefinite (Lemma 4.2.4).

We next establish that it suffices to verify our claims when P is invertible. We begin with a useful lemma.

Lemma 4.6.1. *Let $p_1, \ldots, p_k > 0$ and let $B_1, \ldots, B_{k-1}$ be positive definite matrices. Then, for any positive semidefinite matrix X, we have*

$$\ker X = \ker X^{p_k}B_{k-1}\cdots B_2X^{p_2}B_1X^{p_1}.$$

Proof. Set $X = UDU^*$ for a unitary matrix U and $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, in which $\lambda_1 \geq \ldots \geq \lambda_n \geq 0$. Let $Y = X^{p_k}B_{k-1}\cdots B_2X^{p_2}B_1X^{p_1}$, and notice that $\ker U^*XU = \ker U^*YU$ if and only if $\ker X = \ker Y$. Thus, it suffices to argue that

$$\ker D = \ker D^{p_k}B_{k-1}\cdots B_2D^{p_2}B_1D^{p_1},$$

whenever the B_i are positive definite matrices.

Let m be the largest integer such that $\lambda_m \neq 0$, and for each i, let $\widetilde{B}_i$ denote the $m \times m$ leading principal submatrix of B_i, which will be positive definite (see, for instance, [33, p. 472]). Additionally, set $\widetilde{D} = \operatorname{diag}(\lambda_1, \ldots, \lambda_m)$. A straightforward block matrix multiplication then gives us that

$$D^{p_k}B_{k-1}\cdots B_2D^{p_2}B_1D^{p_1} = \begin{bmatrix} \widetilde{D}^{p_k}\widetilde{B}_{k-1}\cdots\widetilde{B}_2\widetilde{D}^{p_2}\widetilde{B}_1\widetilde{D}^{p_1} & 0 \\ 0 & 0 \end{bmatrix}. \tag{4.6.2}$$

Since the leading principal $m \times m$ matrix in this direct sum is invertible, the claim follows. □

Using this lemma, we can prove the following reduction.

Theorem 4.6.2. *If a symmetric word equation has a solution for every positive definite B_i and P, then the symmetric word equation has a solution for every positive definite B_i and positive semidefinite P.*

Proof. Performing a uniform unitary similarity, we may prove the theorem with the supposition that P is of the form,

$$\begin{bmatrix} \widetilde{P} & 0 \\ 0 & 0 \end{bmatrix},$$

for a positive diagonal matrix $\widetilde{P}$ of rank m. Lemma 4.6.1 implies that any positive semidefinite solution X to the symmetric word equation $S(X, B_i) = P$ has the same block form as P. As in the lemma, let $\widetilde{B}_i$ denote the $m \times m$ leading principal (positive definite) submatrix of each B_i.

From these observations, it follows that positive semidefinite solutions X to the equation $S(X, B_i) = P$ correspond in a one-to-one manner with positive definite solutions $\widetilde{X}$ to the equation $S(\widetilde{X}, \widetilde{B}_i) = \widetilde{P}$. This completes the proof. □

The proof above also shows that the question of uniqueness found in Conjecture 4.1.3 may also be simplified.

Theorem 4.6.3. *If a symmetric word equation has a unique solution for all positive definite matrices B_i and P, then the symmetric word equation has a unique solution for all positive definite B_i and each positive semidefinite P.*

We close this section with an interesting interpretation of unique solvability.

Proposition 4.6.4. *Fix positive definite matrices B_i in the unit ball and an interlaced symmetric word $S(X, B_i)$ whose equations are uniquely solvable. Then, the mapping $X \mapsto S(X, B_i)$ from the set of positive semidefinite matrices in the (closed) unit ball to its image is a homeomorphism.*

Proof. The assumptions imply that our map is bijective. Since the set of positive semidefinite matrices in the unit ball is compact, it follows that its inverse is also continuous. □

4.7 Brouwer Mapping Degree

In this section, we give a brief overview of degree theory and some of its main implications. The bulk of this discussion is material taken from [16, 42, 65]. First we introduce some notation. Let U be a bounded open subset of $\mathbb{R}^m$. We denote the set of r-times differentiable functions from U (resp. $\overline{U}$) to $\mathbb{R}^m$ by $C^r(U, \mathbb{R}^m)$ (resp. $C^r(\overline{U}, \mathbb{R}^m)$) (when $r = 0$, $C^r(U, \mathbb{R}^m)$ is the set of continuous functions). The *identity function* $\mathbb{1}$ satisfies $\mathbb{1}(\boldsymbol{x}) = \boldsymbol{x}$. If $f \in C^1(U, \mathbb{R}^m)$, then the *Jacobi matrix* of f at a point $\boldsymbol{x} \in U$ is

$$J_f(\boldsymbol{x}) = \left[\frac{\partial f_j}{\partial x_i}(\boldsymbol{x})\right]_{1 \leq i,j \leq m}$$

and the *Jacobi determinant* (or simply *Jacobian*) of f at $\boldsymbol{x}$ is

$$\det J_f(\boldsymbol{x}).$$

The set of *regular values* of f is

$$\mathrm{RV}(f) = \left\{\boldsymbol{y} \in \mathbb{R}^m : \forall \boldsymbol{x} \in f^{-1}(\boldsymbol{y}),\ J_f(\boldsymbol{x}) \neq 0\right\}$$

and for $\boldsymbol{y} \in \mathbb{R}^m$, we set

$$D^r_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m) = \left\{f \in C^r(\overline{U}, \mathbb{R}^m) : \boldsymbol{y} \notin f(\partial U)\right\}.$$

A function $\deg : D^0_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m) \to \mathbb{R}$ which assigns to each $\boldsymbol{y} \in \mathbb{R}^m$ and $f \in D^0_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m)$ a real number $\deg(f, U, \boldsymbol{y})$ will be called a *degree* if it satisfies the following conditions:

(1) $\deg(f, U, \boldsymbol{y}) = \deg(f - \boldsymbol{y}, U, 0)$ (*translation invariance*).

(2) $\deg(\mathbb{1}, U, \boldsymbol{y}) = 1$ if $\boldsymbol{y} \in U$ (*normalization*).

(3) If U_1 and U_2 are open, disjoint subsets of U such that $\boldsymbol{y} \notin f(\overline{U} \setminus (U_1 \cup U_2))$, then $\deg(f, U, \boldsymbol{y}) = \deg(f, U_1, \boldsymbol{y}) + \deg(f, U_2, \boldsymbol{y})$ (*additivity*).

(4) If $H(t) = tf + (1-t)g \in D^0_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m)$ for all $t \in [0,1]$, then $\deg(f, U, \boldsymbol{y}) = \deg(g, U, \boldsymbol{y})$ (*homotopy invariance*).

Motivationally, one should think of a degree map as somehow "counting" the number of solutions to $f(\boldsymbol{x}) = \boldsymbol{y}$. Condition (1) reflects that the solutions to $f(\boldsymbol{x}) = \boldsymbol{y}$ are the same as those of $f(\boldsymbol{x}) - \boldsymbol{y} = 0$, and since any multiple of a degree will satisfy (1) and (3), condition (2) is a normalization. Additionally, (3) is natural since it requires deg to be additive with respect to components. The following lemma gives a method to show the existence of solutions to $f(\boldsymbol{x}) = \boldsymbol{y}$ by calculating a degree.

Lemma 4.7.1. *Suppose that* $f \in D^0_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m)$. *If a degree satisfies* $\deg(f, U, \boldsymbol{y}) \neq 0$*, then* $\boldsymbol{y} \in f(U)$.

Proof. Using property (3) above with $U_1 = U$ and $U_2 = \emptyset$, we must have that $\deg(f, \emptyset, \mathbf{y}) = 0$. Again using (3) with $U_1 = U_2 = \emptyset$, it follows that if $\mathbf{y} \notin f(\overline{U})$ then $\deg(f, U, \mathbf{y}) = 0$. The contrapositive is now what we want. □

Of course, we need a theorem guaranteeing that a degree even exists.

Theorem 4.7.2. *There is a unique degree* deg. *Moreover,* $\deg(\cdot, U, \boldsymbol{y}) : D^0_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m) \to \mathbb{Z}$.

When functions are differentiable, the degree can be calculated explicitly in terms of Jacobians at solutions to the equation $f(\boldsymbol{x}) = \boldsymbol{y}$.

Theorem 4.7.3. *Suppose that* $f \in D^1_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m)$ *and* $\boldsymbol{y} \in \mathrm{RV}$. *Then the degree of* f *at* $\boldsymbol{y}$ *with respect to* U *is given by*

$$\deg(f, U, \boldsymbol{y}) = \sum_{\boldsymbol{x} \in f^{-1}(\boldsymbol{y})} \operatorname{sgn} \det J_f(\boldsymbol{x}),$$

where this sum is finite and we adopt the convention that $\sum_{\boldsymbol{x} \in \emptyset} = 0$.

The final property of Brouwer degree that we will need is a stronger form of homotopy invariance than that provided by Property (4). We say that a function $H : \overline{U} \times [0,1] \to \mathbb{R}^m$ is a C^0 *homotopy* between $f, g \in C^r(\overline{U}, \mathbb{R}^m)$ if H is continuous on $\overline{U} \times [0,1]$ and if $H(x, 0) = f(x)$ and $H(x, 1) = g(x)$ for all $x \in \overline{U}$.

Theorem 4.7.4. *Suppose* H *is a* C^0 *homotopy between* $f, g \in D^0_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m)$. *Set* $h_t(x) = H(x, t)$ *and suppose that for each* $t \in [0,1]$, $h_t \in D^0_{\boldsymbol{y}}(\overline{U}, \mathbb{R}^m)$. *Then* $\deg(f, U, \boldsymbol{y}) = \deg(g, U, \boldsymbol{y})$.

4.8 Estimates of Solutions

This section is devoted to estimating the norms of positive definite solutions of symmetric word equations. In particular, we show that the set of positive definite solutions to a fixed symmetric word equation $S(X, B_i) = P$ is bounded. Our estimate is the first step in the proof of Theorem 4.1.5. In what follows, we will be using the spectral norm [33, p. 295] on the set of $n \times n$ matrices, so that for positive semidefinite A, the norm of A is just the largest eigenvalue of A.

Lemma 4.8.1. *Fix an interlaced symmetric word $S(X, B_i)$ and a number $\alpha \geq 1$. Then there exists a constant $C = C_{S,\alpha}$ depending only on S and α such that for all positive definite matrices B_i with $\|B_i\| \leq 1$ and $\|B_i^{-1}\| \leq \alpha$ and all positive semidefinite matrices P with $\|P\| \leq 1$ we have the estimate*

$$\|X\| \leq C \tag{4.8.1}$$

for any solution X of the word equation $S(X, B_i) = P$.

Proof. We proceed by way of contradiction. If the statement is false, then for each positive integer j there exist positive semidefinite matrices X_j, P_j and positive definite matrices $B_{i,j}$ such that $S(X_j, B_{i,j}) = P_j$, where $\|B_{i,j}\| \leq 1$, $\|B_{i,j}^{-1}\| \leq \alpha$, $\|P_j\| \leq 1$, and $\|X_j\| \geq j$. By taking a subsequence, if necessary, we may assume that there are positive semidefinite matrices B_i, P and X such that $B_{i,j} \to B_i$, $P_j \to P$, and $\|X_j\|^{-1}X_j \to X$ as $j \to \infty$. It is clear that

$$\|X\| = 1. \tag{4.8.2}$$

Since $\|B_{i,j}^{-1}\|$ is bounded uniformly in j, each B_i is positive definite. Let s be the degree of S. Since $\|X_j\| \geq j$ for all j, if we let $j \to \infty$ in the equation

$$S(\|X_j\|^{-1}X_j, B_{i,j}) = \|X_j\|^{-s}P_j,$$

it follows that

$$S(X, B_i) = 0.$$

Finally, an application of Lemma 4.6.1 gives $X = 0$, which contradicts (4.8.2) and finishes the proof. □

Lemma 4.8.1 allows us to estimate $\|X\|$ in terms of the norms of the B_i and the norm of the word $S(X, B_i)$.

Proposition 4.8.2. *Fix an interlaced symmetric word $S(X, B_1, \ldots, B_k)$ of the form (4.6.1) with degree s and a number $\alpha \geq 1$. There exists a constant $C = C_{S,\alpha}$ depending only on S and α such that for all positive definite matrices B_i with $\|B_i\|\|B_i^{-1}\| \leq \alpha$ and any positive semidefinite X we have*

$$\|X\| \leq C\|B_1\|^{-\frac{2}{s}} \cdots \|B_k\|^{-\frac{2}{s}} \|S(X, B_i)\|^{\frac{1}{s}}. \tag{4.8.3}$$

Proof. Let $C = C_{S,\alpha}$ be the constant in Lemma 4.8.1. By Lemma 4.6.1, if $S(X, B_i) = 0$, then $X = 0$, and the bound is trivial. Otherwise, set $\tilde{B}_i = \|B_i\|^{-1}B_i$, $P = S(X, B_i)$, $\tilde{P} = \|P\|^{-1}P$, and $\tilde{X} = \|B_1\|^{\frac{2}{s}} \cdots \|B_k\|^{\frac{2}{s}} \|P\|^{-\frac{1}{s}} X$. Noticing that $\|\tilde{B}_i^{-1}\| = \|B_i\|\|B_i^{-1}\| \leq \alpha$ and also that $S(\tilde{X}, \tilde{B}_i) = \tilde{P}$, we may apply Lemma 4.8.1 to get that

$$\|\tilde{X}\| \leq C. \tag{4.8.4}$$

Substituting $\tilde{X} = \|B_1\|^{\frac{2}{s}} \cdots \|B_k\|^{\frac{2}{s}} \|P\|^{-\frac{1}{s}} X$ into (4.8.4) and rearranging produces (4.8.3).

□

4.9 Calculation of Jacobi Matrices

From here on, we focus on real $n \times n$ matrices. For the purposes of this section, we shall identify $\mathbb{M}_n = \mathbb{M}_n(\mathbb{R})$ with $\mathbb{R}^d$, where $d = n^2$, by means of the vec operator. If $A = [a_{ij}] \in \mathbb{M}_n$ then $\operatorname{vec} A$ is the column vector obtained by stacking the columns of A below one another:

$$\operatorname{vec} A = [a_{11} \cdots a_{n1}\, a_{12} \cdots \cdots a_{nn}]^T.$$

Recall that the *Kronecker product* of two $n \times n$ matrices A and B is the matrix

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{bmatrix} \in \mathbb{M}_d.$$

The following lemma can be found in [43, page 30]. We reproduce it here for the reader's convenience.

Lemma 4.9.1. *If $A, B, X \in \mathbb{M}_n$, then*

$$\mathrm{vec}\,(AXB) = (B^T \otimes A)\mathrm{vec}\,X.$$

Proof. For a given matrix Q, let Q_k denote the kth column of Q. Let $B = [b_{ij}]$. Then

$$\begin{aligned} (AXB)_k &= AXB_k \\ &= A\left(\sum_{i=1}^{n} b_{ik}X_i\right) = \begin{bmatrix} b_{1k}A & \cdots & b_{nk}A \end{bmatrix} \mathrm{vec}\,X. \end{aligned}$$

Therefore,

$$\mathrm{vec}(AXB) = \begin{bmatrix} b_{11}A & \cdots & b_{n1}A \\ \vdots & \ddots & \vdots \\ b_{1n}A & \cdots & b_{nn}A \end{bmatrix} \mathrm{vec}\,X = (B^T \otimes A)\,\mathrm{vec}\,X.$$

□

Suppose that $Y(X) \in \mathbb{M}_n$ is a function of the matrix variable $X \in \mathbb{M}_n$. Following [43], we define the *derivative* $\frac{dY}{dX}$ of Y with respect to X to be the Jacobi matrix of $\mathrm{vec}\,Y$ with respect to $\mathrm{vec}\,X$. That is, if $[y_1, \ldots, y_d]^T = \mathrm{vec}\,Y$ and $[x_1, \ldots, x_d]^T = \mathrm{vec}\,X$, then

$$\frac{dY}{dX} = \left[\frac{\partial y_i}{\partial x_j}\right].$$

Notice that it follows from Lemma 4.9.1 that

$$\frac{d(AXB)}{dX} = B^T \otimes A. \tag{4.9.1}$$

Using (4.9.1), we may derive a matrix calculus version of the product rule (see [43] for more on matrix calculus).

Proposition 4.9.2. *Let $Y(X) \in \mathbb{M}_n$ and $Z(X) \in \mathbb{M}_n$ be functions of the matrix variable $X \in \mathbb{M}_n$. Then*

$$\frac{d(YZ)}{dX} = (Z^T \otimes I)\frac{dY}{dX} + (I \otimes Y)\frac{dZ}{dX}. \tag{4.9.2}$$

Motivated by Theorem 4.7.3, we want to calculate the derivative $\frac{dW}{dX}$ of a word $W = W(X, B_1, \ldots, B_k)$. To state the result, we need to introduce some notation. Let W have degree $s \geq 1$. Enumerate the occurrences of X in $W(X, B_i)$ from left to right, and for each $j \in \{1, \ldots, s\}$ let $W_j^L(X, B_i)$ be the portion of $W(X, B_i)$ that appears to the left of the jth occurrence of X. For instance, if

$$W(X, B_1, B_2) = B_2^3 X B_1^2 B_2 X B_2 B_1 X^2 B_2 X,$$

then $W_4^L(X, B_1, B_2) = B_2^3 X B_1^2 B_2 X B_2 B_1 X$. We adopt the convention that $W_1^L = I$ if X is the first letter of the word. In a similar way we define $W_j^R(X, B_i)$ to be the portion of $W(X, B_i)$ that appears to the right of the jth appearance of X. Notice that

$$W(X, B_i) = W_j^L(X, B_i) X W_j^R(X, B_i)$$

for any $j = 1, \ldots, s$.

Proposition 4.9.3. *Let $W = W(X, B_i)$ be a word of degree s, and $B_i \in \mathbb{M}_n$. Then*

$$\frac{dW}{dX} = \sum_{j=1}^{s} W_j^R(X, B_i)^T \otimes W_j^L(X, B_i). \tag{4.9.3}$$

Proof. We proceed by induction on the length of W. For the words X and BX ($B = B_1, \ldots, B_k$), (4.9.3) is a special case of (4.9.1). Now suppose that (4.9.3) holds for a fixed word $W = W(X, B_i)$ of degree s. Pick $B \in \{B_1, \ldots, B_k\}$ and set

$$\overline{W}(X, B_i) = W(X, B_i) B.$$

Then (4.9.1) and (4.9.2) imply that

$$\begin{aligned}
\frac{d\overline{W}}{dX} &= (B^T \otimes I) \frac{dW}{dX} \\
&= (B^T \otimes I) \sum_{j=1}^{s} W_j^R(X, B_i)^T \otimes W_j^L(X, B_i) \\
&= \sum_{j=1}^{s} (W_j^R(X, B_i) B)^T \otimes W_j^L(X, B_i) \\
&= \sum_{j=1}^{s} \overline{W}_j^R(X, B_i)^T \otimes \overline{W}_j^L(X, B_i),
\end{aligned}$$

so formula (4.9.3) holds for $\overline{W}$.

Next set $\widetilde{W}(X, B_i) = W(X, B_i)X$. Appealing again to (4.9.1) and (4.9.2), we compute:

$$\begin{aligned}\frac{d\widetilde{W}}{dX} &= (X^T \otimes I)\frac{dW}{dX} + (I \otimes W(X, B_i)) \\ &= (X^T \otimes I)\sum_{j=1}^{s} W_j^R(X, B_i)^T \otimes W_j^L(X, B_i) + (I \otimes \widetilde{W}_{s+1}^L) \\ &= \sum_{j=1}^{s+1} \widetilde{W}_j^R(X, B_i)^T \otimes \widetilde{W}_j^L(X, B_i),\end{aligned}$$

and so (4.9.3) holds for $\widetilde{W}$. This completes the induction and the proof. □

We next write down expression (4.9.3) for some explicit interlaced symmetric words, beginning with the most basic one.

Example 4.9.4. *For a positive integer s, the Jacobi matrix of $\operatorname{vec} X^s$ with respect to $\operatorname{vec} X$ is given by*

$$\frac{dX^s}{dX} = \sum_{j=1}^{s} (X^{s-j})^T \otimes X^{j-1}. \tag{4.9.4}$$

In particular, since the Kronecker product of two positive (semi)definite matrices is also positive (semi)definite (see [34, p. 245]), $\frac{dX^s}{dX}$ is positive (semi)definite whenever X is positive (semi)definite.

Example 4.9.5. *Consider the symmetric word S in two letters given by*

$$S(X, B) = XBX^2B^3X^2BX.$$

If B is positive definite and X is symmetric, then

$$\begin{aligned}\frac{dS}{dX} &= XBX^2B^3X^2B \otimes I + XBX^2B^3X \otimes XB + XBX^2B^3 \otimes XBX \\ &\quad +XBX \otimes XBX^2B^3 + XB \otimes XBX^2B^3X + I \otimes XBX^2B^3X^2B.\end{aligned}$$

4.10 The Brouwer Degree of Symmetric Word Equations

Our proof of Theorem 4.1.5 consists of two main steps. In the first, we calculate the degree of the simple map $\varphi_s(X) = X^s$ and show that it is 1. And in the second, we create a homotopy from the function $f(X) = S(X, B_i)$ to $\varphi_s(X)$ and apply Theorem 4.7.4. Before initiating our proof, we need to identify the set of real positive definite matrices with an *open* set in Euclidean space. To this end, we identify the set Sym_n of real symmetric matrices with $\mathbb{R}^m$, in which $m = \frac{1}{2}n(n+1)$, by identifying a real symmetric matrix $A = [a_{ij}]$ with the point

$$\mu(A) = (a_{11}, \ldots, a_{n1}, a_{22}, \ldots, a_{n2}, \ldots, a_{nn}).$$

More precisely, if $A \in \mathbb{M}_n$ then we define $\mu(A) = (y_1, \ldots, y_m)$, where

$$y_{\frac{1}{2}(2n-j)(j-1)+i} = a_{ij}, \quad 1 \leq j \leq i \leq n.$$

The restriction $\mu|_{\mathrm{Sym}_n}$ is a linear isomorphism from Sym_n onto $\mathbb{R}^m$. We denote by ν the inverse of $\mu|_{\mathrm{Sym}_n}$. Let

$$\mathcal{O} = \{\mu(X) \mid X \text{ is positive definite}\}.$$

The set of positive definite matrices is therefore identified with the open subset $\mathcal{O} \subset \mathbb{R}^m$, and the set of positive semidefinite matrices is identified with the set $\overline{\mathcal{O}}$.

Define a function $\mathcal{P}_s : \mathbb{R}^m \to \mathbb{R}^m$ by

$$\mathcal{P}_s = \mu \circ \varphi_s \circ \nu.$$

Since φ_s maps Sym_n into itself, it follows that $\mathcal{P}_s(\mu(X)) = \mu(X^s)$ for every symmetric matrix X. We intend to show that $\det J_{\mathcal{P}_s}(\mu(X)) > 0$ when X is positive definite. First, however, we need a lemma describing a relationship between eigenvalues of Jacobi matrices for functions $f : \mathbb{R}^d \to \mathbb{R}^d$ and their restrictions $\widetilde{f}$ to certain subspaces. In what follows, the set of eigenvalues of a matrix H is denoted by $\sigma(H)$.

Lemma 4.10.1. *Let $f : \mathbb{R}^d \to \mathbb{R}^d$ be a C^1 map and $V \subseteq \mathbb{R}^d$ be a linear subspace of $\mathbb{R}^d$ such that $f(V) \subseteq V$. Let $\pi : \mathbb{R}^m \to V$ be a linear isomorphism, and let $\widetilde{f} : \mathbb{R}^m \to \mathbb{R}^m$ be given by $\widetilde{f} = \pi^{-1} \circ f \circ \pi$. Then for every $\boldsymbol{x} \in V$, we have*

$$\sigma(J_{\widetilde{f}}(\pi^{-1}(\boldsymbol{x}))) \subseteq \sigma(J_f(\boldsymbol{x})).$$

In particular, if $\boldsymbol{x} \in V$ and $J_f(\boldsymbol{x})$ is positive definite, then $J_{\widetilde{f}}(\pi^{-1}(\boldsymbol{x}))$ has positive eigenvalues.

Proof. Let $\{e_1, \ldots, e_d\}$ be the standard basis for $\mathbb{R}^d$. By choosing a linear change of variables $u : \mathbb{R}^d \to \mathbb{R}^d$ such that $u(V) = \operatorname{span}\{e_1, \ldots, e_m\}$ and considering the C^1 map $g = u \circ f \circ u^{-1}$, we may reduce to the case that $V = \operatorname{span}\{e_1, \ldots, e_m\}$. We may likewise assume that $\pi(z_1, \ldots, z_m) = (z_1, \ldots, z_m, 0, \ldots, 0)$.

Write $f = (f_1, \ldots, f_d)$ and let $\boldsymbol{x} \in V$. If $j \le m < k$, we have

$$f_k(\boldsymbol{x} + te_j) = 0 \text{ for all } t \in \mathbb{R}$$

since $f(V) \subseteq V$. Therefore,

$$\frac{\partial f_k}{\partial x_j}(\boldsymbol{x}) = 0 \text{ for all } j \le m < k. \tag{4.10.1}$$

It follows that $J_f(\boldsymbol{x})$ has the block form

$$J_f(\boldsymbol{x}) = \begin{bmatrix} J_0 & * \\ 0 & * \end{bmatrix},$$

in which J_0 is the $m \times m$ leading principle submatrix of $J_f(\boldsymbol{x})$. In particular, this implies that $\sigma(J_0) \subset \sigma(J_f(\boldsymbol{x}))$. It is straightforward to verify that

$$\widetilde{f}(x_1, \ldots, x_m) = (f_1(x_1, \ldots, x_m, 0, \ldots, 0), \ldots, f_m(x_1, \ldots, x_m, 0, \ldots, 0)),$$

from which it follows that $J_{\widetilde{f}}(\pi^{-1}(\boldsymbol{x})) = J_0$. This proves the lemma. □

Lemma 4.10.2. *At any positive definite matrix X, the Jacobi matrix $J_{\mathcal{P}_s}(\mu(X))$ of the map $\mathcal{P}_s$ has positive eigenvalues. In particular,* $\det J_{\mathcal{P}_s}(\mu(X)) > 0$.

Proof. Let $V = \{\operatorname{vec} X \mid X \in \operatorname{Sym}_n\}$ be the linear subspace of $\mathbb{R}^d$ identified with Sym_n. The function $\widetilde{\mathcal{P}}_s : \mathbb{R}^d \to \mathbb{R}^d$ defined by

$$\widetilde{\mathcal{P}}_s(\operatorname{vec} X) = \operatorname{vec} X^s$$

maps V into itself. Let $\pi = \operatorname{vec} \circ \nu$, and notice that $\pi : \mathbb{R}^m \to V$ is a linear isomorphism and that $\mathcal{P}_s = \pi^{-1} \circ \widetilde{\mathcal{P}}_s \circ \pi$. By Example 4.9.4, if X is a positive definite matrix, then $J_{\widetilde{\mathcal{P}}_s}(\operatorname{vec} X) = dX^s/dX$ is also positive definite. Applying Lemma 4.10.1, we conclude that the Jacobi matrix $J_{\mathcal{P}_s}(\pi^{-1}(\operatorname{vec} X)) = J_{\mathcal{P}_s}(\mu(X))$ has positive eigenvalues at any positive definite X. □

Proposition 4.10.3. *Let s be a positive integer, P a positive definite matrix, and $\mathcal{V} \subset \mathcal{O}$ a bounded open set containing $\mu(P^{1/s})$. Let g be the function $\mathcal{P}_s$ restricted to $\overline{\mathcal{O}}$. Then*

$$\deg(g, \mathcal{V}, \mu(P)) = 1.$$

Proof. Lemma 4.10.2 implies that $\mu(P)$ is a regular value for g. Using Theorem 4.7.3 and Lemma 4.10.2, we calculate:

$$\deg(g, \mathcal{V}, \mu(P)) = \sum_{\boldsymbol{x} \in g^{-1}(\mu(P))} \operatorname{sgn}\ \det J_g(\boldsymbol{x}) = \operatorname{sgn} \det J_g(\mu(P^{1/s})) = 1.$$

□

We are now ready to calculate the Brouwer degree of a general symmetric word equation.

Proof of Theorem 4.1.5. From the discussion in Section 4.6 we may assume that our interlaced symmetric word $S(X, B_1, \ldots, B_k)$ is of the form (4.6.1). Fix positive definite matrices $B_1, \ldots, B_k$, a positive definite matrix P and set $f(X) = S(X, B_i)$. Also set $\widetilde{f} = \mu \circ f \circ \nu$. We will show that there is a bounded, open subset $\mathcal{V} \subset \mathcal{O}$ such that for all bounded, open $\mathcal{U} \subset \mathcal{O}$ with $\mathcal{V} \subset \mathcal{U}$ we have

$$\deg(\widetilde{f}, \mathcal{U}, \mu(P)) = 1. \tag{4.10.2}$$

By Proposition 4.8.2, there exists a constant K independent of t such that any positive definite solution X of the equation $S(X, tB_i + (1-t)I) = P$ has $\|X\| < K$. Indeed, if

$$\alpha = \max_{1 \le i \le k,\, 0 \le t \le 1} \|tB_i + (1-t)I\| \cdot \|(tB_i + (1-t)I)^{-1}\| < \infty$$

and

$$\beta = \min_{1 \le i \le k,\, 0 \le t \le 1} \|tB_i + (1-t)I\| > 0,$$

then we must have

$$\|X\| \le C_{S,\alpha} \beta^{-\frac{2k}{s}} \|P\|^{\frac{1}{s}} < \infty.$$

Let $V = V_K$ be the open set of positive definite matrices with norm less than K. For each $t \in [0, 1]$, let f_t be the function from the positive semidefinite matrices into itself given by $f_t(X) = S(X, tB_i + (1-t)I)$. From our choice of K, it follows that $f_t(X) \neq P$ when X is positive definite with $\|X\| = K$. Moreover, if X is singular, then taking a determinant shows that $f_t(X) \neq P$. Thus $P \notin f_t(\partial V)$ for each $t \in [0,1]$.

Let $\mathcal{V} = \mu(V)$ and $\widetilde{f}_t = \mu \circ f_t \circ \nu$. Then if $\mathcal{V} \subset \mathcal{U} \subset \mathcal{O}$, we have $\mu(P) \notin \widetilde{f}_t(\partial \mathcal{U})$ for $t \in [0,1]$. Since $(\boldsymbol{x}, t) \mapsto \widetilde{f}_t(\boldsymbol{x})$ is continuous, Theorem 4.7.4 implies that

$$\deg(\widetilde{f}_0, \mathcal{U}, \mu(P)) = \deg(\widetilde{f}_1, \mathcal{U}, \mu(P)).$$

Since $\widetilde{f}_0 = \mathcal{P}_s$ and $\widetilde{f}_1 = \widetilde{f}$, (4.10.2) now follows from Proposition 4.10.3. □

4.11 Proof of Theorem 4.1.4

The following corollary of Theorem 4.1.5 will allow us to prove Theorem 4.1.4.

Corollary 4.11.1. *Fix an interlaced symmetric word S and let $\widetilde{f} = \widetilde{f}_S$ be as in the proof of Theorem 4.1.5. Suppose there is a positive definite matrix X_0 such that*

$$\det J_{\widetilde{f}}(\mu(X_0)) < 0.$$

Then the symmetric word equation

$$S(X, B_i) = S(X_0, B_i)$$

has at least two real solutions X.

Proof. Let X_0 be as in the statement of the corollary, and set $P = S(X_0, B_i)$. If $\mu(P)$ is a regular value of $\widetilde{f}$, then Theorems 4.1.5 and 4.7.3 imply that there must be at least two solutions X_1 and X_2 of $S(X, B_i) = P$ such that

$$\det J_{\widetilde{f}}(\mu(X_i)) > 0, \quad i = 1, 2.$$

If $\mu(P)$ is not a regular value of $\widetilde{f}$, then there exists a positive definite matrix X_1 such that $S(X_1, B_i) = P$ and

$$J_{\widetilde{f}}(\mu(X_1)) = 0.$$

Since $J_{\widetilde{f}}(\mu(X_1)) \neq J_{\widetilde{f}}(\mu(X_0))$, it follows that $X_0 \neq X_1$. □

Let S and $\widetilde{f}$ be as in Corollary 4.11.1. We outline a method for obtaining the smaller Jacobian matrix $J_{\widetilde{f}}(\mu(X))$ from the larger Jacobian matrix dS/dX. To simplify the bookkeeping of indices, define

$$\alpha(i,j) = n(j-1) + i, \quad i, j = 1, \ldots, n$$

and

$$\beta(k,l) = \frac{1}{2}(2n-l)(l-1) + k, \quad 1 \leq l \leq k \leq n.$$

Thus if $X = [x_{ij}] \in \mathbb{M}_n$, then the $\alpha(i,j)$th entry of $\operatorname{vec} X$ is equal to x_{ij}, $i, j = 1, \ldots, n$. Likewise, the $\beta(k,l)$th entry of $\mu(X)$ is x_{kl}, $1 \leq l \leq k \leq 1$.

The Jacobi matrix $J_{\widetilde{f}}$ of the map

$$\begin{aligned} \widetilde{f} &= \mu \circ (X \mapsto S(X, B_i)) \circ \nu \\ &= (\mu \circ \operatorname{vec}^{-1}) \circ (\operatorname{vec} \circ (X \mapsto S(X, B_i)) \circ \operatorname{vec}^{-1}) \circ (\operatorname{vec} \circ \nu) \end{aligned}$$

is given by

$$J_{\widetilde{f}}(\mu(X)) = M(dS/dX)N,$$

in which $M \in \mathbb{M}_{m \times d}$ is the matrix representation of $\mu \circ \operatorname{vec}^{-1}$ and $N \in \mathbb{M}_{d \times m}$ is the matrix representation of $\operatorname{vec} \circ \nu$. It is easy to see that if $1 \leq i, j \leq n$ and $1 \leq l \leq k \leq n$, the $(\alpha(i,j), \beta(k,l))$ entry of N is

$$\begin{cases} 1 & \text{if} \quad i = k, j = l \quad \text{or} \quad i = l, j = k \\ 0 & \text{otherwise} \end{cases}$$

and the $(\beta(k,l), \alpha(i,j))$ entry of M is

$$\begin{cases} 1 & \text{if} \quad i = k, j = l \\ 0 & \text{otherwise.} \end{cases}$$

We are now ready to prove the main result of this section.

Proof of Theorem 4.1.4. Let A_1 and B_1 be as in Section 4.4, and let S be the symmetric word

$$S(X, B) = XBX^2B^3X^2BX.$$

Let $f(X) = S(X, A_1)$ and $\widetilde{f} = \mu \circ f \circ \nu$. Using Maple[1], we calculate

$$\det J_{\widetilde{f}}(B_1) = -633705909477329213831177437148144640 < 0.$$

By Corollary 4.11.1, it follows that the symmetric word equation

$$S(X, A_1) = S(B_1, A_1)$$

has at least two distinct real positive definite solutions X. □

As a final remark, we note that there are many other words which can be shown to have multiple solutions using the techniques found in the proof of Theorem 4.1.4. We list a few of them below:

$$\begin{aligned}
&XBX^kBX, \quad 9 \leq k \leq 20\\
&XBXB^2X^kB^2XBX, \quad 2 \leq k \leq 16\\
&XBX^kB^3X^kBX, \quad 2 \leq k \leq 15\\
&XB^2XBX^kBXB^2X, \quad 6 \leq k \leq 40.
\end{aligned}$$

In general, we do not know how to characterize those equations which give rise to unique solutions.

[1] Code that performs this calculation is available at http://math.berkeley.edu/∼chillar.

Bibliography

[1] W. Adams and P. Loustaunau, *An introduction to Gröbner bases,* Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.

[2] G. Ahlbrandt and M. Ziegler, *Quasi-finitely axiomatizable totally categorical theories,* Stability in model theory (Trento, 1984), Ann. Pure Appl. Logic **30** (1986), no. 1, 63–82.

[3] S. Armstrong and C. Hillar, *A degree theory approach to solving symmetric word equations in positive definite letters*, in preparation.

[4] M. Aschenbrenner and C. Hillar, *Finite generation of symmetric ideals*, Trans. Amer. Math. Soc., to appear.

[5] R. Bhatia, *Matrix analysis*, Springer, New York, 1996.

[6] D. Bessis, P. Moussa, M. Villani, *Monotonic converging variational approximations to the functional integrals in quantum statistical mechanics*, J. Math. Phys. **16**, 2318–2325 (1975).

[7] A.R. Camina and D.M. Evans, *Some infinite permutation modules,* Quart. J. Math. Oxford Ser. (2) **42** (1991), no. 165, 15–26.

[8] D. Cox, J. Little, D. O'Shea, *Using algebraic geometry*, Springer, New York, 1998.

[9] D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, New York, 1997.

[10] M. Drmota, W. Schachermayer, J. Teichmann, *A hyper-geometric approach to the BMV-conjecture*, Monatshefte fur Mathematik, to appear.

[11] J.J. Duistermaat and V. Guillemin, *The spectrum of positive elliptic operators and periodic bicharacteristics*, Inv. Math. 25 (1975) 39-79.

[12] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics **203**, Springer-Verlag, New York, 1995.

[13] P. Erdős and R. Rado, *A theorem on partial well-ordering of sets of vectors,* J. London Math. Soc. **34** (1959), 222–224.

[14] G. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics.* Springer-Verlag London Ltd., London, 1999.

[15] M. Fannes and D. Petz, *Perturbation of Wigner matrices and a conjecture*, Proc. Amer. Math. Soc. **131** (2003), 1981–1988.

[16] I. Fonseca and W. Gangbo, *Degree theory in analysis and applications*, Oxford University Press, New York, 1995.

[17] D. Fried, *Cyclic resultants of reciprocal polynomials*, in Holomorphic Dynamics (Mexico 1986), Lecture Notes in Math. 1345, Springer Verlag, 1988, 124-128.

[18] Guoqiang Ge, *Algorithms related to multiplicative representations of algebraic numbers*, PhD thesis, Math Dept, U. C. Berkeley, 1993.

[19] D. G. D. Gray, *The structure of some permutation modules for the symmetric group of infinite degree,* J. Algebra **193** (1997), no. 1, 122–143.

[20] V. Guillemin, *Wave trace invariants*, Duke Math. J. 83 (1996), 287-352.

[21] W.A. Harris and Jr., Y. Sibuya, *The n-th roots of solutions of linear ordinary differential equations*, Proc. Amer. Math. Soc. **97** (1986), 207–211.

[22] W.A. Harris and Jr., Y. Sibuya, *The reciprocals of solutions of linear ordinary differential equations*, Adv. in Math. **58** (1985), 119–132.

[23] G. Higman, *Ordering by divisibility in abstract algebras*, Proc. London Math. Soc. (3) **2** (1952), 326–336.

[24] C. Hillar, *Logarithmic derivatives of solutions to linear differential equations*, Proc. Amer. Math. Soc., **132** (2004), 2693-2701.

[25] C. Hillar, *Cyclic resultants*, J. Symb. Comp., **39** (2005), 653–669.

[26] C. Hillar, *Advances on the Bessis-Moussa-Villani trace conjecture*, preprint.

[27] C. Hillar and C. R. Johnson, *Eigenvalues of words in two positive definite letters*, SIAM J. Matrix Anal. Appl., **23** (2002), 916–928.

[28] C. Hillar and C. R. Johnson, *Positive eigenvalues of generalized words in two Hermitian positive definite matrices.* Novel approaches to hard discrete optimization (Waterloo, ON, 2001), 111-122, Fields Inst. Commun., 37, Amer. Math. Soc., Providence, RI, 2003.

[29] C. Hillar and C. R. Johnson, *Symmetric word equations in two positive definite letters*, Proc. Amer. Math. Soc., **132** (2004), 945-953.

[30] C. Hillar and C. R. Johnson, *On the positivity of the coefficients of a certain polynomial defined by two positive definite matrices*, J. Stat. Phys., **118** (2005), 781–789.

[31] C. Hillar, C. R. Johnson, I. M. Spitkovsky, *Positive eigenvalues and two-letter generalized words*, Electron. J. Linear Algebra, **9** (2002), 21-26.

[32] C. Hillar and L. Levine, *Polynomial recurrences and cyclic resultants*, preprint.

[33] R. Horn and C. R. Johnson, *Matrix analysis*, Cambridge University Press, New York, 1985.

[34] R. Horn and C. R. Johnson, *Topics in matrix analysis*, Cambridge University Press, New York, 1991.

[35] A. Iantchenko, J. Sjöstrand, M. Zworski, *Birkhoff normal forms in semi-classical inverse problems*, Math. Res. Lett. **9** (2002), 337–362.

[36] T. A. Jenkyns and C. St. J. A. Nash-Williams, *Counterexamples in the theory of well-quasi-ordered sets.* in: F. Harary (ed.), *Proof Techniques in Graph Theory (Proc. Second Ann Arbor Graph Theory Conf., Ann Arbor, Mich., 1968)*, pp. 87–91, Academic Press, New York, 1969.

[37] K. Kedlaya, *Quantum computation of zeta functions of curves*, math.NT/0411623, preprint, 2004.

[38] J. B. Kruskal, *The theory of well-quasi-ordering: A frequently discovered concept*, J. Combinatorial Theory Ser. A **13** (1972), 297–305.

[39] S. Lang, *Algebra -3rd ed*, Addison-Wesley Publishing Company, New York, 1993.

[40] J. Lawson and Y. Lim, *Solving symmetric matrix word equations via symmetric space machinery*, preprint.

[41] E. H. Lieb and R. Seiringer, *Equivalent forms of the Bessis-Moussa-Villani conjecture*, J. Stat. Phys., **115** (2004), 185-190.

[42] N. Lloyd, *Degree theory*, Cambridge University Press, London, 1978.

[43] J. R. Magnus and M. Neudecker, *Matrix differential calculus with applications in statistics and econometrics*, John Wiley, New York, 1999.

[44] A. Mead, E. Ruch, A. Schoenhofer, *Theory of chirality functions, generalized for molecules with chiral ligands.* Theoretica Chimica Acta **29** (1973), 269–304.

[45] R. Michler, *Gröbner bases of symmetric quotients and applications,* in: C. Christensen et al. (eds.), *Algebra, Arithmetic and Geometry with Applications (West Lafayette, IN, 2000),* pp. 627–637, Springer-Verlag, Berlin, 2004.

[46] E. Miller and B. Sturmfels, *Combinatorial commutative algebra*, Springer, 2004.

[47] Nathan Miller, 3×3 *cases of the Bessis-Moussa-Villani conjecture*, Princeton University Senior Thesis, 2004.

[48] E. Milner, *Well-quasi-ordering of sequences of ordinal numbers,* J. London Math. Soc. **43** (1968), 291–296.

[49] C. St. J. A. Nash-Williams, *On well-quasi-ordering finite trees*, Proc. Cambridge Philos. Soc. **59** (1963), 833–835.

[50] C. St. J. A. Nash-Williams, *On well-quasi-ordering transfinite sequences*, Proc. Cambridge Philos. Soc. **61** (1965), 33–39.

[51] Y. E. Nesterov and M. J. Todd, *Self-scaled barriers and interior-point methods for convex programming*, Mathematics of Operations Research **22** (1997), 1-42.

[52] K. Purbhoo, *A nullstellensatz for amoebas*, http://math.berkeley.edu/~kpurbhoo/papers/amoebas.pdf, 2004.

[53] R. Rado, *Partial well-ordering of sets of vectors,* Mathematika **1** (1954), 89–95.

[54] E. Ruch and A. Schoenhofer, *Theory of chirality functions.* Theoretica Chimica Acta **19** (1970), 225–87.

[55] E. Ruch, A. Schoenhofer, I. Ugi, *Vandermonde determinants as an approximation expression for chirality observation, their application in stereo-chemistry, and in the calculation of optical activity*, Theoretica Chimica Acta **7** (1967), 420–32.

[56] B. E. Sagan, *The symmetric group. Representations, combinatorial algorithms, and symmetric functions*, Second edition, Graduate Texts in Mathematics **203**, Springer-Verlag, New York, 2001

[57] M. Saito, B. Sturmfels, N. Takayama, *Gröbner deformations of hypergeometric differential equations*, Springer, New York, 2000.

[58] P. Sebastiani, *On the derivatives of matrix powers*, SIAM J. Matrix Anal. Appl., **17** (1996), 640-648.

[59] I. Shafarevich, *Basic algebraic geometry*, Springer-Verlag, Berlin, 1974.

[60] M.F. Singer, *Algebraic relations among solutions of linear differential equations*, Trans. Amer. Math. Soc. **295** (1986), 753–763.

[61] S. Sperber, *Solutions of differential equations*, Pacific Journal of Mathematics. **124** (1986), 249–256.

[62] R. Stanley, *Enumerative combinatorics, vol. 2*, Cambridge University Press, Cambridge, UK, 1999.

[63] W. H. Stevens, *Recursion formulas for some abelian knot invariants*, Journal of Knot Theory and Its Ramifications, Vol. 9, No. 3 (2000) 413-422.

[64] B. Sturmfels, *Gröbner bases and convex polytopes*, AMS University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996.

[65] G. Teschl, *Nonlinear functional analysis*, www.mat.univie.ac.at/ gerald/ftp/book-nlfa/.

[66] E. Zeidler, *Applied functional analysis: applications to mathematical physics*, Springer-Verlag, New York, 1995.