1-1-2011

Applications of Convex and Algebraic Geometry to Graphs and Polytopes

Mohamed Omar
Harvey Mudd College

Applications of Convex and Algebraic Geometry to Graphs and Polytopes

By

MOHAMED OMAR

B.Math. (University of Waterloo) 2006
M.Math. (University of Waterloo) 2007

DISSERTATION

Submitted in partial satisfaction of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

Mathematics

in the

OFFICE OF GRADUATE STUDIES

of the

UNIVERSITY OF CALIFORNIA

DAVIS

Approved:

Jesús De Loera, Chair

Eric Babson

Brian Osserman

Committee in Charge

2011

Contents

Mohamed Omar
June 2011
Mathematics

Applications of Convex and Algebraic Geometry to Graphs and Polytopes

Abstract

This thesis explores the application of nonlinear algebraic tools to problems on graphs and polytopes. After providing an overview of the thesis in Chapter 1, we begin our study in Chapter 2 by exploring the use of systems of polynomial equations to model computationally hard graph theoretic problems. We show how the algorithmic theory behind solving polynomial systems can be used to detect classical combinatorial properties: k-colorability in graphs, unique Hamiltonicity, and graphs having a trivial automorphism group. Our algebraic tools are diverse and include Nullstellensatz certificates, linear algebra over finite fields, Gröbner bases, toric algebra and real algebraic geometry. We also employ optimization tools, particularly linear and semidefinite programming.

In Chapter 3, we study the convex geometry of permutation polytopes, focusing on those associated to cyclic groups, dihedral groups, groups of automorphisms of tree graphs, and Frobenius groups. We find volumes by computing unimodular triangulations and Ehrhart polynomials. These are determined through the use of Gröbner basis techniques and Gale duality. We also find convex semidefinite approximations to these objects by exploring applications of the theta body hierarchy to these polytopes.

After establishing in earlier chapters that theta bodies play an interesting role in combinatorial analysis, in Chapter 4, we explore their foundational algebraic structure. In particular, we investigate extensions of the theta body hierarchy to ideals that are not necessarily real radical. In doing this, we introduce the notion of *strong nonnegativity* on real varieties. This algebraic condition is more restrictive than nonnegativity, but holds for sums of squares. We show that strong negativity is equivalent to nonnegativity for nonsingular real varieties. Moreover, for singular varieties, we reprove and generalize earlier results of Gouveia and Netzer regarding the obstructions to convergence of the theta body hierarchy.

Acknowledgments

I would like to begin by thanking my advisor Jesús De Loera for his dedication and energy in advising me. His patience, guidance and commitment are unmatchable and I thank him for all that he has given me through this journey. I also thank Brian Osserman for all that he has taught me, and his open invitations to learn many interesting aspects of algebraic geometry. I also thank the many professors who encouraged me in becoming a member of the algebraic optimization community, and their continued efforts in involving me in this community. Thank you Antoine Deza, Matthias Köppe, Monique Laurent, Shmuel Onn, Claus Scheiderer, Frank Sottile, Tamon Stephen, Bernd Sturmfels and Rekha Thomas for their encouragement in becoming a member of the algebraic optimization community, and their continued efforts in involving me in this community. Many thanks go to other professors at Davis and Waterloo whose conversations were very helpful throughout the process, including Eric Babson, Joseph Biello, Greg Kuperberg, Fu Liu, Bruce Richmond, Monica Vazirani, and Qinglan Xia. Along with these people, I thank the outstanding staff in the UC Davis Math Department who have helped tremendously throughout my experience; thanks Celia Davis, Tina Denena, and Perry Gee. Throughout my PhD experience, I was fortunate to have fruitful mathematical interactions with enthusiastic postdoctoral fellows, visitors and graduate students outside Davis: thank you Andrew Berget, Amitabh Basu, João Gouveia, Christopher Hillar, Steven Klee, Peter Malkin, and Cynthia Vinzant.

My friends were invaluable throughout my time as a PhD student, from enriching my life with a supportive community, to giving advice, and much more. I would like to thank all my friends at Davis, especially Deanna Needell, Matthew Stamps, and Rohit Thomas whose friendship and support were essential to my progression as a student and development as a mathematician. I would also like to thank my academic siblings, the older ones for their guidance, and all of them for their involvement with the thesis writing process. Thank you Brandon Dutra, David Haws, Mark Junod, Yvonne Kemper, Edward Kim, Susan Margulies, Tyrrell McAllister and Ruriko Yoshida.

I would like to thank my family. During my years as a PhD student we faced many challenges that we overcame together. Their support in my education throughout my life has gotten me where I am, and I will always be grateful.

Finally I thank the Natural Sciences and Research Council of Canada for their support in my educational endeavors.

CHAPTER 1

Introduction

In graph theory and combinatorial optimization, many problems cannot be approached directly because of issues of their complexity. Instead, computationally tractable relaxations are studied in hopes that such approximations will successfully solve many important instances. Typically, these approximations are easily modeled by systems of linear equations and inequalities, and efficient methods such as linear algebra and linear programming are employed. However, many of these linear models approximate combinatorial problems very coarsely, or do not capture enough of intrinsic combinatorial data. In this thesis, we investigate the use of *nonlinear polynomial* equations in approaching such problems. Our contributions are two-fold: we study the application of algebraic tools in these combinatorial settings, and further develop the algebraic machinery powering the tools themselves. On the application side, we focus particularly on specific examples of high interest in graph theory and combinatorial optimization, particularly arising from permutation groups. On the theory side, we further develop the algebraic theory behind the theta body hierarchy [**GPT10**] of convex bodies approximating the convex hull of a variety. Overall, we give evidence that the power of these higher order algebraic structures gives a deeper understanding of these combinatorics and optimization problems.

We begin in Chapter 2 by investigating the application of standard algebro-geometric techniques to fundamental issues graph theoretic. In his well-known survey [**Alo99**], Noga Alon used the term *polynomial method* to refer to the use of nonlinear polynomial equations when solving combinatorial problems. Although the polynomial method is not yet as widely used as linear algebra methods, an increasing number of researchers have used the algebra of multivariate polynomials to attack combinatorial questions (see for example [**AT92, DL95, DLLMM08, Eli92, Fis88, HL10, HW08, Lov94, LL81, Mat74, Mat01, Onn04, SVV94**] and references therein). Alon concluded his survey [**Alo99**] by asking whether the polynomial method could be used to yield efficient algorithms for solving combinatorial

problems. Based on joint work with Christopher Hillar, Jesús De Loera, and Peter Malkin, we explore this question further. We use polynomial equations and ideals to model three hard recognition problems in graph theory: vertex colorability, Hamiltonicity, and graph automorphism, and investigate the algorithmic consequences of these models.

In what follows, $G = (V, E)$ denotes an undirected simple graph on vertex set $V = \{1, \ldots, n\}$ and edges E. Similarly, $G = (V, A)$ denotes a *directed* graph G with arcs A. When G is undirected, we let

$$Arcs(G) = \{(i, j) : i, j \in V, \text{ and } \{i, j\} \in E\}$$

consist of all possible arcs in G. In Section 2.1, we explore k-colorability using techniques from commutative algebra and algebraic geometry. The following polynomial formulation of k-colorability is well-known [**Bay82**].

PROPOSITION 1.0.1. *Fix a positive integer k, and let $\mathbb{K}$ be a field with characteristic relatively prime to k. The polynomial system*

$$J_G = \{x_i^k - 1 = 0,\ x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1} = 0 :\ i \in V,\ \{i, j\} \in E\}$$

has a solution in $\overline{\mathbb{K}}$ (the algebraic closure of $\mathbb{K}$) if and only if the graph G is k-colorable.

REMARK 1.0.2. *Depending on the context, the fields $\mathbb{K}$ we use in this chapter will be the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$, or finite fields $\mathbb{F}_p$ with p a prime number.*

Hilbert's Nullstellensatz [**CLO07**, Theorem 2, Chapter 4] states that a system of polynomial equations $\{f_1(x) = 0, \ldots, f_r(x) = 0\}$, $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ for all i, with coefficients in $\mathbb{K}$, has no solution with entries in its algebraic closure $\overline{\mathbb{K}}$ if and only if

$$1 = \sum_{i=1}^{r} \beta_i f_i, \quad \text{for some polynomials } \beta_1, \ldots, \beta_r \in \mathbb{K}[x_1, \ldots, x_n].$$

If the system has no solution in $\overline{\mathbb{K}}$, we say $\beta_1, \beta_2, \ldots, \beta_r$ is a *Nullstellensatz certificate* that the associated combinatorial problem is infeasible. We can find a Nullstellensatz certificate $1 = \sum_{i=1}^{r} \beta_i f_i$ of a given degree $D := \max_{1 \le i \le r}\{\deg(\beta_i)\}$ or determine that no such certificate exists by solving a system of *linear equations* whose variables are the coefficients of the monomials used in $\beta_1, \ldots, \beta_r$ (see [**DLMP09**] and the many references therein).

The number of variables in this linear system is at most $\binom{n+D}{D}$, the number of monomials of degree at most D. Consequently, the linear system in the space of coefficients, which can be thought of as a D-th order linear relaxation of the polynomial system, can be solved in time that is polynomial in the input size for fixed degree D (see [**Mar08**, Theorem 4.1.3] or the survey [**DLMP09**]). The degree D of a Nullstellensatz certificate of an infeasible polynomial system cannot be more than known bounds [**Kol88**], and thus, by searching for certificates of increasing degrees, we obtain a finite (but potentially long) procedure to decide whether a system is feasible or not (this is the NulLA algorithm in [**Mar08, DLLMO09, DLLMM08**]). The philosophy of "linearizing" a system of arbitrary polynomials has also been applied in contexts outside combinatorics, including computer algebra [**Fau99, KK05, MT08, Ste04**], logic and complexity [**CEI96**], cryptography [**CKPS00**], and optimization [**LR05, Las02, Lau07, Par03, Par02, PS10**].

As the complexity of solving a combinatorial system with this strategy depends on its certificate degree, it is important to understand the class of problems having small degrees D. In Theorem 1.0.3, we give a combinatorial characterization of non-3-colorable graphs for which the encoding in Proposition 1.0.1 has a degree one Nullstellensatz certificate of infeasibility over $\mathbb{F}_2$. Our characterization involves two types of substructures on the graph G. The first of these are *oriented partial-3-cycles*, which are pairs of arcs $\{(i,j),(j,k)\} \subseteq Arcs(G)$, also denoted (i,j,k), in which $(k,i) \in Arcs(G)$ (the vertices i,j,k induce a 3-cycle in G). The second are *oriented chordless 4-cycles*, which are sets of four arcs $\{(i,j),(j,k),(k,l),(l,i)\} \subseteq Arcs(G)$, denoted (i,j,k,l), with $(i,k),(j,l) \notin Arcs(G)$ (the vertices i,j,k,l induce a chordless 4-cycle).

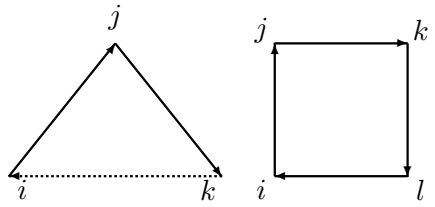

FIGURE 1.1. a partial 3-cycle and a chordless 4-cycle

THEOREM 1.0.3. *For a given simple undirected graph $G = (V, E)$, the polynomial system over $\mathbb{F}_2$ encoding the 3-colorability of G*

$$J_G = \{x_i^3 + 1 = 0,\ x_i^2 + x_i x_j + x_j^2 = 0 :\ i \in V,\ \{i, j\} \in E\}$$

has a degree one Nullstellensatz certificate of infeasibility if and only if there exists a set C of oriented partial 3-cycles and oriented chordless 4-cycles from $Arcs(G)$ such that

(1) $|C_{(i,j)}| + |C_{(j,i)}| \equiv 0 \pmod 2$ *for all* $\{i, j\} \in E$ *and*

(2) $\sum_{(i,j) \in Arcs(G), i<j} |C_{(i,j)}| \equiv 1 \pmod 2$,

where $C_{(i,j)}$ denotes the set of cycles in C in which the arc $(i, j) \in Arcs(G)$ appears. Moreover, the class of non-3-colorable graphs whose encodings have degree one Nullstellensatz infeasibility certificates can be recognized in polynomial time.

Theorem 1.0.3 essentially says that a graph has a degree one Nullsetellensatz certificate over $\mathbb{F}_2$ if there is an edge covering of the graph by three and four cycles obeying some parity conditions on the number of times an edge is covered. In particular, we can consider the set C in Theorem 1.0.3 as a covering of E by directed edges. From this perspective, Condition 1 in Theorem 1.0.3 means that every edge of G is covered by an even number of arcs from cycles in C. On the other hand, Condition 2 says that if $\hat{G}$ is the directed graph obtained from G by the orientation induced by the total ordering on the vertices $1 < 2 < \cdots < n$, then when summing the number of times each arc in $\hat{G}$ appears in the cycles of C, the total is odd. This result is reminiscent of the cycle double cover conjecture of Szekeres (1973) [**Sze73**] and Seymour (1979) [**Sey79**].

If a graph G has a non-3-colorable subgraph whose polynomial encoding has a degree one infeasibility certificate, we will show it is immediate that the encoding of G will also have a degree one infeasibility certificate. In this light, our work extends the work in [**Mar08, DLLMM08, DLMP09**] where it is shown that the class of non-3-colorable graphs with degree one certificates includes graphs with odd wheels as subgraphs.

COROLLARY 1.0.4. *If a graph $G = (V, E)$ has a subgraph that satisfies conditions (1) and (2) of Theorem 1.0.3, then the encoding of 3-colorability of G from Theorem 1.0.3 has a degree one Nullstellensatz certificate of infeasibility. In particular if G has an odd wheel as a subgraph, then it has a degree one Nullstellensatz certificate.*

In our second application of the polynomial method, we use tools from the theory of Gröbner bases to investigate (in Section 2.2) the detection of Hamiltonian cycles of a directed graph G. The following ideals algebraically encode Hamiltonian cycles (see Lemma 2.2.6 for a proof).

PROPOSITION 1.0.5. *Let $G = (V, A)$ be a simple directed graph on vertices $V = \{1, \ldots, n\}$. Assume that the characteristic of $\mathbb{K}$ is relatively prime to n and that $\omega \in \mathbb{K}$ is a primitive n-th root of unity. We let H_G be the ideal in $\mathbb{K}[x_1, \ldots, x_n]$ generated by the polynomials*

$$\left\{ x_i^n - 1, \prod_{j \in \delta^+(i)} (\omega x_i - x_j) : \ i \in V \right\}.$$

Here, $\delta^+(i)$ denotes those vertices j which are connected to i by an arc going from i to j in G. The variety of the ideal H_G is non-empty over $\overline{\mathbb{K}}$ if and only if G has a Hamiltonian cycle.

We prove a decomposition theorem for the ideal H_G, and based on this structure, we give an algebraic characterization of *uniquely Hamiltonian graphs*, those graphs that have a unique Hamiltonian cycle. This result is reminiscent of the one for k-colorability in [**HW08**]. Our results also provide an algorithm to decide this property. We first set up some necessary definitions.

For the purposes Section 2.2, all undirected graphs $G = (V, E)$ are presented as directed graphs with vertex set V and arcs $Arcs(G)$. When a directed graph G has the property that each pair of vertices connected by an arc is also connected by an arc in the opposite direction, then we call G *doubly covered*. Let C be a cycle of length $k > 2$ in a directed graph G, expressed as a sequence of arcs,

$$C = \{(v_1, v_2), (v_2, v_3), \ldots, (v_k, v_1)\}.$$

We call C a *doubly covered cycle* if consecutive vertices in the cycle are connected by arcs in both directions; otherwise, C is simply called *directed*. In particular, each cycle in a doubly covered graph is a doubly covered cycle. These definitions allow us to work with both undirected and directed graphs in the same framework.

DEFINITION 1.0.6. *[Cycle encodings] Let ω be a fixed primitive k-th root of unity and let $\mathbb{K}$ be a field with characteristic not dividing k. If C is a doubly covered cycle of length k and the vertices in C are $\{v_1, \ldots, v_k\}$, then the cycle encoding of C is the following set of k polynomials in $\mathbb{K}[x_{v_1}, \ldots, x_{v_k}]$:*

$$g_i = \begin{cases} x_{v_i} + \frac{(\omega^{2+i} - \omega^{2-i})}{(\omega^3 - \omega)} x_{v_{k-1}} + \frac{(\omega^{1-i} - \omega^{3+i})}{(\omega^3 - \omega)} x_{v_k} & i = 1, \ldots, k-2, \\ (x_{v_{k-1}} - \omega x_{v_k})(x_{v_{k-1}} - \omega^{-1} x_{v_k}) & i = k-1, \\ x_{v_k}^k - 1 & i = k. \end{cases} \tag{1.1}$$

If C is a directed cycle of length k in a directed graph, with vertex set $\{v_1, \ldots, v_k\}$, the cycle encoding of C is the following set of k polynomials:

$$g_i = \begin{cases} x_{v_{k-i}} - \omega^{k-i} x_{v_k} & i = 1, \ldots, k-1, \\ x_{v_k}^k - 1 & i = k. \end{cases} \tag{1.2}$$

DEFINITION 1.0.7. *[Cycle Ideals] The cycle ideal associated to a cycle C is $H_{G,C} = \langle g_1, \ldots, g_k \rangle \subseteq \mathbb{K}[x_{v_1}, \ldots, x_{v_k}]$, where the g_i's are the cycle encoding of C given by (1.1) or (1.2).*

Our main decomposition theorem is:

THEOREM 1.0.8. *Let G be a connected directed graph with n vertices. Then,*

$$H_G = \bigcap_C H_{G,C},$$

where C ranges over all Hamiltonian cycles of the graph G.

Because there are no containments among the ideals $\{H_{G,C} \mid C \text{ is a cycle in } G\}$, we have the following corollary:

COROLLARY 1.0.9. *The graph G is uniquely Hamiltonian if and only if the Hamiltonian ideal H_G is of the form $H_{G,C}$ for some length n cycle C.*

These developments give a computational framework in which to approach the famous conjecture of Sheehan (see [**She75**]) that states that no finite r-regular graph with $r \geq 3$ is uniquely Hamiltonian. We note that it is still an open question to decide the complexity

of finding a second Hamiltonian cycle knowing that it exists [**Cam01**]; our developments provide a framework to test this conjecture.

Finally, in Section 2.3 we explore the problem of determining the automorphisms $Aut(G)$ of an undirected graph G (we will assume G has n vertices throughout). Recall that the elements of $Aut(G)$ are those permutations of the vertices of G which preserve adjacency of vertices. Of particular interest for us is when graphs are *rigid*; that is, $|Aut(G)| = 1$. The complexity of this outstandingly famous decision problem is still wide open [**Cam04**]. As suggested by our theme, the combinatorial object $Aut(G)$ will be encoded as an algebraic variety, particularly the set of $n \times n$ permutation matrices representing the group $Aut(G)$. By this we mean that for each $g \in Aut(G)$, we identify g with the $n \times n$ matrix whose (i, j)-entry is 1 if $g(i) = j$, and 0 otherwise. We note that complementing our focus in Chapter 2, later in Chapter 3 we study the geometry *permutation polytopes*, convex hulls of such permutation matrices arising from general groups (see Definition 1.0.16).

Before presenting the equations defining the variety $Aut(G)$, we recall that for a simple graph G, its adjacency matrix A_G is the $n \times n$ matrix whose (i, j)-entry is 1 if ij is an edge in G, and 0 otherwise.

PROPOSITION 1.0.10. *Let G be a simple undirected graph and A_G its adjacency matrix. Then $Aut(G)$ is the group of permutation matrices $P = [P_{i,j}]_{i,j=1}^n$ given by the zeroes of the ideal $I_G \subseteq \mathbb{R}[x_1, \ldots, x_n]$ generated by the polynomials:*

$$\begin{aligned} &(PA_G - A_G P)_{i,j}, \;\; 1 \leq i, j \leq n; \quad \left(\sum_{i=1}^{n} P_{i,j}\right) - 1, \;\; 1 \leq j \leq n; \\ &\left(\sum_{j=1}^{n} P_{i,j}\right) - 1, \;\; 1 \leq i \leq n; \quad P_{i,j}^2 - P_{i,j}, \;\; 1 \leq i, j \leq n. \end{aligned} \tag{1.3}$$

PROOF. The last three sets of polynomials indicate that P is a permutation matrix, while the first one ensures that this permutation preserves adjacency of vertices ($PA_G P^\top = A_G$). □

From Proposition 1.0.10, $Aut(G)$ consists of the integer vertices of the polytope of doubly stochastic matrices commuting with A_G. By replacing the equations $P_{i,j}^2 - P_{i,j} = 0$ obtained from (1.3) with the linear inequalities $P_{ij} \geq 0$, we obtain a polyhedron P_G which is a convex relaxation of the automorphism group of the graph. Our first result is on the

structure of the vertex-edge graph induced by the integer points of P_G is *quasi-integral* (see Definition 7.1 in Chapter 4 of [**KKY84**]).

PROPOSITION 1.0.11. *The polytope P_G is quasi-integral. That is, the induced subgraph of the integer points of the 1-skeleton of P_G is connected.*

It follows that one can decide whether a graph G has trivial automorphism group by determining the vertex neighbors of the identity matrix in the 1-skeleton of P_G. Another application of this result is an output-sensitive algorithm for enumerating all automorphisms of a given graph [**AF96**].

Notice that if P_G is an integral polytope, then linear programming solves the automorphism problem for G in polynomial time, so understanding this polytope and its integer hull is crucial. Both have been investigated by Friedlander and Tinhofer [**Fri09, Tin86**], where they give sufficient conditions for guaranteeing P_G to be integral. Tinhofer coined the term *compact* for graphs G such that P_G is integral. For more on compact graphs, see [**CG97, Tin86**] and references therein. Unfortunately, it is well known that being compact is very restrictive. For instance, Godsil [**CG97**] shows that any regular compact graph is vertex transitive, which is a very strong restriction. Parallel to the work of Tinhofer, we examine a hierarchy of not necessarily polytopal convex bodies that approximate the integer hull of P_G, and give sufficient conditions for when iterations of this hierarchy equal the integer hull of P_G. The convex bodies in this hierarchy will play a pivotal role throughout this thesis: in Chapter 3, they are used to describe the facial structure of permutation polytopes; in Chapter 4, we further develop the algebraic theory governing this hierarchy. It is therefore essential that we introduce this hierarchy in a very general setting.

In the 1980's, L. Lovász approximated stable set polyhedra from graph theory using a convex body called the *theta body*; see [**Lov94**]. In [**GPT10**], the authors generalize Lovász's construction to generate a sequence of convex bodies that approximate the convex hull of the common zeroes of a set of real polynomials. To introduce this hierarchy, we need some preliminaries that will crucial to our entire exposition. All these can be found in [**GPT10**].

Let $I \subset \mathbb{R}[x_1, \ldots, x_n]$. We denote by $V_{\mathbb{R}}(I) \subseteq \mathbb{R}^n$, read the *real variety of* I, the set of common zeroes of polynomials in I. That is $V_{\mathbb{R}}(I) = \{x \in \mathbb{R}^n \mid f(x) = 0 \ \forall f \in I\}$.

Complementary to this, for any subset $S \subseteq \mathbb{R}^n$, we define $\mathcal{I}(S)$ to be the ideal of polynomials in $\mathbb{R}[x_1, \ldots, x_n]$ that vanish on S. That is, $\mathcal{I}(S) = \{f \in \mathbb{R}[x_1, \ldots, x_n] \mid f(x) = 0 \ \ \forall\, x \in S\}$. We say the ideal I is *real radical* if $I = \mathcal{I}(V_{\mathbb{R}}(I))$. A polynomial f is said to be *nonnegative* mod I (written $f \geq 0 \pmod{I}$) if $f(p) \geq 0$ for all $p \in V_{\mathbb{R}}(I)$. Similarly, a polynomial f is said to be a *sum of squares* mod I if there exist $h_1, \ldots, h_m \in \mathbb{R}[x_1, \ldots, x_n]$ such that $f - \sum_{i=1}^{m} h_i^2 \in I$. If the degrees of $h_1, \ldots, h_m$ are bounded by some positive integer k, we say f is *k-sos* mod I.

Now recall that our goal is to approximate the convex hull of a real variety by convex bodies that are efficiently computable. Classic convex theory tells us that the closure (with respect to the usual topology on $\mathbb{R}^n$) of the convex hull $conv(V_{\mathbb{R}}(I))$ can be described as the intersection of the half-spaces in which $V_{\mathbb{R}}(I)$ is contained (see [**Bar02**]). That is

$$\overline{conv(V_{\mathbb{R}}(I))} = \{x \in \mathbb{R}^n \mid f(x) \geq 0 \ \ \forall\, f \text{ nonnegative on } V_{\mathbb{R}}(I)\}.$$

One can now relax this condition by replacing nonnegativity of f on $V_{\mathbb{R}}(I)$ by f being a sum of squares modulo I, as this guarantees nonnegativity. Moreover, if we vary the maximum degree of the sums of squares representations of such f, we obtain convex bodies that by Corollary 2.9 and Corollary 2.15 of [**GPT10**] can be represented as projections of feasible regions of semidefinite programs (such regions are called *spectrahedra*) if I is real radical.

Definition 1.0.12. *The* k-th theta body *of an ideal* $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$*, denoted* $TH_k(I)$*, is the convex body*

$$TH_k(I) = \{x \in \mathbb{R}^n \mid f(x) \geq 0 \ \ \forall\, f \textit{ linear and } k\textit{-sos mod } I\}.$$

Notice that the theta bodies of I form a hierarchy

$$TH_1(I) \supseteq TH_2(I) \supseteq \cdots \supseteq \overline{conv(V_{\mathbb{R}}(I))}.$$

In the case that the hierarchy collapses at some k, i.e. $TH_k(I) = \overline{conv(V_{\mathbb{R}}(I))}$, we say I is *TH_k-exact*, or *k-exact*. We say a variety $S \subseteq \mathbb{R}^n$ is TH_k-exact (or k-exact) if its vanishing ideal $\mathcal{I}(S)$ is TH_k-exact. Moreover, if $P \subset \mathbb{R}^n$ is a polytope, we say P is TH_k-exact if its vertex set as a variety is TH_k-exact.

EXAMPLE 1.0.13. *Consider the ideal* $I = (x_1^2 x_2 - 1) \subset \mathbb{R}[x_1, x_2]$. *Then* $conv(V_{\mathbb{R}}(I))$ *is the open upper half-plane. Any linear polynomial that is non-negative over* $V_{\mathbb{R}}(I)$ *is of the form* $\alpha x_2 + \beta$ *where* $\alpha, \beta \geq 0$. *Now, mod* I, $\alpha x_2 + \beta \equiv (\sqrt{\alpha} x_1 x_2)^2 + (\sqrt{\beta})^2$, *and so every linear* f *non-negative on* $V_{\mathbb{R}}(I)$ *is* 2*-sos. We conclude* I *is* TH_2*-exact.*

Returning to our immediate goal, we would like to use theta bodies to approximate the convex hull of $Aut(G)$ for a group G. In order to do this, we must establish that the ideal I_G from Proposition 1.0.10 is indeed real radical. We prove an even stronger result.

LEMMA 1.0.14. *If* $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ *is an ideal such that* $V_{\mathbb{R}}(I) = V_{\mathbb{C}}(I)$, *and* $x_i^2 - x_i \in I$ *for each* i, *then* I *is real radical.*

PROOF. Let J be the ideal in $\mathbb{C}[x_1, \ldots, x_n]$ generated by the same polynomials that generate I, and $\sqrt[\mathbb{R}]{I}$ be the real radical of I. Since the polynomial $x_i^2 - x_i \in J$ for each $1 \leq i \leq n$, Lemma 2.1 of [**HW08**] implies $J = \sqrt{J}$ (where $\sqrt{J}$ is the radical of J). Together with the fact that $V_{\mathbb{C}}(J) = V_{\mathbb{R}}(I)$, this implies $J \supseteq \sqrt[\mathbb{R}]{I}$. Since $I = J \cap \mathbb{R}[x_1, \ldots, x_n]$, we conclude $I \supseteq \sqrt[\mathbb{R}]{I}$. The result follows since trivially, $I \subseteq \sqrt[\mathbb{R}]{I}$. □

From Lemma 1.0.14, we conclude that if I_G is k-exact, linear optimization over the automorphisms can be performed using semidefinite programming. In particular, one can use this to approach the graph automorphism problem. The caveat here is that one must first compute a basis for the quotient ring $\mathbb{R}[P_{11}, P_{12}, \ldots, P_{nn}]/I_G$ in order to set up these semidefinite programs (see Section 2 of [**GPT10**] for details). However, for k-exact ideals, one only needs those elements of the basis up to degree $2k$.

The favorable computational consequences of convergence of the theta body hierarchy motivates the need for characterizing those graphs G for which I_G is k-exact. We begin this study by focusing on those graphs G for which I_G is 1-exact. If this is the case we interchangeably use the terminology G or $P(G)$ is *exact* (which is consistent with the comment after Definition 1.0.12). Our main contribution in this direction is that even the coarsest iterate of the theta body hierarchy matches the integer hull of P_G (i.e. $conv(V_{\mathbb{R}}(I_G))$) better than P_G does. In particular, we prove that any compact graph is exact, and that these classes are not equal.

THEOREM 1.0.15. *The class of exact graphs strictly contains the class of compact graphs. More precisely:*

(1) *If G is a compact graph, then G is also exact.*

(2) *Let $G_1, \ldots, G_m$ be k-regular connected compact graphs, and let $G = \bigsqcup_{i=1}^{m} G_i$ be the graph that is the disjoint union of $G_1, \ldots, G_m$. Then G is always exact, but G may not be compact. Indeed, G is compact if and only if $G_i \cong G_j$ for all $1 \leq i, j \leq n$.*

Along with our computational interests in $Aut(G)$, the polytope $conv(Aut(G))$ has beautiful symmetric geometry. For instance, the group action of $Aut(G)$ on itself by left multiplication induces an automorphism of the polytope $conv(Aut(G))$, making it a highly symmetric polytope. In recent years, there has been much interest in understanding the geometry of polytopes arising from general permutation subgroups of S_n, not just those arising as automorphisms of graphs. These polytopes, called *permutation polytopes* have similar symmetry properties as $conv(Aut(G))$. Onn [**Onn93**] proved that they contain traveling salesman polytopes; see his paper along with [**BHNP09**] for references and history on these polytopes. In what follows, we identify the symmetric group S_n on $\{1, 2, \ldots, n\}$ through its representation by $n \times n$ permutation matrices; that is, for any $g \in S_n$, we identify g with the $n \times n$ matrix whose (i, j)-entry is one if $g(i) = j$ and 0 otherwise, and denote the identity by e throughout. We denote a subgroup G of S_n by $G \leq S_n$, and such a subgroup is called a *permutation group*.

DEFINITION 1.0.16. *Let $G \leq S_n$. The* permutation polytope $P(G)$ *is defined as $P(G) = conv\{g \mid g \in G\}$.*

EXAMPLE 1.0.17. *Let $G \leq S_4$ be the group consisting of the four permutations e, (1 2), (3 4), (1 2)(3 4). Then $P(G)$ is the convex hull of the matrices*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

This polytope is geometrically a square. Now let $H \leq S_4$ be the group consisting of the four permutations e, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3). Then $P(H)$ is the convex hull of the

matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

This polytope is geometrically a tetrahedron.

Note that Example 1.0.17 shows that the geometric structure of a permutation polytope depends on the group that defines it and not just its isomorphism class. Both of the examples above are groups isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, but their permutation polytopes are not even combinatorially isomorphic. The focus of Chapter 3, based on joint work with Katherine Burggraf and Jesús De Loera, is the geometric study of permutation polytopes. These polytopes appear everywhere in literature. Perhaps the key example of such a polytope is the *Birkhoff polytope* B_n, the convex hull of all $n \times n$ permutation matrices, whose combinatorial structure has been investigated by many researchers (see [**BP03, Bru88, BG77, CM09, CR99, DLLY09, DG95, Pak00, Stu96**]). Combinatorial properties of general permutation polytopes are established in [**BHNP09, BL91, GP06**], including edge structure and dimension. However, other properties such as facial structure and volumes are not known in general. This is difficult even for particular examples. For instance, a full facet description of the convex hull of all even permutation matrices is not known, nor is there a known efficient algorithm for testing membership in this polytope (see [**Bru88, CP10, CW04**]). Further, effective formulas for volumes, even for B_n, are not known in general, though there are asymptotic formulas (see [**CM09**]). We show through the application of various algebro-geometric tools that volumes and facial structure can be determined for many classes of permutation polytopes. For instance, we give a complete combinatorial and geometric description of permutation polytopes arising from cyclic and dihedral groups, including volumes and Ehrhart polytopes for each. This generalizes the work in [**Ste99**]. More generally, we determine the normalized volume of permutation polytopes arising from Frobenius groups and a method for determining the normalized volume of permutation polytopes arising from automorphism groups of binary trees. These

findings are all consequences of rich algebraic theories: Gröbner bases and Gale duality. Moreover, in all these cases, we show convergence of the first iterate of the theta body hierarchy, which gives us a semidefinite description of the polytopes, an important step toward understanding their facet structure.

Before stating our results, we will clarify some terminology. The *normalized volume* of a d-dimensional polytope $P \subset \mathbb{R}^n$ with respect to an affine lattice $L \subset \mathbb{R}^n$ is the volume form that assigns a volume of one to the smallest d-dimensional simplices in $\mathbb{R}^n$ whose vertices are in L. The *volume* of P is its normalized volume in the lattice $\text{aff}(P) \cap \mathbb{Z}^n$ where $\text{aff}(P)$ is the affine hull of P. The volume of an integer polytope $P \subset \mathbb{R}^n$ can be read off from the leading coefficient of its *Ehrhart polynomial*. This is the counting function $i_P(t)$ defined by $i_P(t) = |tP \cap \mathbb{Z}^n|$ where $tP = \{tx \mid x \in P\}$. The fact that $i_P(t)$ is a polynomial was proven by Eugene Ehrhart [**BR07**]. We say P is *unimodular* with respect to L if it has a triangulation whose simplices are all unimodular; that is, the vertices of any simplex in the triangulation span the lattice L. When P is unimodular with respect to $\text{aff}(P) \cap \mathbb{Z}^n$, its Ehrhart polynomial and hence its volume can be computed directly (see Lemma 3.1.1). For more details on triangulations with respect to particular lattices and Ehrhart polynomials, see Section 3.1.

To begin our study of permutation polytopes, we introduce our first two classes of groups. The *cyclic group* $C_n \leq S_n$ is the group generated by the permutation $(1\ 2\ \cdots\ n)$. The *dihedral group* $D_n \leq S_n$ is the group generated by the permutations $r = (1\ 2\ \cdots\ n)$ and $f = (1\ n)(2\ n-1)\cdots(\lfloor\frac{n+1}{2}\rfloor\ \lceil\frac{n+1}{2}\rceil)$. In Section 3.2, we determine particular unimodular triangulations of $P(C_n)$ and $P(D_n)$ with respect to the lattices $\text{aff}(P(C_n)) \cap \mathbb{Z}^{n\times n}$ and $\text{aff}(P(D_n)) \cap \mathbb{Z}^{n\times n}$ respectively. This allows us to recover their volumes via their Ehrhart polynomials.

THEOREM 1.0.18. *Let n be an integer, $n > 2$.*

(1) *The volume of $P(C_n)$ is $\frac{1}{(n-1)!}$. The Ehrhart polynomial of $P(C_n)$ is $\binom{t+n-1}{n-1}$.*

(2) *If n is odd, the volume of $P(D_n)$ is $\frac{n}{(2n-2)!}$. The Ehrhart polynomial of $P(D_n)$ is*

$$\sum_{k=0}^{n-2}\binom{2n}{k+1}\binom{t-1}{k} + \sum_{k=n-1}^{2n-2}\left(\binom{2n}{k+1} - \binom{n}{k-n+1}\right)\binom{t-1}{k}.$$

(3) *If n is even, $n = 2m$, the volume of $P(D_n)$ is $\frac{n^2}{4\cdot(2n-3)!}$. The Ehrhart polynomial of $P(D_n)$ is*

$$\sum_{k=0}^{m-2}\binom{2n}{k+1}\binom{t-1}{k} - \sum_{k=m-1}^{2m-2}\left(\binom{2n}{k+1} - 2\binom{2n-m}{k+1-m}\right)\binom{t-1}{k} + \sum_{k=2m-1}^{4m-3}\left(\binom{2n}{k+1} - 2\binom{2n-m}{k+1-m} + \binom{2n-2m}{k+1-2m}\right)\binom{t-1}{k}.$$

In Section 3.3, we study *Frobenius polytopes* as introduced by Collins and Perkinson in [**CP10**]. These are permutation polytopes $P(G)$ where G is a *Frobenius group*. A group $G \leq S_n$ is Frobenius if it has a proper subgroup H such that for all $x \in G\backslash H$, $H \cap (xHx^{-1}) = \{e\}$. The special subgroup H is known as the *Frobenius complement* of G and is unique up to conjugation. Moreover, every Frobenius group $G \leq S_n$ has a special proper subgroup N of size n called the *Frobenius kernel* which consists of the identity and all elements of G that have no fixed points; see Chapter 16 of [**AB95**]. The Frobenius kernel and Frobenius complement have trivial intersection, and $G = NH$. The class of Frobenius groups includes semi-direct products of cyclic groups, some matrix groups over finite fields, the alternating group A_4, and many others. See [**Wie64**] for more on Frobenius groups. We determine triangulations of Frobenius polytopes and a formula for their normalized volumes, in particular showing that the normalized volumes are completely characterized by the size of the Frobenius complement and the size of the Frobenius kernel.

THEOREM 1.0.19. *Let $G \leq S_n$ be a Frobenius group with Frobenius complement H and Frobenius kernel N. The normalized volume of $P(G)$ in the sublattice of $\mathbb{Z}^{n\times n}$ spanned by its vertices is*

$$\frac{1}{(|H||N|-|H|)!}\sum_{\ell=0}^{\lfloor\frac{|H|(|N|-1)-1}{|N|}\rfloor}\binom{(|H|-\ell)|N|}{(|H|-\ell)|N|-|H|+1}\binom{|H|-1}{\ell}(-1)^{\ell}.$$

We also study the theta body hierarchy applied to Frobenius polytopes. For instance, we prove that convergence of the first iterate always occurs for Frobenius groups. This implies many structural results, such as the existence of reverse lexicographic unimodular triangulations. See [**Sul06**] for more on this.

PROPOSITION 1.0.20. *If $G \leq S_n$ is a Frobenius group, then $P(G)$ is TH_1-exact.*

In Section 3.4, we develop a method for computing the Ehrhart polynomial of $P(G)$ when G is the automorphism group of a rooted binary tree on n vertices. This method relates the Ehrhart polynomials of permutation polytopes associated to direct products and wreath products of groups to the Ehrhart polynomials of the individual permutation polytopes themselves. A key theorem in this regard is the following:

THEOREM 1.0.21. *Let $G \leq S_n$, and $G \wr S_2$ be the wreath product of G with the symmetric group S_2. Then*

$$i(P(G \wr S_2), t) = \sum_{k=0}^{t} i^2(P(G), k) \cdot i^2(P(G), t-k)$$

for any integer $t \geq 2$.

In Appendix A.1, we comment on miscellaneous permutation polytopes. We begin by examining the permutation polytopes $P(A_n)$ where $A_n \leq S_n$ is the *alternating group* on $\{1, 2, \ldots, n\}$. One of the main focuses in the literature is on determining the facets of $P(A_n)$. Cunningham and Wang [**CW04**], and independently Hood and Perkinson [**HP04**], proved that $P(A_n)$ has exponentially many facets in n, resolving a problem of Brualdi and Liu [**BL91**]. However, a full facet description is still unknown. Moreover, no polynomial time algorithm in n is known for membership in $P(A_n)$. The difficulty of attaining a description of all facets of these polytopes is demonstrated by the following proposition, which states that the first iterate of the theta body hierarchy for the polytopes $P(A_n)$ is almost never equal to $P(A_n)$ itself.

PROPOSITION 1.0.22. *The polytope $P(A_n)$ is two-level, and hence A_n is TH_1-exact, if and only if $n \leq 4$. Moreover, for $n \geq 8$, $P(A_n)$ is at least $(\lfloor \frac{n}{4} \rfloor + 1)$-level.*

We conclude the appendix with computations of volumes and Ehrhart polynomials of permutation polytopes for many subgroups of S_3, S_4, and S_5.

Through Chapter 2, we see that theta bodies are very useful in determining computable relaxations of convex hulls of real varieties. Through Chapter 3, we see that theta bodies give polynomial inequality descriptions of various polytopes that do not necessarily have clear linear inequality descriptions. However, the theory of theta bodies relied on choosing a system of equations whose ideal is real radical. In the context of combinatorial optimization

problems, which are usually modeled by subsets of $\{0,1\}^n$ (this is the case for graph automorphism, as we saw in Proposition 1.0.10), we can represent the varieties as the zero sets of real radical ideals (see Lemma 1.0.14). However, for many purposes outside combinatorial optimization, it is may not be clear that a given presentation of an ideal guarantees it is real radical. This is an especially important issue that arises frequently in the emerging field of convex algebraic geometry, the study convex hulls of arbitrary real algebraic varieties (see [**GT11**] for more on this field). Since an ideal and its real radical have the same variety, one can take an arbitrary ideal and compute its real radical and use theta body theory to compute convex hulls. However, no algorithm is known to compute real radicals except for ideals whose varieties are finite (see [**LLR08**]). Motivated by this, in Chapter 4, based on joint work with Brian Osserman, we generalize the theta body hierarchy to intrinsically incorporate ideals that are not necessarily real radical. In fact, we do this by introducing a strict version of nonnegativity that is characterized algebraically, and is satisfied for sums of squares. As we shall see, this algebraic property has many interesting consequences to the theory of sums of squares relaxations of nonnegativity for singular and nonsingular varieties even outside the context of theta bodies. We begin with a motivating example. We use $V(I)$ in relation to concepts depending on the ring $\mathbb{R}[x_1,\ldots,x_n]/I$, which we will denote by A from now on. That is, $V(I)$ is the scheme $\mathrm{Spec}(A)$ (see Chapter 2 of [**Har77**] for more on schemes). All of our ring homomorphisms are assumed to be $\mathbb{R}$-algebra homomorphisms.

Example 1.0.23. *Suppose $I \subseteq \mathbb{R}[x]$ is the ideal generated by x^2. This ideal is clearly not real radical: $V_{\mathbb{R}}(I) = \{0\}$ and $\mathcal{I}(V_{\mathbb{R}}(I))$ is the ideal generated by x. The function x is nonnegative on $V_{\mathbb{R}}(I)$. However, x is not a sum of squares modulo I. Indeed, if $x = \sum_{i=1}^m f_i^2$, then reducing modulo I, the sum of the squares of the constant terms in each f_i must be 0. This implies the constant terms themselves are 0 and hence $\sum_{i=1}^m f_i^2 = 0$ modulo I.*

However, from a more scheme-theoretic perspective, we should think of $V(I)$ as not consisting only of the origin, but also including an infinitesimal thickening in both directions – in particular, in the negative direction. Thus, we should not think of x as being nonnegative on the scheme $V(I)$.

Example 1.0.23 tells us that for purposes of sums of squares relaxations, we should rule out nonnegative functions that are nonnegative on $V_{\mathbb{R}}(I)$ but not nonnegative on the scheme

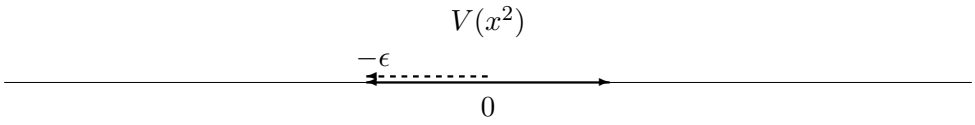

FIGURE 1.2. The scheme-theoretic picture for $V(x^2)$.

$V(I)$ in some sense. Recall that if $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ is an ideal, then the points of $V_{\mathbb{R}}(I)$ correspond precisely to ($\mathbb{R}$-algebra) homomorphisms $A \to \mathbb{R}$. The homomorphism obtained from a given $P \in V_{\mathbb{R}}(I)$ is simply given by evaluating polynomials at P. Thus, one may rephrase nonnegativity as saying that f is nonnegative if its image under any homomorphism $A \to \mathbb{R}$ is nonnegative. Our definition will consider a broader collection of such homomorphisms. In particular, given a point of $V_{\mathbb{R}}(I)$ corresponding to $\varphi : A \to \mathbb{R}$, it is standard that the (scheme-theoretic) tangent space to $V(I)$ at the point is in bijection with homomorphisms $A \to \mathbb{R}[\epsilon]/(\epsilon^2)$ which recover φ after composing with the unique homomorphism $\mathbb{R}[\epsilon]/(\epsilon^2) \to \mathbb{R}$, which necessarily sends ϵ to 0.

In Example 1.0.23, a tangent vector in the "negative direction" is given by the homomorphism $\mathbb{R}[x]/(x^2) \to \mathbb{R}[\epsilon]/(\epsilon^2)$ sending x to $-\epsilon$. If we consider $-\epsilon$ to be "negative", we may thus consider the function x to take a negative value on this tangent vector to $V(I)$. We formalize and generalize this idea by considering also higher-order infinitesimal arcs, as follows. We remark that $\mathbb{R}[\epsilon]/(\epsilon^m)$ has a unique homomorphism to $\mathbb{R}$, necessarily sending ϵ to 0. We say that $\varphi : A \to \mathbb{R}[\epsilon]/(\epsilon^m)$ is *at* P for (a necessarily unique) $P \in V_{\mathbb{R}}(I)$ if P is the point corresponding to the composed homomorphism $A \to \mathbb{R}$.

DEFINITION 1.0.24. *Given $f \in \mathbb{R}[\epsilon]/(\epsilon^n)$, $f = a_0 + a_1\epsilon + \cdots + a_{n-1}\epsilon^{n-1}$, we say f is* nonnegative *if $f = 0$, or $a_N > 0$ where $N = \min\{j \ : \ a_j \neq 0\}$.*

DEFINITION 1.0.25. *Let $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ be an ideal. Given $P \in V_{\mathbb{R}}(I)$, we say $f \in A$ is* strongly nonnegative *at P if for every $m \geq 0$ and for every $\mathbb{R}$-algebra homomorphism*

$$\varphi : A \to \mathbb{R}[\epsilon]/(\epsilon^m)$$

at P, we have $\varphi(f)$ is nonnegative in $\mathbb{R}[\epsilon]/(\epsilon^m)$ (in the sense of Definition 1.0.24). We say f is strongly nonnegative *on $V(I)$ if it is strongly nonnegative at P for all $P \in V_{\mathbb{R}}(I)$.*

We begin Chapter 4 by exploring basic properties of strong nonnegativity, showing in particular in Theorems 1.0.26 and 1.0.27 that strong nonnegativity at a point implies nonnegativity in a neighborhood of that point, and that the converse holds for nonsingular points.

THEOREM 1.0.26. *Given $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ and a point $P \in V_{\mathbb{R}}(I)$, suppose that $f \in A := \mathbb{R}[x_1, \ldots, x_n]/I$ is strongly nonnegative at P. Then f is nonnegative in a (real) neighborhood of P.*

THEOREM 1.0.27. *Given $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ and a point $P \in V_{\mathbb{R}}(I)$, suppose that P is a nonsingular point of $V(I)$, and that $f \in A := \mathbb{R}[x_1, \ldots, x_n]/I$ is nonnegative in a (real) neighborhood of P. Then f is strongly nonnegative at P.*

This implies the equivalence of strong nonnegativity and nonnegativity for nonsingular varieties. In the singular case, we study obstructions to the theta body hierarchy. In Theorem 4.3.8, we are able to recover the obstructions produced by Gouveia and Netzer in [**GN10**] to convergence of this hierarchy. The key is in generalizing their definition of convex-singularity.

DEFINITION 1.0.28. *A point $P \in V_{\mathbb{R}}(I)$ is* convex-singular *if it lies on the relative boundary of* $\operatorname{conv}(V_{\mathbb{R}}(I))$*, and the tangent space to the scheme $V(I)$ at P meets the relative interior of* $\operatorname{conv}(V_{\mathbb{R}}(I))$.

In [**GN10**], the tangent space is only defined set theoretically in terms of $V_{\mathbb{R}}(I)$, so our definition generalizes their construction. Our obstruction theorem is reminiscent of Theorem 4.5 in the same paper:

THEOREM 1.0.29. *Suppose we have $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$, and $P \in V_{\mathbb{R}}(I)$ is convex-singular. Then for every k, there is a linear function that is non-negative on I but not k-sos mod I.*

The together with Corollary 2.12 of [**GPT10**], this gives us a generalized version of the obstruction theorem of [**GN10**].

COROLLARY 1.0.30. *Let $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ be a real radical ideal. If there exists a linear function f that is nonnegative on $V_{\mathbb{R}}(I)$ but not strongly nonnegative, then I is not TH_k-exact for any k.* □

Finally, Proposition 1.0.32 and Corollary 1.0.33 show that our construction behaves well in the context of the foundational constructions of theta bodies. In particular, we introduce the concept of an ideal being *weakly* $(1,k)$-sos, meaning linear functions that are strongly nonnegative on $V(I)$ are k-sos mod I, and show this in itself implies the TH_k-exact property.

DEFINITION 1.0.31. *Given $k \geq 1$, and an ideal $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$, we say that I is* weakly $(1,k)$-sos *if for every linear $f \in \mathbb{R}[x_1, \ldots, x_n]$ which is strongly nonnegative on $V_{\mathbb{R}}(I)$, there exist $g_1, \ldots, g_m \in \mathbb{R}[x_1, \ldots, x_n]$ of degree at most k such that*

$$f \equiv \sum_{i=1}^{m} g_i^2 \pmod{I}.$$

An ideal being $(1,k)$-sos has an analogous definition (see Definition 4.3.1 in Chapter 4). We prove

PROPOSITION 1.0.32. *If I is weakly $(1,k)$-sos, then I is TH_k-exact.*

COROLLARY 1.0.33. *If $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ is a real radical ideal, then the following are equivalent:*

(1) *I is weakly $(1,k)$-sos*

(2) *I is $(1,k)$-sos*

(3) *I is TH_k-exact.*

We conclude the thesis in Chapter 5 with future directions and open questions based on our work. In particular, we propose problems in three fundamental areas. First, we ask how our constructions in Chapter 2 can be used to approach various well-known conjectures in graph theory computationally. Second, we propose extending the work in Chapter 3 by studying various symmetric polytopes akin to permutation polytopes, such as subpolytopes of permutohedra arising from group theoretic constructs. Finally, we propose extensions and open problems related to strong nonnegativity and sums of squares in the context of theta bodies, extending work in Chapter 4.

CHAPTER 2

Recognizing Graph Properties via Polynomial Ideals

2.1. Recognizing Non-3-colorable Graphs

In this section, we give a complete combinatorial characterization of the class of non-3-colorable simple undirected graphs $G = (V, E)$ with a degree one Nullstellensatz certificate of infeasibility for the following system (with $\mathbb{K} = \mathbb{F}_2$) from Proposition 1.0.1:

$$J_G = \{x_i^3 + 1 = 0,\ x_i^2 + x_i x_j + x_j^2 = 0 :\ i \in V,\ \{i,j\} \in E\}, \tag{2.1}$$

focusing on a proof of Theorem 1.0.3. Before proving this theorem, we give a detailed example.

EXAMPLE 2.1.1. *Consider the Grötzsch graph in Figure 2.1, which has no 3-cycles. The following set of oriented chordless 4-cycles gives a certificate of non-3-colorability by Theorem 1.0.3:*

$$C := \{(1,2,3,7),(2,3,4,8),(3,4,5,9),(4,5,1,10),(1,10,11,7),$$
$$(2,6,11,8),(3,7,11,9),(4,8,11,10),(5,9,11,6)\}.$$

Figure 2.1 illustrates the arc directions for the 4-cycles of C. Each edge of the graph is covered by exactly two 4-cycles, so C satisfies Condition 1 of Theorem 1.0.3. Moreover, one can check that Condition 2 is also satisfied. It follows that the graph has no proper 3-coloring. □

We now prove Theorem 1.0.3. Recall that the polynomial system (2.1) has a degree one ($D = 1$) Nullstellensatz certificate of infeasibility if and only if there exist coefficients $a_i, a_{ij}, b_{ij}, b_{ijk} \in \mathbb{F}_2$ such that

$$\sum_{i \in V}(a_i + \sum_{j \in V} a_{ij} x_j)(x_i^3 + 1) + \sum_{\{i,j\} \in E}(b_{ij} + \sum_{k \in V} b_{ijk} x_k)(x_i^2 + x_i x_j + x_j^2) = 1. \tag{2.2}$$

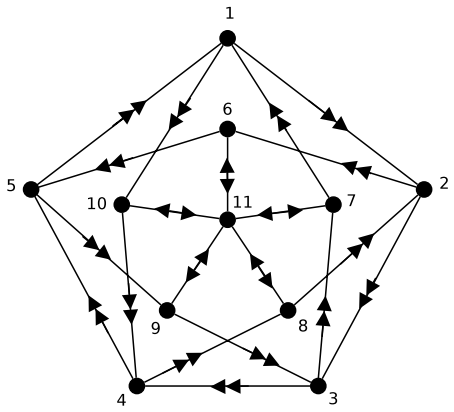

FIGURE 2.1. Grötzsch graph.

First, notice that we can simplify a degree one certificate as follows: Expanding the left-hand side of (2.2) and collecting terms, the only coefficient of $x_j x_i^3$ is a_{ij} and thus $a_{ij} = 0$ for all $i, j \in V$. Similarly, the only coefficient of $x_i x_j$ is b_{ij}, and so $b_{ij} = 0$ for all $\{i, j\} \in E$. We thus arrive at the following simplified expression:

$$\sum_{i \in V} a_i (x_i^3 + 1) + \sum_{\{i,j\} \in E} (\sum_{k \in V} b_{ijk} x_k)(x_i^2 + x_i x_j + x_j^2) = 1. \tag{2.3}$$

Now, consider the following set F of polynomials:

$$x_i^3 + 1 \qquad \forall i \in V, \tag{2.4}$$

$$x_k(x_i^2 + x_i x_j + x_j^2) \qquad \forall \{i, j\} \in E,\ k \in V. \tag{2.5}$$

The elements of F are those polynomials that can appear in a degree one certificate of infeasibility. Thus, there exists a degree one certificate if and only if the constant polynomial 1 is in the linear span of F; that is, $1 \in \langle F \rangle_{\mathbb{F}_2}$, where $\langle F \rangle_{\mathbb{F}_2}$ is the vector space over $\mathbb{F}_2$ generated by the polynomials in F.

We next simplify the set F. Let H be the following set of polynomials:

(2.6)
$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \forall \{i,j\} \in E,$$

(2.7)
$$x_i x_j^2 + x_j x_k^2 \qquad \forall (i,j),(j,k),(k,i) \in Arcs(G),$$

(2.8)
$$x_i x_j^2 + x_j x_k^2 + x_k x_l^2 + x_l x_i^2 \quad \forall (i,j),(j,k),(k,l),(l,i) \in Arcs(G),(i,k),(j,l) \notin Arcs(G).$$

If we identify the monomials $x_i x_j^2$ as the arcs (i,j), then the polynomials (2.7) correspond to oriented partial 3-cycles and the polynomials (2.8) correspond to oriented chordless 4-cycles. The following lemma says that we can use H instead of F to find a degree one certificate.

LEMMA 2.1.2. *We have* $1 \in \langle F \rangle_{\mathbb{F}_2}$ *if and only if* $1 \in \langle H \rangle_{\mathbb{F}_2}$.

PROOF. The polynomials (2.5) above can be split into two classes of equations: (i) $k = i$ or $k = j$ and (ii) $k \neq i$ and $k \neq j$. Thus, the set F consists of

(2.9) $\quad x_i^3 + 1 \qquad \forall i \in V,$

(2.10) $\quad x_i(x_i^2 + x_i x_j + x_j^2) = x_i^3 + x_i^2 x_j + x_i x_j^2 \qquad \forall \{i,j\} \in E,$

(2.11) $\quad x_k(x_i^2 + x_i x_j + x_j^2) = x_i^2 x_k + x_i x_j x_k + x_j^2 x_k \qquad \forall \{i,j\} \in E,\ k \in V, i \neq k \neq j.$

Using polynomials (2.9) to eliminate the x_i^3 terms from (2.10), we arrive at the following set of polynomials, which we label F':

(2.12)
$$x_i^3 + 1 \qquad \forall i \in V,$$

(2.13)
$$x_i^2 x_j + x_i x_j^2 + 1 = (x_i^3 + x_i^2 x_j + x_i x_j^2) + (x_i^3 + 1) \qquad \forall \{i,j\} \in E,$$

(2.14)
$$x_i^2 x_k + x_i x_j x_k + x_j^2 x_k \qquad \forall \{i,j\} \in E,\ k \in V, i \neq k \neq j.$$

Observe that $\langle F \rangle_{\mathbb{F}_2} = \langle F' \rangle_{\mathbb{F}_2}$. We can eliminate the polynomials (2.12) as follows. For every $i \in V$, $(x_i^3 + 1)$ is the only polynomial in F' containing the monomial x_i^3 and thus the

polynomial (x_i^3+1) cannot be present in any nonzero linear combination of the polynomials in F' that equals 1. We arrive at the following smaller set of polynomials, which we label F''.

$$x_i^2x_j + x_ix_j^2 + 1 \qquad \forall\{i,j\} \in E, \tag{2.15}$$

$$x_i^2x_k + x_ix_jx_k + x_j^2x_k \qquad \forall\{i,j\} \in E, k \in V, i \neq k \neq j. \tag{2.16}$$

So far, we have shown $1 \in \langle F\rangle_{\mathbb{F}_2} = \langle F'\rangle_{\mathbb{F}_2}$ if and only if $1 \in \langle F''\rangle_{\mathbb{F}_2}$.

Next, we eliminate monomials of the form $x_ix_jx_k$. There are 3 cases to consider.

Case 1: $\{i,j\} \in E$ but $\{i,k\} \notin E$ and $\{j,k\} \notin E$. In this case, the monomial $x_ix_jx_k$ appears in only one polynomial, $x_k(x_i^2 + x_ix_j + x_j^2) = x_i^2x_k + x_ix_jx_k + x_j^2x_k$, so we can eliminate all such polynomials.

Case 2: $(i,j),(j,k),(k,i) \in Arcs(G)$. Graphically, this represents a 3-cycle in the graph. In this case, the monomial $x_ix_jx_k$ appears in three polynomials:

$$x_k(x_i^2 + x_ix_j + x_j^2) = x_i^2x_k + x_ix_jx_k + x_j^2x_k, \tag{2.17}$$

$$x_j(x_i^2 + x_ix_k + x_k^2) = x_i^2x_j + x_ix_jx_k + x_jx_k^2, \tag{2.18}$$

$$x_i(x_j^2 + x_jx_k + x_k^2) = x_ix_j^2 + x_ix_jx_k + x_ix_k^2. \tag{2.19}$$

Using the first polynomial, we can eliminate $x_ix_jx_k$ from the other two:

$$x_i^2x_j + x_jx_k^2 + x_i^2x_k + x_j^2x_k = (x_i^2x_j + x_ix_jx_k + x_jx_k^2) + (x_i^2x_k + x_ix_jx_k + x_j^2x_k),$$

$$x_ix_j^2 + x_ix_k^2 + x_i^2x_k + x_j^2x_k = (x_ix_j^2 + x_ix_jx_k + x_ix_k^2) + (x_i^2x_k + x_ix_jx_k + x_j^2x_k).$$

We can now eliminate the polynomial (2.17). Moreover, we can use the polynomials from (2.15) to rewrite the above two polynomials as follows.

$$x_kx_i^2 + x_ix_j^2 = (x_i^2x_j + x_jx_k^2 + x_i^2x_k + x_j^2x_k) + (x_jx_k^2 + x_j^2x_k + 1) + (x_ix_j^2 + x_i^2x_j + 1),$$

$$x_ix_j^2 + x_jx_k^2 = (x_ix_j^2 + x_ix_k^2 + x_i^2x_k + x_j^2x_k) + (x_ix_k^2 + x_i^2x_k + 1) + (x_jx_k^2 + x_j^2x_k + 1).$$

Note that both of these polynomials correspond to two of the arcs of the 3-cycle (i,j), (j,k),$(k,i) \in Arcs(G)$.

Case 3: $i, j, k \in V$, $(i, j), (j, k) \in Arcs(G)$ and $(k, i) \notin Arcs(G)$. We have

$$x_k(x_i^2 + x_i x_j + x_j^2) = x_i^2 x_k + x_i x_j x_k + x_j^2 x_k, \tag{2.20}$$

$$x_i(x_j^2 + x_j x_k + x_k^2) = x_i x_j^2 + x_i x_j x_k + x_i x_k^2. \tag{2.21}$$

As before we use the first polynomial to eliminate the monomial $x_i x_j x_k$ from the second:

$$x_i x_j^2 + x_j x_k^2 + (x_i^2 x_k + x_i x_k^2 + 1) = (x_i x_j^2 + x_i x_j x_k + x_i x_k^2) + (x_i^2 x_k + x_i x_j x_k + x_j^2 x_k) + (x_j x_k^2 + x_j^2 x_k + 1).$$

We can now eliminate (2.20); thus, the original system has been reduced to the following one, which we label as F''':

$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \forall \{i, j\} \in E, \tag{2.22}$$

$$x_i x_j^2 + x_j x_k^2 \qquad \forall (i, j), (i, k), (j, k) \in Arcs(G), \tag{2.23}$$

$$x_i x_j^2 + x_j x_k^2 + (x_i^2 x_k + x_i x_k^2 + 1) \qquad \forall (i, j), (j, k) \in Arcs(G), (k, i) \notin Arcs(G). \tag{2.24}$$

Note that $1 \in \langle F \rangle_{\mathbb{F}_2}$ if and only if $1 \in \langle F''' \rangle_{\mathbb{F}_2}$.

The monomials $x_i^2 x_k$ and $x_i x_k^2$ with $(k, i) \notin Arcs(G)$ always appear together and only in the polynomials (2.24) in the expression $(x_i^2 x_k + x_i x_k^2 + 1)$. Thus, we can eliminate the monomials $x_i^2 x_k$ and $x_i x_k^2$ with $(k, i) \notin Arcs(G)$ by choosing one of the polynomials (2.24) and using it to eliminate the expression $(x_i^2 x_k + x_i x_k^2 + 1)$ from all other polynomials in which it appears. Let $i, j, k, l \in V$ be such that $(i, j), (j, k), (k, l), (l, i) \in Arcs(G)$ and $(k, i), (i, k) \notin Arcs(G)$. We can then eliminate the monomials $x_i^2 x_k$ and $x_i x_k^2$ as follows:

$$x_i x_j^2 + x_j x_k^2 + x_k x_l^2 + x_l x_i^2 = (x_i x_j^2 + x_j x_k^2 + x_i^2 x_k + x_i x_k^2 + 1) + (x_k x_l^2 + x_l x_i^2 + x_i^2 x_k + x_i x_k^2 + 1).$$

Finally, after eliminating the polynomials (2.24), we have system H (polynomials (2.6), (2.7), and (2.8)):

$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \forall \{i,j\} \in E,$$

$$x_i x_j^2 + x_j x_k^2 \qquad \forall (i,j),(j,k),(k,i) \in Arcs(G),$$

$$x_i x_j^2 + x_j x_k^2 + x_k x_l^2 + x_l x_i^2 \qquad \forall (i,j),(j,k),(k,l),(l,i) \in Arcs(G), (i,k),(j,l) \notin Arcs(G).$$

The system H has the property that $1 \in \langle F''' \rangle_{\mathbb{F}_2}$ if and only if $1 \in \langle H \rangle_{\mathbb{F}_2}$, and thus, $1 \in \langle F \rangle_{\mathbb{F}_2}$ if and only if $1 \in \langle H \rangle_{\mathbb{F}_2}$ as required □

We now establish that the sufficient condition for infeasibility $1 \in \langle H \rangle_{\mathbb{F}_2}$ is equivalent to the combinatorial parity conditions in Theorem 1.0.3.

LEMMA 2.1.3. *There exists a set C of oriented partial 3-cycles and oriented chordless 4-cycles satisfying Conditions 1. and 2. of Theorem 1.0.3 if and only if* $1 \in \langle H \rangle_{\mathbb{F}_2}$.

PROOF. Assume that $1 \in \langle H \rangle_{\mathbb{F}_2}$. Then there exist coefficients $c_h \in \mathbb{F}_2$ such that $\sum_{h \in H} c_h h = 1$. Let $H' := \{h \in H : c_h = 1\}$; then, $\sum_{h \in H'} h = 1$. Let C be the set of oriented partial 3-cycles (i,j,k) where $x_i x_j^2 + x_j x_k^2 \in H'$ together with the set of oriented chordless 4-cycles (i,j,l,k) where $x_i x_j^2 + x_j x_l^2 + x_l x_k^2 + x_k x_i^2 \in H'$. Now, $|C_{(i,j)}|$ is the number of polynomials in H' of the form (2.7) or (2.8) in which the monomial $x_i x_j^2$ appears, and similarly, $|C_{(j,i)}|$ is the number of polynomials in H' of the form (2.7) or (2.8) in which the monomial $x_j x_i^2$ appears. Thus, $\sum_{h \in H'} h = 1$ implies that, for every pair $x_i x_j^2$ and $x_j x_i^2$, either

(1) $|C_{(i,j)}| \equiv 0 \pmod 2$, $|C_{(j,i)}| \equiv 0 \pmod 2$, and $x_i^2 x_j + x_i x_j^2 + 1 \notin H'$ or

(2) $|C_{(i,j)}| \equiv 1 \pmod 2$, $|C_{(j,i)}| \equiv 1 \pmod 2$, and $x_i^2 x_j + x_i x_j^2 + 1 \in H'$.

In either case, we have $|C_{(i,j)}| + |C_{(j,i)}| \equiv 0 \pmod 2$. Moreover, since $\sum_{h \in H'} h = 1$, there must be an odd number of the polynomials of the form $x_i^2 x_j + x_i x_j^2 + 1$ in H'. That is, case 2 above occurs an odd number of times and therefore, $\sum_{(i,j) \in Arcs(G), i<j} |C_{(i,j)}| \equiv 1 \pmod 2$ as required.

Conversely, assume that there exists a set C of oriented partial 3-cycles and oriented chordless 4-cycles satisfying the conditions of Theorem 1.0.3. Let H' be the set of polynomials $x_i x_j^2 + x_j x_k^2$ where $(i,j,k) \in C$ and the set of polynomials $x_i x_j^2 + x_j x_l^2 + x_l x_k^2 + x_k x_i^2$ where

$(i, j, l, k) \in C$ together with the set of polynomials $x_i^2 x_j + x_i x_j^2 + 1 \in H$ where $|C_{(i,j)}| \equiv 1$. Then, $|C_{(i,j)}| + |C_{(j,i)}| \equiv 0 \pmod 2$ implies that every monomial $x_i x_j^2$ appears in an even number polynomials of H'. Moreover, since $\sum_{(i,j)\in Arcs(G), i<j} |C_{(i,j)}| \equiv 1 \pmod 2$, there are an odd number of polynomials $x_i^2 x_j + x_i x_j^2 + 1$ appearing in H'. Hence, $\sum_{h\in H'} h = 1$ and $1 \in \langle H \rangle_{\mathbb{F}_2}$. □

Combining Lemmas 2.1.2 and 2.1.3, we arrive at the characterization stated in Theorem 1.0.3. That such graphs can be decided in polynomial time follows from the fact that the existence of a certificate of any fixed degree can be decided in polynomial time (as is well known and follows since there are polynomially many monomials up to any fixed degree; see also [**Mar08**, Theorem 4.1.3]). We now prove Corollary 1.0.4, establishing in particular that our combinatorial characterization indeed detects odd wheels.

Proof of Corollary 1.0.4. It is clear that if a subgraph of a graph has a degree 1 Nullstellensatz certificate, which is equivalent satisfying the conditions in Theorem 1.0.3, then the graph itself has such a certificate. Thus, it remains to show odd wheels (or graphs containing odd wheels as subgraphs) satisify the conditions in Theorem 1.0.3. Assume G contains an odd wheel with vertices labelled as in Figure 2.1 below. Let

$$C := \{(i, 1, i+1) : 2 \le i \le n-1\} \cup \{(n, 1, 2)\}.$$

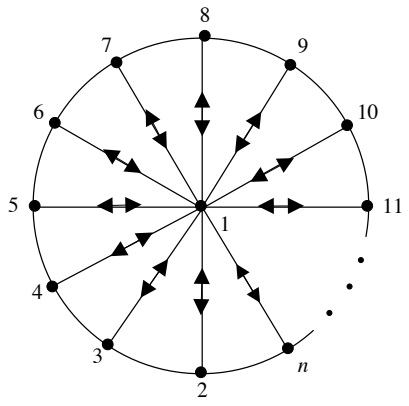

Figure 2.2. Odd wheel

Figure 2.1 illustrates the arc directions for the oriented partial 3-cycles of C. Each edge of G is covered by exactly zero or two partial 3-cycles, so C satisfies Condition 1 of Theorem

1.0.3. Furthermore, each arc $(1, i) \in Arcs(G)$ is covered exactly once by a partial 3-cycle in C, and there is an odd number of such arcs. Thus, C also satisfies Condition 2 of Theorem 1.0.3. □

2.2. Recognizing Uniquely Hamiltonian Graphs

Throughout this section we work over an arbitrary algebraically closed field $\mathbb{K} = \overline{\mathbb{K}}$, although in some cases, we will need to restrict its characteristic. Recall that H_G, which we will call the *Hamiltonian ideal* of G, is generated by the polynomials from Proposition 1.0.5. A connected, directed graph G with n vertices has a Hamiltonian cycle if and only if the equations defined by H_G have a solution over $\mathbb{K}$ (or, in other words, if and only if $V(H_G) \neq \emptyset$ for the algebraic variety $V(H_G)$ associated to the ideal H_G). In a precise sense to be made clear below, the ideal H_G actually encodes *all* Hamiltonian cycles of G. However, we need to be somewhat careful about how to count cycles (see Lemma 2.2.6). In practice ω can be treated as a variable and not as a fixed primitive n-th root of unity. A set of equations ensuring that ω only takes on the value of a *primitive* n-th root of unity is the following:

$$\{\omega^{i(n-1)} + \omega^{i(n-2)} + \cdots + \omega^i + 1 = 0 : \ 1 \leq i \leq n\}.$$

We can also use the cyclotomic polynomial $\Phi_n(\omega)$ [**DF04**], which is the polynomial whose zeroes are the primitive n-th roots of unity.

We shall utilize the theory of Gröbner bases to show that H_G has a special (algebraic) decomposition structure in terms of the different Hamiltonian cycles of G (this is Theorem 1.0.8). We first turn our attention to cycle ideals $H_{G,C}$ (see Definition 1.0.7) of a simple directed graph G. These will be the basic elements in our decomposition of the Hamiltonian ideal H_G, as they algebraically encode single cycles C (up to symmetry).

LEMMA 2.2.1. *Let G be a graph with vertex set $\{v_1, v_2, \ldots, v_k\}$. The cycle encoding polynomials $F = \{g_1, \ldots, g_k\}$ (see Definition 1.0.6) are a reduced Gröbner basis for the cycle ideal $H_{G,C}$ with respect to any term order $\prec$ with $x_{v_k} \prec \cdots \prec x_{v_1}$.*

PROOF. Since the leading monomials in a cycle encoding:

$$\{x_{v_1}, \ldots, x_{v_{k-2}}, x_{v_{k-1}}^2, x_{v_k}^k\} \text{ or } \{x_{v_1}, \ldots, x_{v_{k-2}}, x_{v_{k-1}}, x_{v_k}^k\} \tag{2.25}$$

are relatively prime, the polynomials g_i form a Gröbner basis for $H_{G,C}$ (see Theorem 3 and Proposition 4 in [**CLO07**, Section 2]). That F is reduced follows from inspection of (1.1) and (1.2). □

REMARK 2.2.2. *In particular, since reduced Gröbner bases (with respect to a fixed term order) are unique, it follows that cycle encodings are canonical ways of generating cycle ideals (and thus of representing cycles by Lemma 2.2.4).*

Having explicit Gröbner bases for these ideals allows us to compute their Hilbert series easily.

COROLLARY 2.2.3. *The Hilbert series of* $\mathbb{K}[x_{v_1}, \ldots, x_{v_k}]/H_{G,C}$ *for a doubly covered cycle or a directed cycle is equal to (respectively)*

$$\frac{(1-t^2)(1-t^k)}{(1-t)^2} \text{ or } \frac{(1-t^k)}{(1-t)}.$$

PROOF. If $\prec$ is a graded term order, then the (affine) Hilbert function of an ideal and of its ideal of leading terms are the same [**CLO07**, Chapter 9, §3]. The form of the Hilbert series is now immediate from (2.25). □

The naming of these ideals is motivated by the following result; in words, it says that the cycle C is encoded as a complete intersection by the ideal $H_{G,C}$.

LEMMA 2.2.4. *The following hold for the ideal* $H_{G,C}$.

(1) $H_{G,C}$ *is radical,*
(2) $|V_{\mathbb{K}}(H_{G,C})| = k$ *if* C *is directed, and* $|V_{\mathbb{K}}(H_{G,C})| = 2k$ *if* C *is doubly covered undirected.*

PROOF. Without loss of generality, we suppose that $v_i = i$ for $i = 1, \ldots, k$. Let $\prec$ be any term order in which $x_k \prec \cdots \prec x_1$. From Lemma 2.2.1, the set of g_i form a Gröbner basis for $H_{G,C}$. It follows that the number of standard monomials of $H_{G,C}$ is $2k$ if C is doubly covered undirected (resp. k if it is directed). Therefore by [**HW08**, Lemma 2.1], if we can prove that $|V_{\mathbb{K}}(H_{G,C})| \geq k$ (resp. $|V_{\mathbb{K}}(H_{G,C})| \geq 2k$), then both statements 1. and 2. follow.

When C is directed, this follows easily from the form of (1.2), so we shall assume that C is doubly covered undirected. We claim that the k cyclic permutations of the two points:

$$(\omega, \omega^2, \ldots, \omega^k), (\omega^k, \omega^{k-1}, \ldots, \omega)$$

are zeroes of g_i, $i = 1, \ldots, k$. Since cyclic permutation is multiplication by a power of ω, it is clear that we need only verify this claim for the two points above. In the fist case, when $x_i = \omega^i$, we compute that for $i = 1, \ldots, k-2$:

$$\begin{aligned}(\omega^3 - \omega)g_i(\omega, \ldots, \omega^k) &= (\omega^3 - \omega)\omega^i + (\omega^{2+i} - \omega^{2-i})\omega^{k-1} + (\omega^{1-i} - \omega^{3+i})\omega^k \\ &= \omega^{3+i} - \omega^{1+i} + \omega^{1+i+k} - \omega^{1-i+k} + \omega^{1-i+k} - \omega^{3+i+k} \\ &= 0,\end{aligned}$$

since $\omega^k = 1$. In the second case, when $x_i = \omega^{1-i}$, we again compute that for $i = 1, \ldots, k-2$:

$$\begin{aligned}(\omega^3 - \omega)g_i(\omega^k, \ldots, \omega) &= (\omega^3 - \omega)\omega^{1-i} + (\omega^{2+i} - \omega^{2-i})\omega^2 + (\omega^{1-i} - \omega^{3+i})\omega \\ &= \omega^{4-i} - \omega^{2-i} + \omega^{4+i} - \omega^{4-i} + \omega^{2-i} - \omega^{4+i} \\ &= 0.\end{aligned}$$

Finally, it is obvious that the two points zero g_{k-1} and g_k, and this completes the proof. □

REMARK 2.2.5. *Conversely, it is easy to see that points in $V_{\mathbb{K}}(H_{G,C})$ correspond to cycles of length k in G. That this variety contains k or $2k$ points corresponds to there being k or $2k$ ways of writing down the cycle since we may cyclically permute it and also reverse its orientation (if each arc in the path is bidirectional).*

Before proving Theorem 1.0.8, we need to explain how the Hamiltonian ideal encodes all Hamiltonian cycles of the graph G.

LEMMA 2.2.6. *Let G be a connected directed graph on n vertices. Then,*

$$V_{\mathbb{K}}(H_G) = \bigcup_C V_{\mathbb{K}}(H_{G,C}),$$

where the union is over all Hamiltonian cycles C in G.

PROOF. We only need to verify that points in $V_{\mathbb{K}}(H_G)$ correspond to cycles of length n. Suppose there exists a Hamiltonian cycle in the graph G. Label vertex 1 in the cycle

with the number $x_1 = \omega^0 = 1$ and then successively label vertices along the cycle with one higher power of ω. It is clear that these labels x_i associated to vertices i zero all of the equations generating H_G.

Conversely, let $\mathbf{v} = (x_1, \ldots, x_n)$ be a point in the variety $V_{\mathbb{K}}(H_G)$ associated to H_G; we claim that $\mathbf{v}$ encodes a Hamiltonian cycle. From the edge equations, each vertex must be adjacent to one labeled with the next highest power of ω. Fixing a starting vertex i, it follows that there is a cycle C labeled with (consecutively) increasing powers of ω. Since ω is a primitive n-th root of unity, this cycle must have length n, and thus is Hamiltonian. We prove that elements of $V_{\mathbb{K}}(H_G)$ are in n to 1 correspondence with Hamiltonian cycles of G. Suppose C is a Hamiltonian cycle in G. Label vertex 1 in the cycle with the number $x_1 = \omega^i$ for any $i \in [n]$, and then successively label vertices along the cycle with one higher power of ω. It is clear that these labels x_i associated to vertices i zero all of the equations generating H_G. Conversely, let $\mathbf{v} = (x_1, \ldots, x_n)$ be a point in the variety $V_{\mathbb{K}}(H_G)$ associated to H_G; we claim that each point $(\omega^i x_1, \ldots, \omega^i x_n)$, with $i \in [n]$, encodes the same Hamiltonian cycle. First $\mathbf{v}$ itself encodes a Hamiltonian cycle. From the edge equations, each vertex must be adjacent to one labeled with the next highest power of ω. Fixing a starting vertex j, it follows that there is a cycle C labeled with (consecutively) increasing powers of ω. Since ω is a primitive n-th root of unity, this cycle must have length n, and thus is Hamiltonian. That $(\omega^i x_1, \ldots, \omega^i x_n)$, with $i \in [n]$ all encode the same cycle C follows from our arbitrary choice of the starting vertex j. The proof of this lemma then follows from the n to 1 correspondence between $V_{\mathbb{K}}(H_G)$ and Hamiltonian cycles of G, together with the definition of $H_{G,C}$ and Lemma 2.2.4. □

Proof of Theorem 1.0.8. Since H_G contains a square-free univariate polynomial in each indeterminate, it is radical (see for instance [**HW08**, Lemma 2.1]). It follows that

$$\begin{aligned} H_G &= I(V_{\mathbb{K}}(H_G)) \\ &= \mathcal{I}\left(\bigcup_C V_{\mathbb{K}}(H_{G,C})\right) \\ &= \bigcap_C \mathcal{I}(V_{\mathbb{K}}(H_{G,C})) \\ &= \bigcap_C H_{G,C}, \end{aligned} \tag{2.26}$$

where the second equality comes from Lemma 2.2.6 and the last one from $H_{G,C}$ being a radical ideal (Lemma 2.2.4). □

Theorem 1.0.8 immediately gives Corollary 1.0.9 which inherently provides an algorithm to check whether a graph is uniquely Hamiltonian. We simply compute a unique reduced Gröbner basis of H_G and then check that it has the same form as that of an ideal $H_{G,C}$. Another approach is to count the number of standard monomials of any Gröbner basis for H_G and compare with n or $2n$ (since H_G is radical). We remark, however, that it is well-known that computing a Gröbner basis in general cannot be done in polynomial time [**Yap00**, p. 400]. We close this section with a directed and an undirected example of Theorem 1.0.8.

EXAMPLE 2.2.7. *Let G be the directed graph with vertex set $V = \{1, 2, 3, 4, 5\}$ and arcs $A = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 1), (1, 3), (1, 4)\}$. Moreover, let ω be a primitive 5-th root of unity. The ideal $H_G \subset \mathbb{K}[x_1, x_2, x_3, x_4, x_5]$ is generated by the polynomials*

$$\{x_i^5 - 1 : 1 \leq i \leq 5\} \cup \{(\omega x_1 - x_2)(\omega x_1 - x_3)(\omega x_1 - x_4), \omega x_2 - x_3, \omega x_3 - x_4, \omega x_4 - x_5, \omega x_5 - x_1\}.$$

A reduced Gröbner basis for H_G with respect to the ordering $x_5 \prec x_4 \prec x_3 \prec x_2 \prec x_1$ is

$$\{x_5^5 - 1, x_4 - \omega^4 x_5, x_3 - \omega^3 x_5, x_2 - \omega^2 x_5, x_1 - \omega x_5\},$$

which is a generating set for $H_{G,C}$ with $C = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 1)\}$. □

Let G be an undirected graph with vertex set V and edge set E, and consider the auxiliary directed graph $\tilde{G}$ with vertices V and arcs $Arcs(G)$. Notice that $\tilde{G}$ is doubly covered, and hence each of its cycles are doubly covered. We apply Theorem 1.0.8 to $H_{\tilde{G}}$ to determine and count Hamiltonian cycles in G. In particular, the cycle $C = \{v_1, v_2, \ldots, v_n\}$ of G is Hamiltonian if and only if $\{(v_1, v_2), (v_2, v_3), \ldots, (v_{n-1}, v_n), (v_n, v_1)\}$ and $\{(v_2, v_1), (v_3, v_2), \ldots, (v_n, v_{n-1}), (v_1, v_n)\}$ are Hamiltonian cycles of $\tilde{G}$.

EXAMPLE 2.2.8. *Let G be the undirected complete graph on the vertex set $V = \{1, 2, 3, 4\}$. Let $\tilde{G}$ be the doubly covered graph with vertex set V and arcs $Arcs(G)$. Notice that $\tilde{G}$ has*

twelve Hamiltonian cycles:

$$C_1 = \{(1,2),(2,3),(3,4),(4,1)\}, \qquad C_2 = \{(2,1),(3,2),(4,3),(1,4)\},$$
$$C_3 = \{(1,2),(2,4),(4,3),(3,1)\}, \qquad C_4 = \{(2,1),(4,2),(3,4),(1,3)\},$$
$$C_5 = \{(1,3),(3,2),(2,4),(4,1)\}, \qquad C_6 = \{(3,1),(2,3),(4,2),(1,4)\},$$
$$C_7 = \{(1,3),(3,4),(4,2),(2,1)\}, \qquad C_8 = \{(3,1),(4,3),(2,4),(1,2)\},$$
$$C_9 = \{(1,4),(4,2),(2,3),(3,1)\}, \qquad C_{10} = \{(4,1),(2,4),(3,2),(1,3)\},$$
$$C_{11} = \{(1,4),(4,3),(3,2),(2,1)\}, \qquad C_{12} = \{(4,1),(3,4),(2,3),(1,2)\}.$$

One can check in a symbolic algebra system such as SINGULAR or Macaulay 2 that the ideal $H_{\tilde{G}}$ is the intersection of the cycle ideals $H_{\tilde{G},C_i}$ for $i = 1, \ldots, 12$.

2.3. Automorphism Groups as Algebraic Varieties and their Convex Approximations

In this section, we study the convex hull of automorphism groups of undirected simple graphs. Recall that if G is a graph on n vertices, its automorphism group $Aut(G)$ can be represented by $n \times n$ permutation matrices, and this set of matrices is precisely the variety of the ideal in Proposition 1.0.10. We also recall $Aut(G)$ is precisely the integer vertices of the polytope P_G, so we are particularly interested in approximating the *integer hull* $IP_G = conv(P_G \cap \mathbb{Z}^{n \times n})$ of P_G. In the special case that G is an independent set on n vertices, $Aut(G) = S_n$ and P_G is the polytope B_n (see Chapter 5 of [**KKY84**]). One can therefore view P_G as a generalization of the Birkhoff polytope to arbitrary graphs. Unfortunately, the polytope P_G is not always integral. For instance, P_G is not integral when G is the Petersen graph ([**CG97**]). Nevertheless, we prove quasi-integrality.

Proof of Proposition 1.0.11. We claim that there exists a 0/1 matrix A such that P_G is the set of points $\{x \in \mathbb{R}^{n \times n} \ : \ Ax = \mathbf{1}, x \geq 0\}$ (where $\mathbf{1}$ is the all 1s vector). By the main theorem of Trubin [**Tru69**] and independently [**BP72**], polytopes given by such systems are quasi-integral (see also Theorem 7.2 in Chapter 4 of [**KKY84**]). Therefore, we need to rewrite the defining equations presented in Proposition 1.0.10 to fit this desired

shape. Fix indices $1 \leq i, j \leq n$ and consider the row of P_G defined by the equation

$$\sum_{r \in \delta(j)} P_{ir} - \sum_{k \in \delta(i)} P_{kj} = 0.$$

Here $\delta(i)$ denotes those vertices j which are connected to i. Adding the equation $\sum_{r=1}^{n} P_{rj} = 1$ to both sides of this expression yields

$$\sum_{r \in \delta(j)} P_{ir} + \sum_{k \notin \delta(i)} P_{kj} = 1. \tag{2.27}$$

We can therefore replace the original n^2 equations defining P_G by (2.27) over all $1 \leq i, j \leq n$. The result now follows provided that no summand in each of these equations repeats. However, this is clear since if summands P_{kj} and P_{ir} are the same, then $r = j$, which is impossible since $r \in \delta(j)$. □

We would still like to find a tighter description of IP_G in terms of inequalities. For this purpose, recall the radical polynomial ideal I_G in Proposition 1.0.10 and its real variety $V_{\mathbb{R}}(I_G)$. In this section we focus on finding graphs G such that I_G is 1-exact; we shall call such graphs *exact* in what follows. The key to finding exact graphs is the following combinatorial-geometric characterization.

THEOREM 2.3.1. [**GPT10**] *Let $V_{\mathbb{R}}(I) \subset \mathbb{R}^n$ be a finite real variety. Then $V_{\mathbb{R}}(I)$ is exact if and only if there is a finite linear inequality description of $conv(V_{\mathbb{R}}(I))$ such that for every inequality $g(x) \geq 0$, there is a hyperplane $g(x) = \alpha$ such that every point in $V_{\mathbb{R}}(I)$ lies either on the hyperplane $g(x) = 0$ or the hyperplane $g(x) = \alpha$.*

A result of Sullivant (see Theorem 2.4 in [**Sul06**]) directly implies that when the polytope $P = conv(V_{\mathbb{R}}(I))$ is lattice isomorphic to an integral polytope of the form $[0, 1]^n \cap L$ where L is an affine subspace, then P satisfies the condition of Theorem 2.3.1. From this, we can prove Theorem 1.0.15, which genearlizes the work of Tinhofer [**Tin86**].

PROOF OF THEOREM 1.0.15. If G is compact, then the integer hull of P_G is precisely the affine space

$$\{P \in \mathbb{R}^{n \times n} \ : \ PA_G = A_G P, \ \sum_{i=1}^{n} P_{ij} = \sum_{j=1}^{n} P_{ij} = 1, \ 1 \leq i, j \leq n\}$$

intersected with the cube $[0,1]^{n\times n}$. That G is exact follows from Theorem 2.4 of [**Sul06**].

We now prove Statement 2. If $G_i \ncong G_j$ for some pair (i,j), then G was shown to be non-compact by Tinhofer (see [**Tin86**, Lemma 2]). Nevertheless, G is exact. We prove this for $m = 2$, and the result will follow by induction. We claim that if $G = G_1 \sqcup G_2$ with $G_1 \ncong G_2$, then the integer hull IP_G is the solution set to the following system (which we denote by $\widetilde{IP}_G$):

$$\begin{aligned}
(PA_G - A_G P)_{i,j} &= 0 \qquad && 1 \le i,j \le n,\\
\sum_{i=1}^{n} P_{i,j} &= 1 && 1 \le j \le n,\\
\sum_{j=1}^{n} P_{i,j} &= 1 && 1 \le i \le n,\\
\sum_{i=1}^{n_1}\sum_{j=n_1+1}^{n_1+n_2} P_{i,j} &= 0,\\
0 \le P_{i,j} &\le 1,
\end{aligned}$$

where $n_i = |V(G_i)|$ with $n_1 \le n_2$. Statement 2 then follows again from Theorem 2.4 of [**Sul06**].

We now prove the claim. Let A_{G_i} be the adjacency matrix of G_i. Index the adjacency matrix of $G = G_1 \sqcup G_2$ so that the first n_1 rows (and hence first n_1 columns) index the vertices of G_1. Any feasible P of P_G can be written as a block matrix

$$P = \begin{pmatrix} A_P & B_P \\ C_P & D_P \end{pmatrix},$$

in which A_P is $n_1 \times n_1$. Since G_1 and G_2 are not isomorphic, the only integer vertices of P_G are of the form $\begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$ where P_i is an automorphism of G_i.

Now let P be any non-integer vertex of P_G. We claim that the row sums of B_P must be 1. This will establish that IP_G is described by the system $\widetilde{IP}_G$. To see this, observe that if Q is any point in P_G not in IP_G, it is a convex combination of points in P_G, one of which (say P) is non-integer. If the row sums of B_P are 1, then Q violates the system $\widetilde{IP}_G$.

We now prove that if P is a non-integer vertex of P_G, then the row sums of B_P must be 1. Since P commutes with the adjacency matrix A_G of G, we must have

$$A_P A_{G_1} = A_{G_1} A_P, \quad B_P A_{G_2} = A_{G_1} B_P, \quad C_P A_{G_2} = A_{G_1} C_P, \quad D_P A_{G_2} = A_{G_2} D_P.$$

Let $\{b_1, \ldots, b_{n_2}\}$ be the column sums of B_P. We shall calculate the sum of the entries in each column of $B_P A_{G_2} = A_{G_1} B_P$ in two ways. First, consider $A_{G_1} B_P$. Since G_1 is k-regular, each entry of the i-th column of B_P will contribute exactly k times to the sum of the entries of the i-th column of $A_{G_1} B_P$. Thus, the sum of the entries of the i-th column of $A_{G_1} B_P$ is kb_i.

Second, consider $B_P A_{G_2}$. The sum of the entries in its i-th column is the sum of the entries of the columns of B_P indexed by the neighbors of i in G_2. Thus, the sum of the entries in the i-th column of $B_P A_{G_2}$ is $\sum_{l \in \delta_{G_2}(i)} b_l$. It follows that $kb_i = \sum_{l \in \delta_{G_2}(i)} b_l$ for each $1 \leq i \leq n$. This equality can be written concisely as:

$$\left(kI_{n_2 \times n_2} - A_{G_2}\right) \begin{pmatrix} b_1 \\ \vdots \\ b_{n_2} \end{pmatrix} = 0.$$

The matrix $kI_{n_2 \times n_2} - A_{G_2}$ is the Laplacian of G_2. It is well known that the kernel of the Laplacian of a connected graph is one dimensional (see [**CG97**], Lemma 13.1.1). Since G_2 is regular, the kernel contains the all ones vector. It follows that $b_1 = \cdots = b_{n_2}$. By a similar argument, the row sums of C_P are all the same. Since all row sums and column sums of P are 1, and the row sums and column sums of A_{G_1} are the same, it follows that the row sums of B_P are equal and are the same as the column sums of C_P.

Now assume for contradiction that the row sums of B_P are not 1. If the row sums are 0, then B_P and C_P would be 0 matrices. Since G_1 and G_2 are compact this would imply A_P and D_P are permutation matrices, contradicting that P is not integral. Thus the sum of each row of B_P is λ with $0 < \lambda < 1$. This implies the sum of the rows of A_P is $1 - \lambda$ and that $\frac{1}{1-\lambda} A_P$ is a feasible solution to P_{G_1}. By compactness of G_1, the matrix $\frac{1}{1-\lambda} A_P$ is

a convex combination $\sum_{i=1}^{k} \mu_k Q_k$ of permutations Q_k of G_1. This implies that

$$P = \sum_{i=1}^{k} \mu_i \begin{pmatrix} (1-\lambda)Q_k & B_P \\ C_P & D_P \end{pmatrix},$$

which is a convex combination of feasible solutions to P_G, contradicting P being a vertex. It follows that the row sums of B_P must be 1. □

Exact graphs are then more abundant than compact graphs and the convex hull of automorphisms of an exact graph has a description in terms of semidefinite programming. It is thus desirable to find nice classes of graphs that are exact. Notice that being exact here is really a property of the set of permutation matrices representing an automorphism group. This motivates the study of general subgroups of $n \times n$ permutation matrices and their behavior with respect to the theta body hierarchy. This along with understanding the convex geometry of the convex hull of such subgroups is the focus of Chapter 3.

CHAPTER 3

The Convex Geometry of Permutation Polytopes

3.1. Preliminaries

We begin this chapter with some preliminaries that will be necessary in order to further understand the geometry of permutation polytopes. First, we quickly introduce a lemma that allows us to compute the Ehrhart polynomial of an integer polytope $P \subset \mathbb{R}^n$ that is unimodular in $\text{aff}(P) \cap \mathbb{Z}^n$. This will be useful in proving Theorem 1.0.18.

LEMMA 3.1.1. *(See Theorem 9.3.25 in* [**DLRS10**]*) Let $P \subset \mathbb{R}^n$ be a lattice polytope. Assume that P has a $\mathbb{Z}$-unimodular triangulation with f_k faces of dimension k. Then the Ehrhart polynomial of P is*

$$i(P,t) = \sum_{k=0}^{n} \binom{t-1}{k} f_k.$$

In order to employ Lemma 3.1.1, we need to shift our focus to determining unimodular triangulations. We do this by using Gale duality, which we now introduce. In what follows, let $P \subset \mathbb{R}^n$ be a polytope with r vertices $V = \{v_1, v_2, \ldots, v_r\}$ that lie on a common subspace and let $d = \dim(P)$. Let $V \in \mathbb{R}^{n \times r}$ be the matrix given by

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_r \end{pmatrix}. \tag{3.1}$$

Let $\mathcal{G} \in \mathbb{R}^{(r-d-1)\times r}$ be a matrix whose rows form a basis for the space of linear dependences of the columns of (3.1). The *Gale dual* of P is the vector configuration $\{\overline{v}_1, \overline{v}_2, \ldots, \overline{v}_r\}$ consisting of the columns of $\mathcal{G}$. Note that $\mathcal{G}$ is unique up to linear coordinate transformations. The relationship between triangulations of a polytope and the structure of its Gale dual hinges on the *chamber complex* of $\mathcal{G}$. Denote by $\Sigma_{\mathcal{G}}$ the set of cones generated by all bases of $\mathcal{G}$, that is, all subsets of $\{\overline{v}_1, \overline{v}_2, \ldots, \overline{v}_r\}$ that form bases for the column space of $\mathcal{G}$. If $\sigma \in \Sigma_{\mathcal{G}}$, let $\partial\sigma$ denote its boundary, and let $\partial\Sigma_{\mathcal{G}}$ be the union of the boundaries of all cones $\sigma \in \Sigma_{\mathcal{G}}$. The complement of $\partial\Sigma_{\mathcal{G}}$ inside the cone generated by $\{\overline{v}_1, \overline{v}_2, \ldots, \overline{v}_r\}$ consists of open convex cones. The closure of such an open convex cone is called a *chamber*, and the

chamber complex of $\mathcal{G}$ is the collection of all these chambers. The chamber complex of $\mathcal{G}$ and its relationship to triangulations of P is encapsulated in the following lemma.

LEMMA 3.1.2. *(See Theorem 5.4.5, Theorem 5.4.7, and Theorem 5.4.9 in* [**DLRS10**]*) Let $P \subset \mathbb{R}^n$ be a d-dimensional polytope with vertex set $V = \{v_1, v_2, \ldots, v_r\}$ and Gale dual $\{\overline{v}_1, \overline{v}_2, \ldots, \overline{v}_r\}$. Let τ be a chamber of the chamber complex of $\mathcal{G}$. Then*

$$\Delta = \bigcup conv(V \backslash \{v_{j_1}, v_{j_2}, \ldots, v_{j_{r-d-1}}\}),$$

taken over all $\{v_{j_1}, v_{j_2}, \ldots, v_{j_{r-d-1}}\}$ such that $\tau \subseteq conv\{\overline{v}_{j_1}, \overline{v}_{j_2}, \ldots, \overline{v}_{j_{r-d-1}}\}$ is a full-dimensional cone in the Gale dual, is a regular triangulation of P. Moreover, all regular triangulations of P arise in this way from some chamber τ.

Unfortunately, the aforementioned triangulations given by the Gale dual may not be $\mathbb{Z}$- nor P-unimodular, so we still need methods to determine if a given polytope P has a $\mathbb{Z}$-unimodular or P-unimodular triangulation. One way to do this is through the use of Gröbner bases of toric ideals. Though this can be addressed in a more general setting, we will restrict ourselves to permutation polytopes arising from subgroups of a particular S_n. Let $G = \{g_1, g_2, \ldots, g_k\}$ be elements of such a subgroup, and as usual consider g_i as an $n \times n$ permutation matrix for each i. Let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_{g_1}, x_{g_2}, \ldots, x_{g_k}]$ be the polynomial ring in k indeterminates indexed by the elements of G and let $\mathbb{C}[\mathbf{t}] := \mathbb{C}[t_{\ell m} : 1 \leq \ell, m \leq n]$. The algebra homomorphism induced by the map

$$\hat{\pi}_G : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{t}],\ \hat{\pi}_G(x_{g_i}) = \prod_{1 \leq \ell, m \leq n} t_{\ell m}^{(g_i)_{\ell m}},\quad 1 \leq i \leq k$$

has as its kernel the ideal I_G. Given a monomial order $\prec$ on $\mathbb{C}[\mathbf{x}]$, the ideal I_G can determine a $P(G)$-unimodular triangulation of $P(G)$. Moreover, this triangulation is always regular. See [**DLRS10, Stu96**] for more on regular triangulations.

LEMMA 3.1.3. *(See Corollary 8.9 in* [**Stu96**] *and Theorem 9.4.5 in* [**DLRS10**]*) Let $in_\prec(I_G)$ be the initial ideal of I_G with respect to the term order $\prec$. The support vectors of the generators of the radical of $in_\prec(I_G)$ are the minimal non-faces of a regular triangulation of $P(G)$. Moreover, $in_\prec(I_G)$ is square-free if and only if the corresponding triangulation $\Delta_\prec$ of $P(G)$ is $P(G)$-unimodular.*

By Lemma 3.1.3 and the theory of Gröbner bases, $P(G)$ will have a $P(G)$-unimodular triangulation if there is a term order $\prec$ on $\mathbb{C}[\mathbf{x}]$ such that the Gröbner basis of I_G is generated by polynomials whose initial terms are square-free. This will be exploited in Section 3.3. For more on the relationship between toric ideals, Gröbner bases, and triangulations, see [**Stu96**].

Gale duality is also useful for determining whether a group $G \leq S_n$ is exact, as illustrated in the following lemma.

LEMMA 3.1.4. *Let $P(G) \subseteq \mathbb{R}^{n\times n}$ be a permutation polytope with vertex set $\{v_1, v_2, \ldots, v_r\}$ and Gale dual $\{\overline{v}_1, \overline{v}_2, \ldots, \overline{v}_r\}$. Then G is TH_1-exact if and only if for every $J \subseteq \{1, 2, \ldots, r\}$ such that conv$\{v_j \mid j \in J\}$ is a facet of $P(G)$, $\sum_{j\notin J} \overline{v}_j = 0$.*

PROOF. Throughout this proof, we use the equivalence of TH_1-exactness with the property of $P(G)$ being two-level, which was proved in Lemma 2.3.1. Let $J \subseteq \{1, 2, \ldots, r\}$ such that conv$\{v_j \mid j \in J\}$ is a facet of $P(G)$ with the defining inequality $c \cdot x - \alpha \geq 0$ valid on $P(G)$. Then

$$0 = (c, -\alpha) \begin{pmatrix} v_1 & v_2 & \cdots & v_r \\ 1 & 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \overline{v}_1 \\ \overline{v}_2 \\ \vdots \\ \overline{v}_r \end{pmatrix} = (c \cdot v_1 - \alpha, c \cdot v_2 - \alpha, \cdots, c \cdot v_r - \alpha) \begin{pmatrix} \overline{v}_1 \\ \overline{v}_2 \\ \vdots \\ \overline{v}_r \end{pmatrix}.$$

Since G is exact, $c \cdot v_j - \alpha$ can take at most two values. By construction, one of these values is zero. If the other value is β, then $c \cdot v_j - \alpha = \beta$ if and only if $j \notin J$. Thus $\sum_{j\notin J} \beta\overline{v}_j = 0$, which implies that $\sum_{j\notin J} \overline{v}_j = 0$ since $\beta \neq 0$.

For the converse, suppose that $\sum_{j\notin J} \overline{v}_j = 0$ for every J such that conv$\{v_j \mid j \in J\}$ is a facet. Fix such a J and assume that the facet inequality of $P(G)$ defining it is $c \cdot x - \alpha \geq 0$. Then, as we have done above,

$$0 = \sum_{j\notin J} (c \cdot v_j - \alpha)\overline{v}_j = \sum_{j\notin J} (c \cdot v_j)\overline{v}_j - \alpha \sum_{j\notin J} \overline{v}_j = \sum_{j\notin J} (c \cdot v_j)\overline{v}_j.$$

Suppose that there are at least two distinct values among $\{c \cdot v_j \mid j \notin J\}$ and that γ is the least value. Then

$$0 = \sum_{j \notin J} (c \cdot v_j - \gamma)\overline{v}_j$$

yields a positive dependence relation on $\{\overline{v}_j \mid j \notin J\}$ that does not use all the elements in the set. This contradicts the assumption that J induces a facet of $P(G)$. Thus $\{c \cdot v_j \mid j \notin J\}$ has only one element, and hence G is exact. □

Note that in particular if $P(G)$ is TH_1-exact, then it contains a $P(G)$-unimodular triangulation. Moreover, as we will see, all simplices in this triangulation have the same volume.

3.2. Cyclic and Dihedral Groups

We dedicate this section to the proof of Theorem 1.0.18. We begin with the following lemma, which determines the Ehrhart polynomial of $P(C_n)$ and proves part (1) of Theorem 1.0.18.

LEMMA 3.2.1. *The Ehrhart polynomial of $P(C_n)$ is $i(P(C_n), t) = \binom{t+n-1}{n-1}$.*

PROOF. Let t be a positive integer and let $\phi : tP(C_n) \to t\Delta_n$ be the affine map given by $\phi(X) = [X_{1,1},\ X_{1,2},\ \cdots\ X_{1,n}]^T$. Here, Δ_n is the standard $(n-1)$-simplex $\text{conv}\{e_i \mid 1 \leq i \leq n\} \subseteq \mathbb{R}^n$. Note that ϕ is a well-defined map since the sum of the first row of any matrix in $tP(C_n)$ is t. We claim that ϕ induces a bijection between the sets $tP(C_n) \cap \mathbb{Z}^{n \times n}$ and $t\Delta_n \cap \mathbb{Z}^{n \times n}$. If $X \in tP(C_n)$ is an integer matrix, then its first row contains integer entries whose sum is t, so $\phi(X)$ is indeed an integer point in $t\Delta_n$. It suffices to show that every integer point in $t\Delta_n$ has a unique integral pre-image. Let $[X_{1,1},\ X_{1,2}, \cdots X_{1,n}]^T \in t\Delta_n \cap \mathbb{Z}^n$. Then $\phi(X_{1,1} \cdot e + X_{1,2} \cdot g + \cdots + X_{1,n} \cdot g^{n-1}) = [X_{1,1},\ X_{1,2}, \cdots X_{1,n}]^T$, so $[X_{1,1},\ X_{1,2}, \cdots X_{1,n}]^T$ has an integral pre-image. Moreover, this pre-image is unique, since g^i is the only vertex of $tP(C_n)$ whose $(1, i+1)$-entry is non-zero. Thus ϕ induces a bijection between $tP(C_n) \cap \mathbb{Z}^{n \times n}$ and $t\Delta_n \cap \mathbb{Z}^{n \times n}$, and the result follows since $i(\Delta_n, t) = \binom{t+n-1}{n-1}$. The fact that the volume of $P(C_n)$ is $\frac{1}{(n-1)!}$ follows because the first coefficient of $i(P(C_n), t)$ is $\frac{1}{(n-1)!}$ and Δ_n is $\mathbb{Z}$-unimodular. □

We now investigate the polytopes $P(D_n)$ and their Ehrhart polynomials. Recall the following lemma concerning the dimension of $P(D_n)$.

LEMMA 3.2.2. *(See Theorem 4.1 of* [**Ste99**]*) The dimension of the polytope $P(D_n)$ is $2n-2$ if n is odd and $2n-3$ if n is even.*

Lemma 3.2.2 indicates that Gale duality is very useful for determining the Ehrhart polynomial of $P(D_n)$, since the Gale dual lies in a space of dimension $|D_n| - \dim(P(D_n)) - 1$, which is one if n is odd and two if n is even.

LEMMA 3.2.3. *If n is odd, the Gale dual of $P(D_n)$ is a vector configuration in $\mathbb{R}$ consisting of n copies of each of the vectors ± 1. If n is even, $n = 2m$, the Gale dual of $P(D_n)$ is the vector configuration in $\mathbb{R}^2$ consisting of m copies of each of the four vectors $[\pm 1, 0]^T, [0, \pm 1]^T$.*

PROOF. Throughout this proof, let $\mathcal{G}$ be the matrix whose columns form the Gale dual of $P(D_n)$ with its columns indexed by $\{e, r, r^2, \ldots, r^{n-1}, f, fr, fr^2, \ldots, fr^{n-1}\}$ in that order. The following linear relation holds for D_n:

$$e + r + r^2 + \ldots + r^{n-1} = f + fr + fr^2 + \ldots + fr^{n-1} = J_{n\times n}, \tag{3.2}$$

where $J_{n\times n}$ is the $n \times n$ matrix whose entries are all one. When n is odd, Lemma 3.2.2 implies that $P(D_n)$ is $2n-2$ dimensional, so the Gale dual of $P(D_n)$ is one dimensional. Thus, Equation (3.2) implies that

$$\mathcal{G} = \begin{pmatrix} 1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 \end{pmatrix},$$

with n copies of 1 and n copies of -1. When n is even, $n = 2m$, Lemma 3.2.2 implies that $P(D_n)$ is $2n-3$ dimensional, so the Gale dual of $P(D_n)$ is two dimensional. We observe that the relation

$$\sum_{j=0}^{m-1} r^{2j+1} = \sum_{j=0}^{m-1} fr^{2j} \tag{3.3}$$

holds for D_n when n is even. The linear relations (3.2)-(3.3) and (3.3) are linearly independent, so we deduce that

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & -1 & \dots & -1 \\ 0 & 1 & \dots & 1 & -1 & 0 & \dots & 0 \end{pmatrix}.$$

We conclude that the Gale dual is the vector configuration in $\mathbb{R}^2$ consisting of n copies of each of the four vectors $[\pm 1, 0]^T, [0, \pm 1]^T$. □

We now compute the Ehrhart polynomial of $P(D_n)$. The symmetry in its Gale dual shows that the number of faces of a given dimension in any regular triangulation of $P(D_n)$ is the same. Note that this in principle completely describes the secondary polytope of $P(D_n)$. Thus, if we find any $\mathbb{Z}$-unimodular triangulation of $P(D_n)$ and compute the number of faces of each dimension in any other regular triangulation of it, we can recover its Ehrhart polynomial via Lemma 3.1.1. We begin by finding a $P(D_n)$-unimodular triangulation.

PROPOSITION 3.2.4. *The polytope $P(D_n)$ has a $P(D_n)$-unimodular regular triangulation.*

PROOF. Let G be the graph with vertices $\{1, 2, \dots, n\}$ and edges $i, i+1$ for each $i \in \{1, 2, \dots, n\}$. Let A_G be the adjacency matrix of G. Consider the polytope

$$P_G = \left\{ X \in [0,1]^{n \times n} \ : \ A_G X = X A_G, \ \sum_{j=1}^{n} X_{ij} = 1 \ \forall i, \ \sum_{i=1}^{n} X_{ij} = 1 \ \forall j \right\}.$$

The integer points of P_G are permutations commuting with A_G, so they are precisely the automorphisms of G. Since the automorphism group of G is D_n and P_G is integral (see Theorem 2 of [**Tin86**]), this implies that $P_G = P(D_n)$. But by Theorem 1.0.15, this implies the vertex set of P_G is exact, which by Theorem 2.4 of [**Sul06**] and Theorem 4.2 of [**GPT10**] implies that every reverse lexicographic triangulation of $P(D_n)$ is $P(D_n)$-unimodular. Since reverse lexicographic triangulations are regular, the result follows. □

In order to establish that $P(D_n)$ is $\mathbb{Z}$-unimodular, we prove that the index of the lattice generated by its vertices in the lattice $\text{aff}(P(D_n)) \cap \mathbb{Z}^{n \times n}$ is one.

PROPOSITION 3.2.5. *The index of the lattice generated by the vertices of $P(D_n)$ has index one in the lattice aff$(D_n) \cap \mathbb{Z}^{n \times n}$.*

PROOF. First, consider when n is odd. For simplicity, let D_n consist of the matrices $v_1, v_2, \ldots, v_{2n}$, where $v_{2i+1} = r^i$ and v_{2i+2} is the unique flip in D_n fixing $i+1$, $0 \leq i \leq n-1$. It suffices to prove that if $X \in \mathbb{Z}^{n\times n}$ and X is an $\mathbb{R}$-linear combination of the matrices $\{v_{2n} - v_1, v_{2n-1} - v_1, \ldots, v_2 - v_1\}$, then X is a $\mathbb{Z}$-linear combination of these matrices. Assume then that $X = \sum_{j=2}^{2n} \alpha_j(v_1 - v_j) = \left(\sum_{j=2}^{2n} \alpha_j\right) v_1 - \sum_{j=2}^{2n} \alpha_j v_j$, with $\alpha_j \in \mathbb{R}$. Let $\alpha \in [0,1)$ such that $\sum_{j=2}^{2n} \alpha_j + \alpha \in \mathbb{Z}$. Since e and v_{2i+2} are the only elements of D_n with the $(i+1, i+1)$-entry in their support, and since X has integer entries, we conclude that $\alpha_{2i+2} - \alpha \in \mathbb{Z}$ for all $0 \leq i \leq n-1$. Moreover, for any i, there is a unique flip with the $(1, i+1)$-entry in its support. Since r^i is the only rotation with the $(1, i+1)$-entry in its support, and again since X has integer entries, we deduce that $\alpha_{2i+1} + \alpha \in \mathbb{Z}$ for all $0 \leq i \leq n-1$. Now recall from Equation (3.2) in the proof of Lemma 3.2.3 that $\sum_{i=0}^{n-1} v_{2i+1} - \sum_{i=0}^{n-1} v_{2i+2} = 0$, so we have that

$$\begin{aligned} X &= \left(\sum_{j=2}^{2n} \alpha_j\right) v_1 - \sum_{j=2}^{2n} \alpha_j v_j - \alpha\left(\sum_{i=0}^{n-1} v_{2i+1} - \sum_{i=0}^{n-1} v_{2i+2}\right) \\ &= \sum_{i=1}^{n-1} (\alpha_{2i+1} + \alpha)(v_1 - v_{2i+1}) + \sum_{i=0}^{n-1} (\alpha_{2i+2} - \alpha)(v_1 - v_{2i+2}), \end{aligned}$$

and hence X is a $\mathbb{Z}$-linear combination of $\{v_{2n} - v_1, v_{2n-1} - v_1, \ldots, v_2 - v_1\}$.

Now consider when n is even, $n = 2m$. We let D_n consist of the $4m$ vectors $\{u_1, u_2, \ldots, u_{2m}\}$, $\{v_1, v_2, \ldots, v_{2m}\}$, where $u_{2i+1} = r^{2i}$, $v_{2i+1} = r^{2i+1}$, u_{2i+2} is the unique flip supported on the $(1, 2i+1)$-entry, and v_{2i+1} is the unique flip supported on the $(1, n+2i)$-entry, entries taken mod i and $0 \leq i \leq m-1$. Suppose that X is an $\mathbb{R}$-linear combination of the form

$$X = \sum_{i=2}^{2m} \alpha_i(u_1 - u_i) + \sum_{i=1}^{2m} \beta_i(u_1 - v_i) = \left(\sum_{i=2}^{2m} \alpha_i + \sum_{i=1}^{2m} \beta_i\right) u_1 - \sum_{i=2}^{2m} \alpha_i u_i - \sum_{i=1}^{2m} \beta_i v_i.$$

Let $\alpha \in [0,1)$ such that $\sum_{i=2}^{2m} \alpha_i + \sum_{i=1}^{2m} \beta_i - \alpha \in \mathbb{Z}$. Notice that $u_1 = e$. Since e and u_{2i+2} are the only elements of D_n with the (i,i)-entry in their support and X has integer entries, we conclude that $\alpha_{2i_2} - \alpha \in \mathbb{Z}$ for all $0 \leq i \leq m-1$. Moreover, u_{2i+1} and u_{2i+2} are the only elements with the $(1, 2i+1)$-entry in their support, so $\alpha_{2i+1} + \alpha \in \mathbb{Z}$ for all $0 \leq i \leq m-1$. Similarly, if $\beta \in [0,1)$ such that $\beta_1 + \beta \in \mathbb{Z}$, then $\beta_{2i+1} + \beta, \beta_{2i+2} - \beta \in \mathbb{Z}$ for all $0 \leq i \leq m-1$. Now from Equation (3.2)-Equation (3.3) and Equation (3.3) in the

proof of Lemma 3.2.3, we have that

$$\sum_{i=0}^{m-1} u_{2i+1} = \sum_{i=0}^{m-1} u_{2i+2}, \quad \sum_{i=0}^{m-1} v_{2i+1} = \sum_{i=0}^{m-1} v_{2i+2}.$$

We conclude then that

$$\begin{aligned} X &= \left(\sum_{i=2}^{2m} \alpha_i + \sum_{i=1}^{2m} \beta_i\right) u_1 - \sum_{i=2}^{2m} \alpha_i u_i - \sum_{i=1}^{2m} \beta_i v_i - \alpha \left(\sum_{i=0}^{m-1} u_{2i+1} - \sum_{i=0}^{m-1} u_{2i+2}\right) \\ &\quad - \beta \left(\sum_{i=0}^{m-1} v_{2i+1} - \sum_{i=0}^{m-1} v_{2i+2}\right) \\ &= \sum_{i=1}^{m-1} (\alpha_{2i+1} + \alpha)(u_1 - u_{2i+1}) + \sum_{i=0}^{m-1} (\alpha_{2i+2} - \alpha)(u_1 - u_{2i+2}) \\ &\quad + \sum_{i=0}^{m-1} (\beta_{2i+1} + \beta)(u_1 - v_{2i+1}) + \sum_{i=0}^{m-1} (\beta_{2i+2} - \beta)(u_1 - v_{2i+2}), \end{aligned}$$

which is a $\mathbb{Z}$-linear combination of the required vectors. □

We now determine the number of faces of each dimension in a particular triangulation of $P(D_n)$. This together with Lemma 3.1.1, Proposition 3.2.4, and Proposition 3.2.5 proves parts (2) and (3) of Theorem 1.0.18.

Proof of Theorem 1.0.18. First, consider when n is odd. By Lemma 3.2.3, the Gale dual of $P(D_n)$ consists of the vectors $\{e_1^{(1)}, e_1^{(2)}, \ldots, e_1^{(n)}, -e_1^{(1)}, -e_1^{(2)}, \ldots, -e_1^{(n)}\}$ where the $e_1^{(i)}, -e_1^{(i)}$ are copies of the vectors $e_1, -e_1$ in $\mathbb{R}$ respectively, $1 \leq i \leq n$. The set consisting of the vector e_1 is the only extreme ray in one chamber in the Gale dual, so by Lemma 3.1.2, $P(D_n)$ has a triangulation Δ with maximal dimensional simplices $\big\{\text{conv}\{G\backslash\{r^i\}\} |\ 1 \leq i \leq n\big\}$. The number of $(k+1)$-element subsets of G is $\binom{2n}{k+1}$. By Lemma 3.1.2, of these subsets, the ones that are not simplices in Δ are those that contain all of $\{e, r, r^2, \ldots, r^{n-1}\}$. There are precisely $\binom{2n-n}{k+1-n}$ such subsets, so we conclude that the number of k-dimensional faces f_k in Δ is

$$f_k = \binom{2n}{k+1} - \binom{n}{k+1-n}.$$

By the symmetry in the Gale dual, this is also the number of k-dimensional faces in a reverse lexicographic triangulation of $P(D_n)$, which is $P(D_n)$-unimodular by Proposition 3.2.4 and hence $\mathbb{Z}$-unimodular by Propostion 3.2.5. The Ehrhart polynomial follows

from Lemma 3.1.1. Moreover, we see that $f_{2n-2} = \binom{2n}{2n-1} - \binom{n}{n-1} = n$, so the volume of $P(D_n)$ is $\frac{n}{(2n-2)!}$.

Now consider $P(D_n)$ when n is even, $n = 2m$. By Lemma 3.2.3, the Gale dual of $P(D_n)$ consists of the copies $\{e_1^{(i)}, e_2^{(i)}, -e_1^{(i)}, -e_2^{(i)} \mid 1 \leq i \leq m\}$ of $e_1, e_2, -e_1, -e_2$ respectively in $\mathbb{R}^2$. Consider the chamber of the Gale dual whose extreme rays are the vectors $\{e_1, e_2\}$. By Lemma 3.1.2, this chamber gives the regular triangulation Δ of $P(D_n)$ whose maximal dimensional simplices are $\big\{\text{conv}\{G\backslash\{r^{2i-1}, r^{2j}\}\} \big| \ 1 \leq i, j \leq n\big\}$. By a similar counting argument as in the odd case, we conclude that

$$f_k = \binom{2n}{k+1} - \binom{2}{1}\binom{2n-m}{k+1-m} + \binom{2n-2m}{k+1-2m}.$$

Again, since Lemma 3.1.1 implies that $P(D_n)$ has a $P(D_n)$-unimodular triangulation and hence by Proposition 3.2.4 a $\mathbb{Z}$-unimodular triangulation with the same face numbers, the Ehrhart polynomial follows by Lemma 3.1.1. Lastly, we see that the volume of $P(D_n)$ when n is even is f_{2n-3}, which is

$$\frac{1}{(2n-3)!}\left(\binom{2n}{2n-2} - 2\binom{2n-m}{2n-m-2} + \binom{2n-m}{2n-2m-2}\right) = \frac{n^2}{4 \cdot (2n-3)!}.$$

□

Remark. One can further show from the proof of Theorem 1.0.18 that all simplices in the given triangulations have the same volume.

Example 3.2.6. *We use Theorem 1.0.18 to determine the Ehrhart polynomials and volumes of $P(D_4)$ and $P(D_5)$. First, we have that $i(P(D_4), t)$ is*

$$8\binom{t-1}{0} + 26\binom{t-1}{1} + 44\binom{t-1}{2} + 41\binom{t-1}{3} + 20\binom{t-1}{4} + 4\binom{t-1}{5},$$

which is precisely the polynomial

$$\frac{1}{30}t^5 + \frac{1}{3}t^4 + \frac{4}{3}t^3 + \frac{8}{3}t^2 + \frac{79}{30}t + 1.$$

The volume of $P(D_4)$ is therefore $\frac{1}{30}$. Similarly, we have that $i(P(D_5), t)$ is

$$10\binom{t-1}{0} + 45\binom{t-1}{1} + 120\binom{t-1}{2} + 210\binom{t-1}{3} + 251\binom{t-1}{4} + 205\binom{t-1}{5} + 110\binom{t-1}{6} + 35\binom{t-1}{7} + 5\binom{t-1}{8},$$

which is precisely the polynomial

$$\frac{1}{8064}t^8 + \frac{5}{2016}t^7 + \frac{5}{192}t^6 + \frac{25}{144}t^5 + \frac{95}{128}t^4 + \frac{575}{288}t^3 + \frac{6515}{2016}t^2 + \frac{475}{168}t + 1.$$

The volume of $P(D_5)$ is therefore $\frac{1}{8064}$.

3.3. Frobenius Groups

In this section, we discuss triangulations and normalized volumes of Frobenius polytopes, leading to a proof of Theorem 1.0.19. We also establish that all Frobenius groups are exact, hence proving Proposition 1.0.20. For the remainder of this section, we assume that $G \leq S_n$ is a Frobenius group. We let $N = \{u_1, u_2, \ldots, u_n\}$ be its Frobenius kernel ($n = |N|$), and we let $H = \{v_1, v_2, \ldots, v_h\}$ be its Frobenius complement ($h = |H|$). We assume throughout that H is the set of coset representatives for N in G. We let $\mathcal{G}$ denote the matrix whose columns form the Gale dual of $P(G)$. Recall that $G = NH$ and $H \cap N = \{e\}$, and so G consists of the nh matrices

$$u_1v_1, u_2v_1, \ldots, u_nv_1, u_1v_2, u_2v_2, \ldots, u_nv_2, \ldots, u_1v_h, u_2v_h, \ldots, u_nv_h$$

and we index the columns of $\mathcal{G}$ by G in this order. The following lemmas are proven in [**CP10**].

LEMMA 3.3.1. *(See Proposition 4.2 in* [**CP10**]*) If $G \leq S_n$ is Frobenius, then $\sum_{i=1}^{n} u_iv_j = J_{n\times n}$ for all j, $1 \leq j \leq h$, where $J_{n\times n}$ is the $n \times n$ matrix of all 1s.*

LEMMA 3.3.2. *(See Corollary 4.5 in* [**CP10**]*) If $G \leq S_n$ is Frobenius, the dimension of $P(G)$ is $|G| - |H|$.*

Lemma 3.3.1 gives us the $|H| - 1$ linearly independent relations $\sum_{i=1}^{n} u_iv_1 = \sum_{i=1}^{n} u_iv_j$, $2 \leq j \leq h$. The dimension formula in Lemma 3.3.2 tells us that the $|H| - 1$ relations

in Lemma 3.3.1 actually form a basis for the space of linear dependences of G. As a consequence, we get the Gale dual of $P(G)$.

PROPOSITION 3.3.3. *The Gale dual of $P(G)$ consists of n copies $\{\mathbf{1}^{(1)}, \mathbf{1}^{(2)}, \ldots, \mathbf{1}^{(n)}\}$ of the all-ones vector $\mathbf{1}$ in $\mathbb{R}^{h-1}$, and n copies $\{-e_i^{(1)}, -e_i^{(2)}, \ldots, -e_i^{(n)}\}$ in $\mathbb{R}^{h-1}$ of $-e_i$ for $1 \leq i \leq h-1$, where e_i is the i^{th} standard basis vector. In particular, the $u_i v_j$ column of the matrix $\mathcal{G}$ is the vector $\mathbf{1}$ if $j = 1$, and $-e_{j-1}$ otherwise.*

PROOF. This follows directly from Lemma 3.3.1 and Lemma 3.3.2. □

Now consider the chamber in the Gale dual whose extreme rays are $-e_1$,$-e_2$,...,$-e_{h-1}$. From Lemma 3.1.2, $P(G)$ has a corresponding regular triangulation Δ whose maximal dimensional simplices are

$$\Delta = \left\{\text{conv}\left\{G\backslash\{u_{i_1}v_2, u_{i_2}v_3, \ldots, u_{i_{h-1}}v_h\}\right\} \mid 1 \leq i_j \leq n\right\} \tag{3.4}$$

Furthermore, from the structure of the Gale dual as given by Proposition 3.3.3, all triangulations of $P(G)$ have the same number of k-dimensional faces for any k. Thus, if we can determine a $P(G)$-unimodular triangulation of $P(G)$ and count the number of faces of dimension k for each k in the triangulation Δ, we can prove Theorem 1.0.19. We proceed by showing that $P(G)$ has a $P(G)$-unimodular triangulation and then by determining the number of faces of given dimensions in Δ.

PROPOSITION 3.3.4. *If G is Frobenius then G has a $P(G)$-unimodular triangulation.*

PROOF. Our proof appeals to toric algebra. Let $A \in \mathbb{R}^{n^2 \times |G|}$ be the matrix whose columns are the elements of G written as n^2-dimensional column vectors by reading rows left to right and top to bottom. We index the columns of A by the elements of G as in $\mathcal{G}$. The toric ideal $I_G \subseteq \mathbb{C}[\mathbf{x}] = \mathbb{C}[x_{u_r v_s} : 1 \leq r \leq n,\ 1 \leq s \leq h]$ is the kernel of the homomorphism

$$\hat{\pi} : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{t}], \quad \hat{\pi}(x_{u_r v_s}) = \prod_{1 \leq \ell, m \leq n} t_{\ell m}^{(u_r v_s)_{\ell m}},$$

and by Lemma 4.1 of [**Stu96**], $I_G = \langle x^u - x^v \mid A(u-v) = 0,\ u, v \in \mathbb{Z}^{|G|}\rangle$. By Lemma 3.3.1 and Lemma 3.3.2, $\ker(A)$ has the basis $\{b_1, b_2, \ldots, b_k\}$ where $b_i = e_{u_1} + e_{u_2} + \cdots + e_{u_n} - e_{u_1 v_i} - e_{u_2 v_i} - \cdots - e_{u_n v_i}$ for each i. Now if $u - v \in \ker(A)$ is integral, then $u - v = \sum_{i=1}^{h} \lambda_i b_i$,

where $\lambda_i \in \mathbb{Q}$ for each i. In fact, $\lambda_i \in \mathbb{Z}$ for each i since the $u_\ell v_i$ component of $u - v$ is $\pm\lambda_i$. We conclude by Corollary 4.4 of [**Stu96**] that $I_G = \langle x_{H_1} - x_{H_\ell} : 2 \leq \ell \leq h \rangle$ where $x_{H_\ell} = \prod_{i=1}^{n} x_{u_i v_\ell}$ for each ℓ.

In fact, $\{x_{H_1} - x_{H_\ell} : 2 \leq \ell \leq h\}$ is a Gröbner basis for I_G with respect to the reverse lexicographic order $\prec$; here, $u_{r_1} v_{s_1}$ comes lexicographically before $u_{r_2} v_{s_2}$ if and only if $r_1 \leq r_2, s_1 \leq s_2$. To see this, we use Buchberger's algorithm. For an introduction to this algorithm and details of terms to follow, see [**CLO07**]. Consider any pair of polynomials $f_r = x_{H_1} - x_{H_r}, f_s = x_{H_1} - x_{H_s}$ in our generating set for I_G. With respect to $\prec$, we compute the S-pair $S(f_r, f_s)$ and see that

$$S(f_r, f_s) = \frac{x_{H_r} x_{H_s}}{-x_{H_r}}(x_{H_1} - x_{H_r}) - \frac{x_{H_r} x_{H_s}}{-x_{H_s}}(x_{H_1} - x_{H_s}) = x_{H_1} x_{H_r} - x_{H_1} x_{H_s}.$$

Now since $x_{H_1} x_{H_r} - x_{H_1} x_{H_s} = x_{H_1}(x_{H_1} - x_{H_s}) - x_{H_1}(x_{H_1} - x_{H_r})$, we see that $\overline{S(f_r, f_s)}^{f_r f_s} = 0$. Since r, s were arbitrary, Buchberger's algorithm concludes that $\{x_{H_1} - x_{H_\ell} : 2 \leq \ell \leq h\}$ is a Gröbner basis for I_G. By Lemma 3.1.3, we conclude that $P(G)$ has a $P(G)$-unimodular triangulation. □

We note here that unlike cyclic and dihedral groups, it is not always the case that Frobenius groups have $\mathbb{Z}$-unimodular triangulations, so with these methods we except to only uncover the normalized volume of these polytopes.

EXAMPLE 3.3.5. *Consider the group $A_4 \leq S_4$ (see introduction for definition). This group is Frobenius with Frobenius kernel $N = \langle (12)(34), (13)(24) \rangle$ and Frobenius complement $H = \langle (123) \rangle$. According to Theorem 1.0.19, if $P(A_4)$ was $\mathbb{Z}$-unimodular then its volume would be $\frac{1}{22680}$, however from the table in A, the volume is $\frac{1}{5670}$.*

If our methods are to be used for Frobenius groups that are not $\mathbb{Z}$-unimodular, one needs to determine the index of the lattice generated by the vertices inside the lattice $\mathbb{Z}^n$ to determine volume of the simplices in the $P(G)$-unimodular triangulation. This is enough to recover the volume because the volumes of the individual simplices are the same; this is immediate from the symmetry in the Gale dual. We comment here that from communication with Raman Sanyal and Bernd Strumfels, one can also determine the volume of $P(G)$-unimodular groups in general if one can determine the edge lengths of all edges eminating from a fixed vertex. We now proceed to proving Theorem 1.0.19.

PROOF OF THEOREM 1.0.19. By Proposition 3.3.4, $P(G)$ has a $P(G)$-unimodular triangulation, and by Proposition 3.3.3 and Lemma 3.1.2, all triangulations of $P(G)$ have the same face numbers. Thus it suffices to determine the number of top dimensional faces in the triangulation Δ in (3.4) and apply Lemma 3.1.1. We more generally determine the number of k-dimensional faces f_k for each k. Any k-simplex in Δ must be a subset of some maximal dimensional simplex of Δ, and by Lemma 3.1.2, all maximal dimensional simplices in Δ do not contain $\{u_1v_i, u_2v_i, \ldots, u_nv_i\}$ as a subset for any $i \geq 2$. Conversely, if a $(k+1)$-element subset of G does not contain $\{u_1v_i, u_2v_i, \ldots, u_nv_i\}$ as a subset for any $i \geq 2$, then there exists m_i for each $i \geq 2$ such that $u_{m_i}v_i$ is not in the given subset, and this $(k+1)$-element subset is therefore a k-simplex that is a face of the maximal dimensional simplex $\text{conv}\{G \backslash \{u_{m_1}v_2, u_{m_2}v_3, \ldots, u_{m_{h-1}}v_h\}\}$. We conclude that a $(k+1)$-element subset of G is a k-simplex in Δ if and only if it does not contain $\{u_1v_i, u_2v_i, \ldots, u_nv_i\}$ as a subset for any $i \geq 2$. Thus, to determine f_k, we need to count the number of $(k+1)$-element subsets of G that do not contain $\{u_1v_i, u_2v_i, \ldots, u_nv_i\}$ as a subset for any $i \geq 2$.

Let us call a subset of the form $\{u_1v_i, u_2v_i, \ldots, u_nv_i\}$ a *complete copy*. There are $\binom{(h+1)n}{k+1}$ $(k+1)$-element subsets of G, and the number of such subsets that contain ℓ complete copies as subsets is $\binom{hn-\ell n}{k+1-\ell n}\binom{h-1}{\ell}$. Thus by inclusion-exclusion,

$$f_k = \sum_{\ell \geq 0} \binom{(h-\ell)n}{k+1-\ell n}\binom{h-1}{\ell}(-1)^\ell.$$

Since each maximal dimensional simplex in Δ has volume $\frac{1}{\dim(P(G))!}$, the result follows. □

We now establish that Frobenius groups are two-level, hence proving Proposition 1.0.20. In the special case of Frobenius groups, we can immediately read off the list of all vertices contained in all facets of $P(G)$, however this list was determined in [**CP10**] by other means.

LEMMA 3.3.6. *(See Corollary 4.5 in* [**CP10**]*) The complement of any set of $|H|$ elements of G, one chosen from each of the cosets of N, forms the set of vertices of a facet of $P(G)$. All facets of $P(G)$ arise this way.*

We note that a description of these facets is not immediate, nor is it immediate that there is an efficient way to list them, so we still have interest in the semidefinite descriptions given by the theta body hierarchy. In this light, we now prove Proposition 1.0.20.

PROOF OF PROPOSITION 1.0.20. Let $J \subseteq G$ be the set of vertices of a facet of G. Choose H to be the set of coset representatives of N. By Lemma 3.3.6, J is G without $\{u_i, u_iv_1, u_iv_2, \ldots, u_iv_h\}$ for some fixed i. Now let $\mathbf{1}$ be the all ones vector in $\mathbb{R}^{h-1}$ and let e_i be the standard basis vectors. Then we have

$$\sum_{j \notin J} \overline{j} = \overline{u}_i + \overline{u_iv_1} + \overline{u_iv_2} + \cdots + \overline{u_iv_h} = \mathbf{1} - e_1 - e_2 - \cdots - e_k = 0.$$

Since J was arbitrary, we conclude by Lemma 3.1.4 that $P(G)$ is two-level and thus TH_1-exact. □

3.4. Automorphism Groups of Binary Trees

In this section, we present a method for computing the Ehrhart polynomials of groups that arise as automorphism groups of finite rooted binary trees. The crux of this method lies in Theorem 1.0.21. We first introduce some necessary group theoretic preliminaries. For any groups $G \leq S_m$, $H \leq S_n$, the *direct product* $G \times H \leq S_m \times S_m \leq S_{m+n}$ consists of elements $\{(g,h) : g \in G,\ h \in H\}$ with product $(g_1,h_1) \cdot (g_2,h_2) = (g_1g_2, h_1h_2)$. By construction, the vertices of the permutation polytope of $G \times H$ are block matrices of the form $\{g \oplus h : g \in G,\ h \in H\}$. The *wreath product* of G by S_n, denoted $G \wr S_n$, is the group $\{(g,h) : g \in G^n, h \in S_n\}$ under the operation defined by

$$\begin{aligned}(g',h') \cdot (g,h) &= ((g'_1, g'_2, \ldots, g'_n), h') \cdot ((g_1, g_2, \ldots, g_n), h) \\ &:= ((g'_{h'(1)}g_1, g'_{h'(2)}g_2, \ldots, g'_{h'(n)}g_n), h'h).\end{aligned}$$

The vertices of the permutation polytope $P(G \wr S_n)$ are the $mn \times mn$ matrices $\{g \otimes h : g \in G,\ h \in S_n\}$. For more on this, see [**Ste99**].

We now prove that automorphism groups of rooted binary trees are always composed of direct products and wreath products of groups.

LEMMA 3.4.1. *Let G be the automorphism group of a rooted binary tree. Then G can be written as a sequence of direct products of groups, and wreath products by symmetric groups of order at most two.*

PROOF. Label the vertices of T by the positive integers $\{1, 2, \ldots, n\}$ such that the root vertex is labeled 1. First assume the root of T has one child, and without loss of generality assume its label is 2. Letting T_2 be the subtree of T rooted at 2, we have $\mathrm{Aut}(T) = S_1 \times \mathrm{Aut}(T_2)$. Now assume instead that the root has two children that are labeled 2 and 3 without loss of generality. Let T_2 be the subtree of T rooted at 2 and T_3 be the subtree of T rooted at 3. If T_2 and T_3 are not isomorphic, then $\mathrm{Aut}(T) = S_1 \times (\mathrm{Aut}(T_2) \times \mathrm{Aut}(T_3))$. If T_2 and T_3 are isomorphic, then $\mathrm{Aut}(T) = S_1 \times (\mathrm{Aut}(T_2) \wr S_2)$. The result then follows inductively. □

The proof of Lemma 3.4.1 indicates that computing the Ehrhart polynomial of groups arising as automorphism groups of rooted binary trees requires repeated computation of Ehrhart polynomials of direct products and wreath products by symmetric groups of order two. Theorem 1.0.21 indicates how Ehrhart polynomials behave under wreath products by symmetric groups of order two, and we prove this theorem now.

PROOF OF THEOREM 1.0.21. The vertices of the polytope $P(G \wr S_2)$ are precisely the matrices

$$\left\{ \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}, \begin{pmatrix} 0 & X_1 \\ X_2 & 0 \end{pmatrix} \right\}, \tag{3.5}$$

where the X_i are vertices of $P(G)$. Let $t \geq 2$ be an integer. If X_1, X_2 are integer matrices in $kP(G)$ and X_3, X_4 are integer matrices in $(t-k)P(G)$, then

$$X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix} + \begin{pmatrix} 0 & X_3 \\ X_4 & 0 \end{pmatrix} \tag{3.6}$$

is an integer matrix in $tP(G \wr S_2)$. Moreover, if X is an integer matrix in $tP(G \wr S_2)$, then there is a unique k and unique integer matrices $X_1, X_2 \in kP(G)$ and $X_3, X_4 \in (t-k)P(G)$ such that X can be decomposed as in (3.6). To see this, note that the supports of the above matrices imply that X can be uniquely expressed as a convex combination of the t^{th} dilations of matrices in (3.5), so

$$X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix} + \begin{pmatrix} 0 & X_3 \\ X_4 & 0 \end{pmatrix}$$

for some matrices $\{X_i \mid 1 \leq i \leq 4\}$. Since the two summands have disjoint support, X_1, X_2, X_3, X_4 are all integer matrices. Moreover, X_1 and X_2 have the same integer row and column sum, say k. Consequently, X_3 and X_4 have row and column sum $(t-k)$. Thus we conclude that the set of integer matrices in $tP(G \wr S_2)$ is in bijection with

$$\bigcup_{k=0}^{n} \left(k(P(G) \times P(G)) \cap \mathbb{Z}^{n \times n}\right) \times \left((t-k)(P(G) \times P(G)) \cap \mathbb{Z}^{n \times n}\right),$$

and the result follows. □

Theorem 1.0.21 gives us a method for computing Ehrhart polynomials and hence volumes of permutation polytopes from groups arising as automorphism groups of rooted binary trees. First, given a rooted binary tree T, we compute the automorphism group $\mathrm{Aut}(T)$ as a sequence of direct products and wreath products. Then we read the group $\mathrm{Aut}(T)$ from left to right. If we encounter a direct product, we compute the Ehrhart polynomials of the corresponding groups and take the product of the polynomials. If we encounter a wreath product, we apply Theorem 1.0.21. This produces the Ehrhart polynomial of the permutation polytope associated to the tree T.

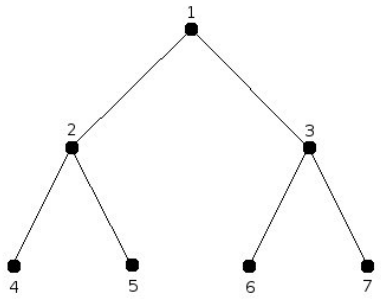

FIGURE 3.1. A rooted binary tree T

EXAMPLE 3.4.2. *Consider the tree T shown in Figure 3.1. Let T_2, T_3 be the subtrees rooted at 2 and 3 respectively. Notice that $Aut(T_2) = Aut(T_3)$ because T is in fact unlabeled (we only place labels to illustrate how to compute the automorphism group). The automorphism group of T is therefore $S_1 \times [(Aut(T_2)) \wr S_2]$. Thus, by Theorem 1.0.21, its Ehrhart*

polynomial is

$$\begin{aligned} i(P(Aut(T)),t) &= i(P(S_1),t)\cdot\left(\sum_{k=0}^{t} i^2(P(Aut(T_2)),k)\cdot i^2(P(Aut(T_2)),t-k)\right)\\ &= 1\cdot\left(\sum_{k=0}^{t}(k+1)^2\cdot(t-k+1)^2\right)\\ &= \sum_{k=0}^{t}(k+1)^2\cdot(t-k+1)^2\\ &= \sum_{k=0}^{t}k^4+(-2t)\sum_{k=0}^{t}k^3+(t^2-2t-2)\sum_{k=0}^{t}k^2+(t^2-1)\sum_{k=0}^{t}k+(t+1)^2\\ &= \frac{1}{30}(t+1)(t+2)(t^2+4t+5). \end{aligned}$$

By Theorem 1.0.18, this is precisely the Ehrhart polynomial of D_4, which we should expect, since $Aut(T)$ is $S_1\times D_4$ up to a relabeling of the generating set of D_4. Moreover, we conclude that the volume of $P(Aut(T))$ is $\frac{1}{30}$.

We can further prove that for any rooted T, $P(\mathrm{Aut}(T))$ has a $P(\mathrm{Aut}(T))$-unimodular regular triangulation.

PROPOSITION 3.4.3. *If T is a rooted tree, then $P(Aut(T))$ has a $P(Aut(T))$-unimodular regular triangulation.*

PROOF. Let T be any rooted tree, and let A_T be its adjacency matrix. Consider the polytope

$$P_T=\left\{X\in[0,1]^{n\times n}\ :\ A_TX=XA_T,\ \ \sum_{j=1}^{n}X_{ij}=1\ \forall i,\ \ \sum_{i=1}^{n}X_{ij}=1\ \forall j\right\}.$$

The integer points of P_T are permutations commuting with A_T, so they are precisely the automorphisms in $\mathrm{Aut}(T)$. Since P_T is integral (see Theorem 2 of [**Tin86**]), this implies that $P_T=P(\mathrm{Aut}(T))$. But by Theorem 1.0.15, P_T is exact, which by Theorem 2.4 of [**Sul06**] and Theorem 4.2 of [**GPT10**] implies that any reverse lexicographic triangulation of $P(\mathrm{Aut}(T))$ is $P(\mathrm{Aut}(T))$-unimodular. Since reverse lexicographic triangulations are regular, the result follows. □

We notice that many classes of permutation polytopes are exact and hence have effectively (and potentially efficiently) computable descriptions as feasible regions of semidefinite programs. This is all due to the power of the theta body hierarchy, and the fact that permutation polytopes arising from subgroups of S_n are subvarieties of $\{0,1\}^{n\times n}$ (see Lemma 1.0.14). In Chapter 4, we investigate the theta body hierarchy when varieties are not necessarily presented by real radical ideals. This allows for an understanding of the theta body hierarchy in a larger context than that of combinatorial optimization, for example, in the context of general polynomial optimization and convex algebraic geometry.

CHAPTER 4

Strong Nonnegativity on Real Varieties

4.1. Strong nonnegativity

We begin with some basic observations on the property of strong nonnegativity (as introduced in the Introduction, see Definition 1.0.25).

PROPOSITION 4.1.1. *Given $f \in A$, we have the following statements.*

(1) *If f is strongly nonnegative at $P \in V_{\mathbb{R}}(I)$, then f is nonnegative at P.*
(2) *If f is strictly positive at $P \in V_{\mathbb{R}}(I)$, then f is strongly nonnegative at P.*
(3) *If f is a sum of squares, then f is strongly nonnegative.*

PROOF. We obtain (1) immediately by setting $m = 1$ in the definition, since this yields the evaluation map at P. For (2), given any homomorphism $\varphi : A \to \mathbb{R}[\epsilon]/(\epsilon^m)$ at P, by definition we have that composing with $\mathbb{R}[\epsilon]/(\epsilon^m) \to \mathbb{R}$ gives the evaluation map at P, under which f is strictly positive by hypothesis. But then if we write $\varphi(f) = a_0 + a_1\epsilon + \cdots + a_{n-1}\epsilon^{n-1}$, we must have $a_0 = f(P) > 0$, and thus $\varphi(f)$ is nonnegative. Since φ was arbitrary at P, we conclude f is strongly nonnegative at P. Finally, for (3) if $f = \sum_{i=1}^{r} h_i^2$, and $\varphi : A \to \mathbb{R}[\epsilon]/(\epsilon^m)$ is an $\mathbb{R}$-algebra homomorphism, then the leading term of each $(\varphi(h_i))^2$ is nonnegative, and hence so is that of $\varphi(f)$. □

We present another example to show the power of our definition and an application of Proposition 4.1.1.

EXAMPLE 4.1.2. *Consider $I = (y - x^2, y^2) \subseteq \mathbb{R}[x, y]$, and $P = (0, 0)$ the only point of $V_{\mathbb{R}}(I)$. Then $-y$ is not strongly nonnegative on $V(I)$: under the homomorphism $\varphi : \mathbb{R}[x, y]/I \to \mathbb{R}[\epsilon]/(\epsilon^3)$ at P sending x to ϵ and y to ϵ^2, we have $\varphi(-y) = -\epsilon^2$ is not nonnegative. But y is strongly nonnegative on $V(I)$ by Proposition 4.1.1 (3) because $y = x^2$ modulo I.*

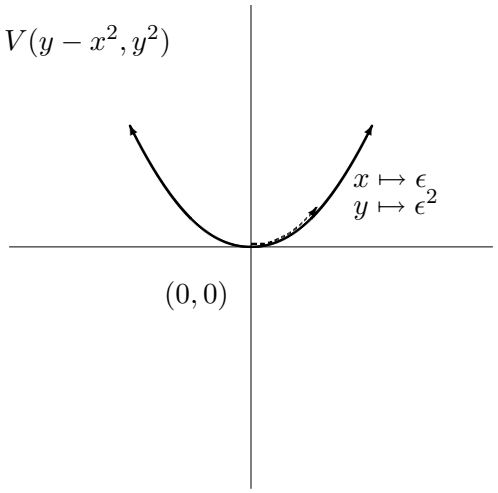

FIGURE 4.1. $-y$ is not strongly nonnegative on $V(y - x^2, y^2)$

We make two observations regarding Proposition 4.1.1. First, a suitable local version of Proposition 4.1.1 (3) may be described in terms of the complete local ring $\hat{A}_P$ of $V(I)$ at P. In particular, if f is a sum of squares in $\hat{A}_P$, then f is strongly nonnegative at P. The proof is the same, since any homomorphism $A \to \mathbb{R}[\epsilon]/(\epsilon^m)$ at P factors through the complete local ring. Though this is potentially advantageous from a theoretical point of view, we stick with our original definition for it has a more likely chance to be effectively computable. Second, we have an immediate test for failure of strong nonnegativity; the existence of a homomorphism $A \to \mathbb{R}[\epsilon]/(\epsilon^m)$ such that the image of f has its leading term in odd degree. Indeed if this is the case, then f is not strongly nonnegative, since we may change the sign of the coefficient by composing with the map from $\mathbb{R}[\epsilon]/(\epsilon^m)$ to itself sending ϵ to $-\epsilon$.

4.2. Nonnegativity on neighborhoods

In this section, we explore the relationship between strong nonnegativity at a point, and nonnegativity in a neighborhood at that point. This requires concepts related to nonsingularity, which for the sake of clarity, we now recall (see Chapter 15.3 of [**DF04**]):

DEFINITION 4.2.1. *Given $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ and $P \in V_{\mathbb{R}}(I)$, set $A = \mathbb{R}[x_1, \ldots, x_n]/I$, and let $\mathfrak{m}_P \subseteq A$ be the maximal ideal of A consisting of polynomials vanishing at P. Note*

*that because $P \in V_{\mathbb{R}}(I)$, we have $A/\mathfrak{m}_P \cong \mathbb{R}$. The **cotangent space** of $V(I)$ at P is the real vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$, and the **tangent space** of $V(I)$ at P is the dual space $\mathrm{Hom}_{\mathbb{R}}(\mathfrak{m}_P/\mathfrak{m}_P^2, \mathbb{R})$. The **dimension** of $V(I)$ at P is the dimension of the local ring $A_{\mathfrak{m}_P}$. Finally, $V(I)$ is **nonsingular** at P if the tangent space at P has dimension equal to the dimension of $V(I)$ at P.*

It will be convenient to extend our terminology as follows:

DEFINITION 4.2.2. *Suppose $P \in V_{\mathbb{R}}(I)$. Then a homomorphism $\varphi : A \to \mathbb{R}[[t]]$ is **at** P if the preimage of the ideal generated by t is the (maximal) ideal of functions vanishing at P.*

In order to establish the equivalence of strong nonnegativity and nonnegativity for nonsingular varieties, we will make repeated use of the following technical lemma, that does not involve strong nonnegativity and applies even in the context of singular varieties. The lemma says that nonnegativity in a real neighborhood of a point P is equivalent to nonnegativity on all *analytic arcs* at P; analytic maps from a small interval $(a, -a)$ for some $a > 0$ sending 0 to P. This is conveyed by part (2). Then, it establishes the equivalence of nonnegativity on all analytic arcs and nonnegativity on all formal arcs; homomorphisms $A \to \mathbb{R}[[t]]$ with nonnegative leading coefficient. We refer the reader to [**Har77**] for algebraic geometry notions in the proof that are not defined here.

LEMMA 4.2.3. *Given $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ a point $P \in V_{\mathbb{R}}(I)$, and $f \in A := \mathbb{R}[x_1, \ldots, x_n]/I$, the following are equivalent:*

(1) *f is nonnegative in a (real) neighborhood of P;*
(2) *for every homomorphism $\varphi : A \to \mathbb{R}[[t]]$ at P taking values in locally convergent power series, we have that the leading term of $\varphi(f)$ is nonnegative.*
(3) *for every homomorphism $\varphi : A \to \mathbb{R}[[t]]$ at P, we have that the leading term of $\varphi(f)$ is nonnegative.*

PROOF. We first show that (1) and (2) are equivalent. The implication that (1) implies (2) is straightforward. Indeed, if $\varphi(f)$ has negative leading term for some φ, then for t_0 sufficiently small and positive, we would have $\varphi(f)(t_0) < 0$, and because

$$\varphi(f)(t_0) = f(\varphi(x_1)(t_0), \ldots, \varphi(x_n)(t_0)),$$

the points $(\varphi(x_1)(t_0), \ldots, \varphi(x_n)(t_0))$ would yield points arbitrarily close to P with f negative.

On the other hand, to prove the converse we apply deep resolution theorems of Hironaka. Suppose that f is not nonnegative on any neighborhood of P. We first observe that it is enough to treat the case that I is real radical, since if $\sqrt[\mathbb{R}]{I}$ is the real radical ideal associated to I, we have $V_{\mathbb{R}}(I) = V_{\mathbb{R}}(\sqrt[\mathbb{R}]{I})$, and if we produce a homomorphism $\mathbb{R}[x_1, \ldots, x_n]/\sqrt[\mathbb{R}]{I} \to \mathbb{R}[[t]]$ at P under which (the image of) f has negative leading term, we obtain the desired map by composing with the canonical quotient map $\mathbb{R}[x_1, \ldots, x_n]/I \to \mathbb{R}[x_1, \ldots, x_n]/\sqrt[\mathbb{R}]{I}$. By a similar argument, we may assume that $V(I)$ is irreducible, since there must be some irreducible component on which P is in the closure of the negative locus of f.

Assuming I is real radical and irreducible, we can then apply resolution of singularities to reduce to the case that $V(I)$ is nonsingular. Indeed, according to Hironaka (Main Theorem 1 of [**Hir64**]), there exists a proper morphism $g : X \to V(I)$ for some nonsingular real variety X, which is an isomorphism above the nonsingular locus of $V(I)$. We claim that if $\tilde{f}$ is the pullback of f under g, there exists $\tilde{P} \in g^{-1}(P)$ such that $\tilde{f}$ is not nonnegative on any neighborhood of $\tilde{P}$. To prove this, we observe that the hypothesis that $V(I)$ is real radical implies that the real nonsingular points are an open dense subset of $V_{\mathbb{R}}(I)$, and it then follows that P is in the closure of the nonsingular real points on which f is negative. Let $\overline{U} \subseteq V_{\mathbb{R}}(I)$ be the closure of a bounded neighborhood of P, hence compact. By the properness of g, we have that $g^{-1}(\overline{U})$ is likewise compact. Now consider the sequence $c_0, c_1, \cdots \in \overline{U}$ of nonsingular points converging to P with $f(c_i) < 0$ for all i. Since g is an isomorphism on nonsingular points, for each i there exists a unique lift $\tilde{c}_i \in X(\mathbb{R})$ with $g(\tilde{c}_i) = c_i$. Moreover, by compactness of $g^{-1}(\overline{U})$ the $\tilde{c}_i$ must have a convergent subsequence; let $\tilde{P}$ be the limit. Then $\tilde{P}$ must be in $g^{-1}(P)$ by continuity, and it is by construction a limit of points on which f is strictly negative, as desired. We may now replace X by an affine neighborhood of $\tilde{P}$, and it is clear that if we have an analytic arc in X at $\tilde{P}$ on which $\tilde{f}$ has negative leading term, then by composing with g we obtain an analytic arc in $V(I)$ at P on which f has negative leading term, so we have reduced to the case that $V(I)$ is nonsingular.

In the process of proving resolution of singularities, Hironaka also proved (Corollary 3 of [**Hir64**]) an imbedded form of resolution of singularities, which implies that in our case, if

we now consider $V(I, f)$ inside of $V(I)$, we can find a proper morphism $g : X \to V(I)$ which is an isomorphism above the complement of $V(I, f)$, and such that if $\tilde{f}$ is the pullback of f under g, we have that $V(\tilde{f})$ is "locally monomial" in X, in the sense that for any $Q \in X$, there exist local coordinates $z_1, \ldots, z_d$ on X at Q, and on some (Zariski) neighborhood of Q, we have $V(\tilde{f})$ equal to the vanishing set of a monomial in the z_i. In particular, $\tilde{f} = u \prod_i z_i^{e_i}$ for some u nonvanishing at Q. Arguing as above, we may replace $V(I)$ by an affine open subset of X, and thus assume that f is locally monomial. Having done this, we further observe that since $u(P) \neq 0$, we either have $u > 0$ in a neighborhood of P, or $u < 0$ in a neighborhood of P, so we may assume that $f = \pm \prod_i z_i^{e_i}$. Note here that replacing u by its sign at 0 will not affect whether a given analytic arc has negative leading term.

Finally, because the z_i are local coordinates, they induce a real analytic isomorphism from a neighborhood of P in $V(I)$ to a neighborhood of 0 in $\mathbb{R}^d$, where $d = \dim V(I)$. Because it is an analytic isomorphism, analytic arcs at 0 in $\mathbb{R}^d$ lift uniquely to analytic arcs at P in $V(I)$, so we have finally reduced to the trivial case that $P = 0$ in $\mathbb{R}^d$, and f is plus or minus a monomial. Clearly, 0 cannot be in the closure of the negative locus if $f = \prod_i z_i^{e_i}$ with all e_i even. If some e_i is odd, we can construct our analytic arc by sending z_i to $-t$ and z_j to t for $j \neq i$. If $f = -\prod_i z_i^{e_i}$, we can send all z_i to t. In either case, we have an analytic arc with negative leading term, as desired.

We now move on to proving the equivalence of (2) and (3). Of course, (3) trivially implies (2). The key ingredient for the converse is an Artin-style approximation theorem. Suppose we have $\varphi : A \to \mathbb{R}[[t]]$ at P such that $\varphi(f)$ has negative leading term. A theorem of Greenberg [**Gre66**] (which is a special case of Artin's approximation theorem) asserts that we can replace φ by a homomorphism φ' which takes values in locally convergent power series and agrees with φ to arbitrarily high order; that is, for any fixed N, we can find φ' such that for all $g \in A$, we have that the first N terms of $\varphi'(g)$ agree with the first N terms of $\varphi(g)$. In particular, we may choose φ' such that $\varphi'(f)$ still has negative leading term, and we thus conclude the desired result. □

This now allows us to establish the proofs of our main theorems.

Proof of Theorem 1.0.26. This is almost immediate from Lemma 4.2.3. Indeed, if f is not nonnegative on any neighborhood of P, the lemma implies that there exists a

homomorphism $A \to \mathbb{R}[[t]]$ under which f has negative leading term. If the leading term occurs in degree $m-1$, truncating from $\mathbb{R}[[t]]$ to $\mathbb{R}[\epsilon]/(\epsilon^m)$ via $t \mapsto \epsilon$ then shows that f is not strongly nonnegative. □

Proof of Theorem 1.0.27. Suppose that f is nonnegative on a neighborhood of P in $V_{\mathbb{R}}(I)$, and $V(I)$ is nonsingular at P. Because nonsingularity is equivalent to smoothness in characteristic 0, by a generalization of Hensel's lemma if we have a homomorphism $\varphi : A \to \mathbb{R}[\epsilon]/(\epsilon^m)$ at P, we can lift to $\mathbb{R}[\epsilon]/(\epsilon^{m'})$ for m' arbitrarily large (see Proposition 2.2.15 and Proposition 2.2.6 of [**BWR90**]). Passing to the limit as m' goes to ∞, we obtain a homomorphism $\widetilde{\varphi} : A \to \mathbb{R}[[t]]$ lifting φ. It follows from Lemma 4.2.3 that $\widetilde{\varphi}(f)$ must either be 0 or have positive leading coefficient, and we thus conclude the same for $\varphi(f)$. Thus, f is strongly nonnegative. □

Example 4.2.4. *The heart of our main theorems lie in Lemma 4.2.3 so we discuss an example in this light. Consider the function $f = y^2 - x^3$ in $\mathbb{R}[x, y]$, with $P = (0, 0)$. Even though the negative locus of f is an open subset containing P in its closure, we have to take a certain amount of care if we wish to directly construct an analytic arc at P which goes into the negative locus of f. Specifically, the tangent vector to the arc must be in the direction of $(1, 0)$. This is in contrast with the behavior after resolution, where we have a great deal of freedom in choosing our analytic arcs.*

To resolve f fully into monomials takes several blowups, but we can already see the geometry after the first blowup, which is represented locally by the map $\mathbb{R}^2 \to \mathbb{R}^2$ sending (s, t) to (s, st). Under this map, the preimage of f is $s^2t^2 - s^3 = s^2(t^2 - s)$. Thus, in the (s, t)-plane we have considerably more leeway in choosing our analytic arc, and in particular any analytic arc with tangent direction of the form (s_0, t_0), with $s_0 > 0$, will do. The reason for the discrepency is that the blowup map $\mathbb{R}^2 \to \mathbb{R}^2$ is not an isomorphism on tangent spaces at the origin; rather, the entire tangent space of the (s, t)-plane at the origin is mapped into the line $y = 0$ in the (x, y)-plane.

In general, the resolution process will take a potentially highly constrained problem (finding an analytic arc inside the negative locus of a function with potentially highly singular zero set), and transform it into a much less constrained problem.

4.3. Obstructions to sums of squares & theta exactness

We now apply the concept of strong nonnegativity to study obstructions to nonnegative functions being sums of squares. We will use the concept of degrees of functions, and consequently from this point on the choice of imbedding of $V(I)$ into affine space becomes relevant. We will need the following definition found in [**GPT10**]:

DEFINITION 4.3.1. [**GPT10**] *Given $d, k \geq 1$, and an ideal $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$, we say that I is (d,k)-**sos** if for every $f \in \mathbb{R}[x_1, \ldots, x_n]$ of degree at most d which is nonnegative on $V_{\mathbb{R}}(I)$, there exist $g_1, \ldots, g_m \in \mathbb{R}[x_1, \ldots, x_n]$ of degree at most k such that*

$$f \equiv \sum_{i=1}^{m} g_i^2 \pmod{I}.$$

Proposition 4.1.1 (3) then immediately implies:

COROLLARY 4.3.2. *Let $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ be an ideal. If there exists a function $f \in A$ of degree less than or equal to d which is nonnegative on $V_{\mathbb{R}}(I)$ but not strongly nonnegative, then I is not (d,k)-sos for any k.*

We now specialize to linear functions, and generalize the obstruction theorem of Gouveia and Netzer (see Theorem 4.5 of [**GN10**]) in Theorem 1.0.29 regarding convex-singular points (see Definition 1.0.28) on varieties. We first make a few observations regarding our generalization of convex singularity. First, in order for this definition to make sense we need a concept of what the tangent space of $V(I)$ at P is, but this is canonically a subspace of the tangent space at P in the ambient affine space $\mathbb{R}^n$, which is identified with $\mathbb{R}^n$ itself. Secondly we comment on the difference between our definition and that given in [**GN10**]. There, they consider tangent space of the real radical $V(\sqrt[\mathbb{R}]{(I)})$, not the tangent space of $V(I)$ itself. As an example, the origin in $\mathbb{R}^2$ is convex-singular in $V(x^2+y^2)$ in our definition, which it should be since the variety consists of $(0,0)$ and vanishes at order higher than 1 there. This example is not convex-singular in the definition in [**GN10**], as the real radical is just (x,y) and the origin vanishes at order 1 there.

PROOF OF THEOREM 1.0.29. We claim that there is a linear function f which is nonnegative on $V_{\mathbb{R}}(I)$, vanishes at P, and induces a nonzero linear function on the tangent space of $V(I)$ at P. In the case that $V_{\mathbb{R}}(I) = \{P\}$, this is trivial: we may take any f whose

zero set contains P but not the tangent space at P. Thus suppose $V_{\mathbb{R}}(I)$ is not a single point. If we choose a sequence of points in the affine hull of $V_{\mathbb{R}}(I)$ but outside $\overline{\text{conv}(V_{\mathbb{R}}(I))}$ converging to P, the Separation Theorem (Theorem III.1.3 in [**Bar02**]) gives us a sequence of linear functions on the affine hull, nonnegative on $V_{\mathbb{R}}(I)$ and negative on the points in our sequence. Taking a suitable limit of these (rescaling as necessary) gives a nonzero linear function $\bar{f}$ on the affine hull, nonnegative on $V_{\mathbb{R}}(I)$, and with $\bar{f}(P) = 0$. We then have that $\bar{f}$ must be strictly positive on the relative interior of $V_{\mathbb{R}}(I)$. Choose f to be any lift of $\bar{f}$ to a linear function on $\mathbb{R}^n$. Now, since f is linear it induces the same function on the tangent space to $\mathbb{R}^n$ at P, and by hypothesis there is a tangent vector to $V(I)$ at P in the locus where f is positive, so we see that the induced function on the tangent space is nonzero, completing the proof of the claim.

Now, because f induces a nonzero linear function on the tangent space, there is a tangent vector on which f is negative, and this corresponds to a homomorphism $\varphi : A \to \mathbb{R}[\epsilon]/(\epsilon^2)$ sending f to a negative multiple of ϵ. Thus, f is not strongly nonnegative. By Corollary 1.0.30, we have that f is not a sum of squares, and hence I is not $(1, k)$-sos for any k. □

Hypersurfaces present a particularly nice case of the theorem.

COROLLARY 4.3.3. *Suppose $I = (g)$ is principal in $\mathbb{R}[x_1, \ldots, x_n]$, and suppose $P \in V_{\mathbb{R}}(I)$ is a singularity lying on the boundary of* $\text{conv}(V_{\mathbb{R}}(I))$. *Then I is not $(1, k)$-sos for any k.*

PROOF. The variety $V(I)$ has codimension one, so the tangent space at the singular point 0 is all of $\mathbb{R}^n$. Thus, P is convex-singular, and we conclude the desired result from Theorem 1.0.29. □

We now illustrate some examples regarding convex-singular varieties. Our first example also illustrates that strong nonnegativity has limitations in its ability to recognize functions which are not sums of squares. For instance, the functions $f = x + a$ with $a > 0$ are all strictly positive on the variety in Example 4.3.4 and hence strong nonnegative, but still not a sum of squares.

EXAMPLE 4.3.4. *Consider the ideal $I = (y^2 - x^3) \subseteq \mathbb{R}[x, y]$, and the function $f(x, y) = x$ nonnegative on $V_{\mathbb{R}}(I)$. The singular point $P = (0, 0)$ of $V(I)$ lies on the boundary of* $\text{conv}(V_{\mathbb{R}}(I))$, *so by Corollary 4.3.3 we have that I is not $(1, k)$-sos for any k. We may see the argument explicitly as follows. Note that $f(x, y)$ is negative on the direction $(-1, 0)$ at*

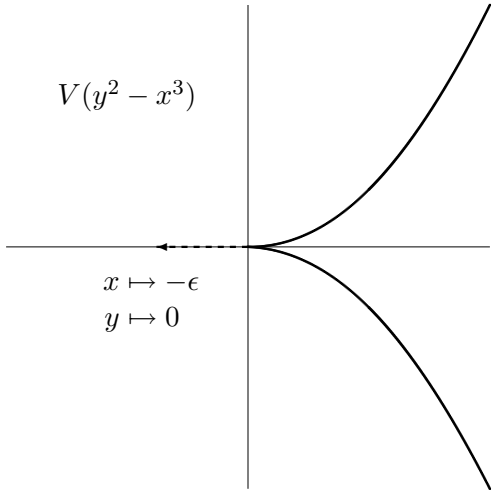

FIGURE 4.2. The negative direction $(-1, 0)$ at $(0, 0)$ on $V(y^2 - x^3)$

the singular point $(0, 0)$ *of* $V(I)$*. This is realized algebraically by the homomorphism*

$$\varphi : \mathbb{R}[x, y]/(y^2 - x^3) \to \mathbb{R}[\epsilon]/(\epsilon^2), \quad \varphi(x) = -\epsilon \quad \varphi(y) = 0,$$

at P*, which proves* f *is not strongly nonnegative since the leading coefficient of* $\varphi(f) = \varphi(x) = -\epsilon$ *is negative. Thus,* f *cannot be a sum of squares. This example may be made compact by instead setting* $I = (y^2 - x^3 + x^4)$*.*

However, we also see that Corollary 4.3.2 works more generally than for convex singularities. Indeed, convex singularities may be viewed as causing strong nonnegativity to fail at first order, while the general definition requires examining all orders.

EXAMPLE 4.3.5. *Consider the ideal* $I = (y^2 - x^5, z - x^3) \subseteq \mathbb{R}[x, y, z]$*, and the function* $f(x, y, z) = z$ *nonnegative on* $V_{\mathbb{R}}(I)$*. The only singular point of* $V(I)$ *is* $P = (0, 0, 0)$*, and the tangent space to* $V(I)$ *at* P *is precisely the plane* $z = 0$*, so* P *is not a convex singularity. However,* $V(I)$ *has higher-order infinitesimal arcs pointing into the negative direction of* z*, for instance given by the homomorphism*

$$\varphi : \mathbb{R}[x, y, z]/(y^2 - x^5, z - x^3) \to \mathbb{R}[\epsilon]/(\epsilon^4), \quad \varphi(x) = -\epsilon \quad \varphi(y) = 0, \quad \varphi(z) = -\epsilon^3$$

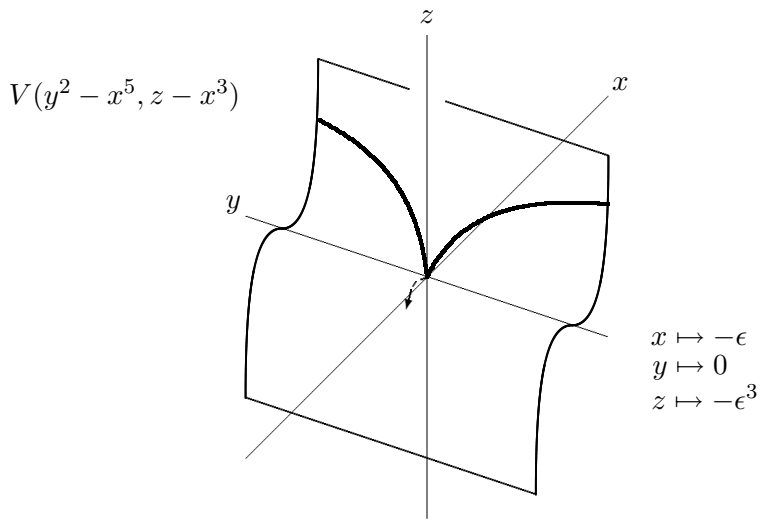

FIGURE 4.3. A higher-order infinitesimal arc on $V(y^2 - x^5, z - x^3)$ pointing in the negative direction.

at P. Once again, we see that f is not strongly nonnegative, and we conclude by Corollary 4.3.2 that I is not TH_k-exact for any k. This example may also be made compact, by setting $I = (y^2 - x^5 + x^6, z - x^3)$.

Concerning the compact versions of the above examples, the celebrated Schmüdgen's Positivstellensatz implies (see Corollary 3 of [**Sch91**]) that if $V_{\mathbb{R}}(I)$ is compact and f is strictly positive, then f is a sum of squares. Since strong nonnegativity lies between nonnegativity and strict positivity, it is natural to wonder if a strongly nonnegative function is a sum of squares when $V_{\mathbb{R}}(I)$ is compact. The following example shows that this is not the case.

EXAMPLE 4.3.6. *Let $I = (x_1^2 + \cdots + x_n^2 - 1) \subset \mathbb{R}^n$, with $n \geq 4$. According to Theorem 2.6.3 of* [**Mur08**]*, there exists a polynomial function f which is nonnegative on $V_{\mathbb{R}}(I)$ but not a sum of squares modulo I. Since $V(I)$ is nonsingular, we have by Theorem 1.0.27 that f is strongly nonnegative on $V(I)$. Of course, we want examples that are linear for the purposes of overarching theory. This example can be modified to do so by adding an auxiliary variable y, and add to I the relation $y = f$, so that the resulting coordinate rings are isomorphic. Then y is strongly nonnegative, but is not a sum of squares modulo I.*

We now present obstructions to theta exactness in the context of strong nonnegativity. We first visit some theory developed in [**GPT10**]. The key to their theory is the relationship between TH_k-exactness of an ideal, and the ideal being $(1,k)$-sos. They establish the following:

LEMMA 4.3.7. *(see Corollary 2.12 of* [**GPT10**]*) Let $I \subseteq \mathbb{R}[x_1,\dots,x_n]$ be an ideal. If I is $(1,k)$-sos then I is TH_k-exact. Moreover, if I is real radical, then I is $(1,k)$-sos if and only if I is TH_k-exact.*

Lemma 4.3.7, together with our results on obstructions to an ideal being $(1,k)$-sos, immediately establish Corollary 1.0.30. Moreover, the obstruction theorem of Gouveia and Netzer as they stated it is equivalent to the following:

THEOREM 4.3.8. *Suppose we have $I \subseteq \mathbb{R}[x_1,\dots,x_n]$, and $P \in V_{\mathbb{R}}(I)$ is a convex-singular point of $V(\sqrt[\mathbb{R}]{I})$, where $\sqrt[\mathbb{R}]{I}$ is the real radical ideal associated to I. Then I is not TH_k-exact for any k.*

PROOF. We conclude from Theorem 1.0.29 that $\sqrt[\mathbb{R}]{I}$ is not $(1,k)$-sos, and thus Theorem 4.3.7 implies that $\sqrt[\mathbb{R}]{I}$ is not TH_k-exact. Since $TH_k(\sqrt[\mathbb{R}]{I}) \subseteq TH_k(I)$, we conclude the desired statement. □

Similarly, we conclude:

COROLLARY 4.3.9. *Suppose $I = (g)$ is principal and real radical in $\mathbb{R}[x_1,\dots,x_n]$, and suppose $P \in V_{\mathbb{R}}(I)$ is a singularity lying on the boundary of* $\operatorname{conv}(V_{\mathbb{R}}(I))$*. Then I is not TH_k-exact for any k.*

As before, Example 4.3.5 gives an example in which Corollary 1.0.30 goes further than Theorem 4.3.8; indeed, in this case the ideal is real radical, so we conclude that it is not TH_k-exact for any k.

4.4. A new sum of squares condition

We conclude with our new sums of squares condition for theta exactness in terms of weakly $(1,k)$-sos ideals, in particular proving Proposition 1.0.32 and Corollary 1.0.33. This key point is that, despite the fact that being weakly $(1,k)$-sos relaxes the notion of being

$(1,k)$-sos, it still implies TH_k-exactness. We note that in fact, Corollary 1.0.33 follows immediately from Theorem 4.3.7 and Proposition 1.0.32.

PROOF OF PROPOSITION 1.0.32. Let $P \in \mathbb{R}^n$ such that $P \notin \overline{\text{conv}(V_{\mathbb{R}}(I))}$. By the Separation Theorem, there is a linear polynomial f such that f is nonnegative on $\text{conv}(V_{\mathbb{R}}(I))$ and $f(P) < 0$. Consider the linear function $g = f - \frac{f(P)}{2}$. We have $g(P) < 0$, and g is *positive* on $\overline{\text{conv}(V_{\mathbb{R}}(I))}$ and hence positive on $V_{\mathbb{R}}(I)$. This implies g is strongly nonnegative by Proposition 4.1.1 (2), and g is then a sum of squares of polynomials of degree at most k by hypothesis. Since P was arbitrary outside $\overline{\text{conv}(V_{\mathbb{R}}(I))}$, the result follows. □

We created strong nonnegativity with the aim of generalizing the condition $(1,k)$-sos condition in Lemma 4.3.7 with a weaker condition (our weakly $(1,k)$-sos condition) so that Lemma 4.3.7 would hold in the general case of real radical ideals, but we still do not know whether for general ideals, $(1,k)$-sos and TH_k-exact ideals are one in the same. We suspect that there are examples of TH_k-exact but not weakly $(1,k)$-sos ideals. If so, one place to look is at ideals I whose complex varieties $V_{\mathbb{C}}(I)$ are arbitrarily complicated, but whose real varieties $V_{\mathbb{R}}(I)$ are empty. In this case, the Positivstellensatz (2.2.1 of [**Mur08**]) tells us that -1 is sos mod I, and so we automatically get all linear polynomials (in fact all polynomials) are sos mod I.

CHAPTER 5

Future Directions & Open Questions

5.1. Nonlinear Algebraic Graph Theory

We now discuss future directions and open problems on the Nullstellensatz Linear Algebra algorithm applied to k-colorability. Our main result,Theorem 1.0.3, establishes a combinatorial characterization of non-3-colorable graphs with degree 1 Nullstellensatz certificates. One could consider a few natural directions to extend this work, if tackling colorability using the model as Proposition 1.0.1. Likely the most natural problem is

PROBLEM 5.1.1. *Characterize those graphs with a given k-colorability Nullstellensatz certificate of degree D.*

This problem seems quite complicated because the linear algebra systems in the Nullstellensatz Linear Algebra algorithm grow exponentially with D. However, employing software to handle large scale linear algebra systems might be effective in conjecturing the combinatorial obstructions to 3-colorability illuminated by degree D certificates. Another natural direction to consider is to ask for obstructions to degree 1 Nullstellensatz certificates for k-colorability when $k > 3$. However, evidence shows that the behavior here is quite erratic (see [**DLLMM08**]). Finally, one can consider changing the base field to compute with. In our investigation of 3-colorability, we restricted ourselves to working with the simplest field, $\mathbb{F}_2$, because of its simple algebraic properties and easy computational encoding. However, it would be of great interest to investigate certificates over other fields, as they may lead to combinatorial obstructions not apparent by $\mathbb{F}_2$ certificates.

Our algebraic encoding of Hamiltonicity provides a rich computational framework in which to investigate important graph theoretic conjectures systematically. For instance, recall the following conjecture of Sheehan ([**She75**]):

CONJECTURE 5.1.2. *Let G be a simple r-regular graph with $r > 2$. Then G is not uniquely Hamiltonian.*

In fact, by Petersen's Theorem ([**Die10**]), it suffices to prove this theorem in the case $r = 4$. To begin this problem, one could use software and compute Gröbner bases of the ideal H_G to understand its structure better. With this, one could see if for various famous families of 4-regular graphs (for instance, strongly regular ones), that the structure of H_G allows or forbids it from taking on the form of an ideal $H_{G,C}$ for some cycle C. This would hinge on computational investigations involving Theorem 1.0.8 and Corollary 1.0.9.

Finally we address using the theta body hierarchy to approach the problem of determining if a graph has trivial automorphism group. As we established in Theorem 1.0.15, the class of exact graphs are more fruitful to investigate for the graph automorphism problem than classes of compact graphs investigated by Tinhofer. However, there is one important computational fact here that needs to be addressed. Recall in the discussion after Lemma 1.0.14 that in order to describe the first theta body of I_G as the feasible region of a semidefinite program, one needs to determine a basis for the quotient ring $\mathbb{R}[P_{11}, P_{12}, \ldots, P_{nn}]/I_G$. A natural question in this light is:

QUESTION 5.1.3. *For which graphs G does $\mathbb{R}[P_{11}, P_{12}, \ldots, P_{nn}]/I_G$ have an $\mathbb{R}$-vector space basis that be computed in polynomial time in n?*

One might suspect Problem 5.1.3 to be very difficult in general. One reason is that traditional methods for exploring such problems involve computing Gröbner basis, and algorithms related to this are notoriously computationally inefficient in general. More critically, such methods only work over polynomial rings with coefficients in an algebraically closed field, however since our ideals here are finite we can investigate methods developed in [**LLR08**]. Though perhaps the best evidence is that by our analysis in Chapter 2, an algorithm that efficiently computes a basis for the quotient would solve the graph automorphism problem, which is one of the most notoriously difficult problems to decide the complexity of. However, one could restrict attention to particularly important families of graphs for which I_G has potentially special structure allowing the computation of a basis for the quotient to be easy. One place to start in this direction is to find methods for efficiently computing a basis for the quotient for families of graphs that are known to have polynomial time graph automorphism algorithms. One such family is trees (see [**CG97, Tin86**]).

PROBLEM 5.1.4. *Determine a polynomial time algorithm for computing an $\mathbb{R}$-vector space basis for $\mathbb{R}[P_{11}, P_{12}, \ldots, P_{nn}]/I_G$ when G is a tree.*

5.2. Permutation Polytopes

Many interesting directions and questions arise from our study of permutation polytopes. We begin by discussing linear inequality and semidefinite descriptions of these polytopes. As we mentioned in the introduction, determining linear inequality descriptions for permutation polytopes is hard in general, even for the particular case of the convex hull of even permutation matrices. In our study, we showed that for cyclic groups, dihedral groups, Frobenius groups, and groups arising from automorphism groups of tree graphs, polynomial inequality descriptions for their associated permutation polytopes are possible because they are exact (and moreover, this leads to rich convex geometric properties). These groups are only the tip of the iceberg. Having a complete understanding of which groups have permutation polytopes that are TH_k-exact is one interesting direction to pursue in determining polynomial inequality descriptions of these polytopes.

PROBLEM 5.2.1. *Give a group theoretic characterization of the graphs G for which $P(G)$ is TH_k-exact.*

Another interesting direction is the computation of volumes and Ehrhart polynomials. Our methods focused on the application of Gale duality because for cyclic, dihedral and Frobenius groups, the Gale duals are quite manageable. However, for general groups, this may not be the case, so other methods are preferable. Formulas for the volumes, relativel volumes of faces and Ehrhart polynomials for the Birkhoff polytopes B_n were computed by De Loera, Liu and Yoshida [**DLLY09**]. Here, they use rational generating functions and techniques of Brion and Barvinok (see [**BP99**]) to explicitly find these formulas. However, for B_n, this formulas are generally computational ineffective. Of course, this leads to the natural question:

QUESTION 5.2.2. *For which groups G do the tools in* [**DLLY09**] *work effectively for computing volumes, relative volumes of faces and Ehrhart polynomials?*

Every permutation polytope is a subpolytope of some Birkhoff polytope B_n, so in a sense we can think of the polytopes B_n act as our universal symmetric objects of study.

However, there are many interesting highly symmetric polytopes that also come from group actions. One particular well studied example is the permutohedron.

DEFINITION 5.2.3. *(see Section 1 of* [**Pos09**]*) Let* $(x_1, x_2, \ldots, x_{n+1}) \in \mathbb{R}^{n+1}$*. The* permutohedron $P_n(x_1, x_2, \ldots, x_{n+1})$ *is the polytope defined by*

$$P(x_1, x_2, \ldots, x_{n+1}) = conv\left\{(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n+1)}) \ : \ \sigma \in S_{n+1}\right\}.$$

In his seminal paper [**Pos09**], Postnikov determines formulas and generating functions for volumes and counting integer points in permutohedra, and more generally convex hulls $P_W(x) = conv(\{w(x) \mid w \in W\}) \subset \mathbb{R}^{n+1}$ where W is an arbitrary Weyl group. More generally, many researchers have studied the convex hull $conv(G \cdot x) = conv(g \cdot x \mid g \in G)$ for an *arbitrary* group G that acts on $\mathbb{R}^n$. Such polytopes are called *orbitopes* and appear throughout literature (see [**SFB11**] for a review on this). Motivated by our study of permutation polytopes, we are interested in studying orbitopes where G is in fact a subgroup of S_n.

PROBLEM 5.2.4. *Determine facets, volumes, and theta ranks of orbitopes associated to subgroups of* S_n*.*

In [**Pos09**], Postnikov shows that there is a natural projection from B_n onto the permutohedron $P_n(1, 2, \ldots, n+1)$. This projection, combined with our developments in Chapter 3, may give us insight on how to solve Problem 5.2.4 when the group in question is, for instance, a Frobenius group.

5.3. Theta Bodies & Convex Hulls of Varieties

There are a few very important questions that arise from Chapter 4. The first is addressing the effectiveness of our definition of nonnegativity. Recall from Definition 1.0.25 that strong nonnegativity of f at a point P in $V_{\mathbb{R}}(I)$ requires checking that the lowest degree coefficient of every homomorphism $A \to \mathbb{R}[\epsilon]/(\epsilon^m)$ for every m is nonnegative (or the image of f is 0). Checking such a condition seems quite daunting at first, so we ask the question of checking this condition for fixed m. This motivates the following definition:

DEFINITION 5.3.1. *Let $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ be an ideal. Given $P \in V_{\mathbb{R}}(I)$, we say $f \in A$ is **M-strongly nonnegative at** P if for every $m \leq M$ and for every $\mathbb{R}$-algebra homomorphism*

$$\varphi : A \to \mathbb{R}[\epsilon]/(\epsilon^m)$$

*at P, we have $\varphi(f)$ is nonnegative in $\mathbb{R}[\epsilon]/(\epsilon^m)$ (in the sense of Definition 1.0.24). We say f is **M-strongly nonnegative** on $V(I)$ if it is strongly nonnegative at P for all $P \in V_{\mathbb{R}}(I)$. We denote the set of functions $f \in A$ that are $M - strongnonnegative$ by $SN_I(M)$.*

Notice that the 1-strongly nonnegative functions on the real variety $V_{\mathbb{R}}(I)$ are simply the functions that are nonnegative on $V_{\mathbb{R}}(I)$. A natural first question is then

QUESTION 5.3.2. *Let $I \in \mathbb{R}[x_1, \ldots, x_n]$ be an ideal, and $f \in A$. Is there an algorithm to test if f is in $SN_I(2)$? $SN_I(3)$? $SN_I(M)$ for larger M?*

Observe moreover that for a given ideal I, the family of functions $SN_I(M)$ form a hierarchy

$$\{\text{non-negative functions on } I\} = SN_I(1) \supseteq SN_I(2) \supseteq \cdots \supseteq SN_I(M) \supseteq \cdots .$$

A curious question is to understand how much these families of functions differ from each other. For instance, one could ask

QUESTION 5.3.3. *For a given ideal $I \subset \mathbb{R}[x_1, \ldots, x_n]$, how can one characterize the functions in $SN_I(M)$ not in $SN_I(M+1)$? for a given M?*

Finally, we address the relationship between theta body convergence and strong nonnegativity. Perhaps the most pertinent question in this light stems from our original motivation.

QUESTION 5.3.4. *Is there an ideal I that is TH_k-exact but not weakly $(1,k)$-sos?*

We believe this question is very tangible but have not yet constructed a particular example. We suspect that understanding the computational techniques to address questions (5.3.2) and (5.3.3) may shed light on how to construct such an ideal if one exists.

APPENDIX A

Appendix

A.1. Miscellaneous Permutation Polytopes

In this section, we study miscellaneous permutation polytopes. We begin by proving Proposition 1.0.22. This proposition shows the difficulty of dealing with general permutation polytopes, in the context of finding complete facet descriptions, or even descriptions as spectrahedra.

Proof of Proposition 1.0.22. Since $P(A_2)$ and $P(A_3)$ have one and three vertices respectively, they are trivially two-level. Since A_4 is a Frobenius group, Proposition 1.0.20 implies that $P(A_4)$ is two-level. For $n \geq 5$, by choosing $(\sigma, t, h) = (e, 1, 2)$ as in Theorem 3 of [**CW04**], we deduce that $P(A_n)$ has the facet defining inequality $\ell(x) \leq n-2$, where $\ell(x) = \sum_{j=3}^{n} x_{j,j} + \sum_{j=3}^{n} x_{j,1} + \sum_{j=3}^{n} x_{1,j}$. Now $\ell(e) = n-2$, $\ell((1\ 2)(4\ 5)) = n-4$, and $\ell((3\ 4\ 5)) = n-5$, and hence $P(A_n)$ is not two-level for $n \geq 5$. To show that $P(A_n)$ is at least $(\lfloor \frac{n}{4} \rfloor + 1)$-level for $n \geq 8$, we evaluate ℓ on σ_i, where $\sigma_0 = e$ and $\sigma_k = (1\ 2)(3\ 4)\cdots(4k-1\ 4k)$ for $1 \leq k \leq \lfloor \frac{n}{4} \rfloor$. In particular, we notice that $\ell(\sigma_k) = n - 4k$, and hence $P(A_n)$ is at least $(\lfloor \frac{n}{4} \rfloor + 1)$-level. □

We conclude with a list of subgroups of S_3, S_4, and S_5 and some their Ehrhart polynomials. Two groups stand out as incomplete, the alternating group A_5 and the general affine group of degree one over the field of five elements. The latter group is generated by taking the semidirect product of the additive and multiplicative groups of the field of five elements, and is denoted by $GA(1, 5)$.

Subgroups of S_3			
Order	Generators	Dim	Ehrhart Polynomial
1	$< e > \cong \{e\}$	0	1
2	$< (1\ 2) > \cong C_2$	1	$t+1$
3	$< (1\ 2\ 3) > \cong C_3$	2	$\frac{1}{2}t^2+\frac{3}{2}t+1$
6	$< (1\ 2), (1\ 3), (2\ 3) > \cong S_3$	4	$\frac{1}{8}t^4+\frac{3}{4}t^3+\frac{15}{8}t^2+\frac{9}{4}t+1$
Subgroups of S_4			
Order	Group	Dim	Ehrhart Polynomial
1	$< e > \cong \{e\}$	0	1
2	$< (1\ 2) > \cong C_2$	1	$t+1$
2	$< (1\ 2)(3\ 4) > \cong C_2$	1	$t+1$
3	$< (1\ 2\ 3) > \cong C_3$	2	$\frac{1}{2}t^2+\frac{3}{2}t+1$
4	$< (1\ 2), (3\ 4) > \cong C_2 \times C_2$	2	t^2+2t+1
4	$< (1\ 2)(3\ 4), (1\ 3)(2\ 4) > \cong C_2 \times C_2$	3	$\frac{1}{6}t^3+t^2+\frac{11}{6}t+1$
4	$< (1\ 2\ 3\ 4) > \cong C_4$	3	$\frac{1}{6}t^3+t^2+\frac{11}{6}t+1$
6	$< (1\ 2), (1\ 3), (2\ 3) > \cong S_3$	4	$\frac{1}{8}t^4+\frac{3}{4}t^3+\frac{15}{8}t^2+\frac{9}{4}t+1$
8	$< (1\ 2\ 3\ 4), (1\ 2)(3\ 4) > \cong D_4$	5	$\frac{1}{30}t^5+\frac{1}{3}t^4+\frac{4}{3}t^3+\frac{8}{3}t^2+\frac{79}{30}t+1$
12	$< (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4),\ (2\ 3\ 4) > \cong A_4$	9	$\frac{1}{5670}t^9+\frac{1}{504}t^8+\frac{23}{1890}t^7+\frac{1}{15}t^6+\frac{173}{540}t^5+\frac{9}{8}t^4+\frac{29797}{11340}t^3+\frac{1199}{315}t^2+\frac{383}{126}t+1$
24	$< (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4) > \cong S_4$	9	$\frac{11}{11340}t^9+\frac{11}{630}t^8+\frac{19}{135}t^7\frac{2}{3}t^6+\frac{1109}{540}t^5+\frac{43}{10}t^4+\frac{35117}{5670}t^3+\frac{379}{63}t^2+\frac{65}{18}t+1$
Subgroups of S_5			
Order	Generators	Dim	Ehrhart Polynomial
1	$< e > \cong \{e\}$	0	1
2	$< (1\ 2) > \cong C_2$	1	$t+1$
2	$< (1\ 2)(3\ 4) > \cong C_2$	1	$t+1$
3	$< (1\ 2\ 3) > \cong C_3$	2	$\frac{1}{2}t^2+\frac{3}{2}t+1$
4	$< (1\ 2), (3\ 4) > \cong C_2 \times C_2$	2	t^2+2t+1
4	$< (1\ 2)(3\ 4), (1\ 3)(2\ 4) > \cong C_2 \times C_2$	3	$\frac{1}{6}t^3+t^2+\frac{11}{6}t+1$
4	$< (1\ 2\ 3\ 4) > \cong C_4$	3	$\frac{1}{6}t^3+t^2+\frac{11}{6}t+1$
5	$< (1\ 2\ 3\ 4\ 5) > \cong C_5$	4	$\frac{1}{24}t^4+\frac{5}{12}t^3+\frac{35}{24}t^2+\frac{25}{12}t+1$
6	$< (1\ 2\ 3)(4\ 5) > \cong C_6$	3	$\frac{1}{2}t^3+2t^2+\frac{5}{2}t+1$
6	$< (1\ 2), (2\ 3), (1\ 3) > \cong S_3$	4	$\frac{1}{8}t^4+\frac{3}{4}t^3+\frac{15}{8}t^2+\frac{9}{4}t+1$
6	$< (1\ 2)(4\ 5), (1\ 3)(4\ 5), (2\ 3)(4\ 5) > \cong S_3$	5	$\frac{1}{40}t^5+\frac{1}{8}t^4+\frac{5}{8}t^3+\frac{15}{8}t^2+\frac{47}{20}t+1$
8	$< (1\ 2\ 3\ 4), (1\ 2)(3\ 4) > \cong D_4$	5	$\frac{1}{30}t^5+\frac{1}{3}t^4+\frac{4}{3}t^3+\frac{8}{3}t^2+\frac{79}{30}t+1$
10	$< (1\ 2\ 3\ 4\ 5), (2\ 5)(3\ 4) > \cong D_5$	8	$\frac{1}{8064}t^8+\frac{5}{2016}t^7+\frac{5}{192}t^6+\frac{25}{144}t^5+\frac{95}{128}t^4+\frac{575}{288}t^3+\frac{6515}{2016}t^2+\frac{475}{168}t+1$
12	$< (1\ 2\ 3)(4\ 5), (1\ 2)(4\ 5) > \cong D_6$	5	$\frac{1}{8}t^5+\frac{7}{8}t^4+\frac{21}{8}t^3+\frac{33}{8}t^2+\frac{13}{4}t+1$
12	$< (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4),\ (2\ 3\ 4) > \cong A_4$	9	$\frac{1}{5670}t^9+\frac{1}{504}t^8+\frac{23}{1890}t^7+\frac{1}{15}t^6+\frac{173}{540}t^5+\frac{9}{8}t^4+\frac{29797}{11340}t^3+\frac{1199}{315}t^2+\frac{383}{126}t+1$
24	$< (1\ 2),\ (1\ 3), (1\ 4),\ (2\ 3), (2\ 4),\ (3\ 4) > \cong S_4$	9	$\frac{11}{11340}t^9+\frac{11}{630}t^8+\frac{19}{135}t^7+\frac{2}{3}t^6+\frac{1109}{540}t^5+\frac{43}{10}t^4+\frac{35117}{5670}t^3+\frac{379}{63}t^2+\frac{65}{18}t+1$
120	$< (1\ 2), (1\ 3), (1\ 4), (1\ 5), (2\ 3), (2\ 4), (2\ 5), (3\ 4),$ $(3\ 5), (4\ 5) > \cong S_5$	16	$\frac{188723}{836911595520}t^{16}+\frac{188723}{20922789888}t^{15}+\frac{1008757}{5977939968}t^{14}+\frac{112655}{57480192}t^{13}+$ $\frac{72750523}{4598415360}t^{12}+\frac{984101}{10450944}t^{11}+\frac{125188639}{292626432}t^{10}+\frac{55426325}{36578304}t^9+$ $\frac{3541860299}{836075520}t^8+\frac{196563587}{20901888}t^7+\frac{3812839477}{229920768}t^6+\frac{664118435}{28740096}t^5+$ $\frac{438177965089}{17435658240}t^4+\frac{3028287247}{145297152}t^3+\frac{6229735}{494208}t^2+\frac{725}{144}t^1+1$

Bibliography

[AB95] J. L. Alperin and R. B. Bell, *Groups and representations*, Graduate Texts in Mathematics, vol. 162, Springer-Verlag, New York, 1995.

[AF96] D. Avis and K. Fukuda, *Reverse search for enumeration*, Discrete Appl. Math. **65** (1996), no. 1-3, 21–46, First International Colloquium on Graphs and Optimization (GOI), 1992 (Grimentz).

[Alo99] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29, Recent trends in combinatorics (Mátraháza, 1995).

[AT92] N. Alon and M. Tarsi, *Colorings and orientations of graphs*, Combinatorica **12** (1992), no. 2, 125–134.

[Bar02] A. I. Barvinok, *A course in convexity*, Graduate Studies in Mathematics, vol. 54, American Mathematical Society, Providence, RI, 2002.

[Bay82] D. Bayer, *The Division Algorithm and the Hilbert Scheme*, Ph.D. thesis, Harvard University, 1982.

[BG77] R. A. Brualdi and P. M. Gibson, *Convex polyhedra of double stochastic matrices. II. Graph of U_n*, J. Combinatorial Theory Ser. B **22** (1977), no. 2, 175–198.

[BHNP09] B. Baumeister, C. Haase, B. Nill, and A. Paffenholz, *On permutation polytopes*, Adv. Math. **222** (2009), no. 2, 431–452.

[BL91] R. A. Brualdi and B. L. Liu, *The polytope of even doubly stochastic matrices*, J. Combin. Theory Ser. A **57** (1991), no. 2, 243–253.

[BP72] E. Balas and M. Padberg, *On the set-covering problem*, Operations Res. **20** (1972), 1152–1161.

[BP99] A. I. Barvinok and J. E. Pommersheim, *An algorithmic theory of lattice points in polyhedra*, New Perspectives in Algebraic Combinatorics (L. J. Billera, A. Björner, C. Greene, R. E. Simion, and R. P. Stanley, eds.), Math. Sci. Res. Inst. Publ., vol. 38, Cambridge Univ. Press, Cambridge, 1999, pp. 91–147.

[BP03] M. Beck and D. Pixton, *The Ehrhart polynomial of the Birkhoff polytope*, Discrete Comput. Geom. **30** (2003), no. 4, 623–637.

[BR07] M. Beck and S. Robins, *Computing the continuous discretely*, Undergraduate Texts in Mathematics, Springer, New York, 2007, Integer-point enumeration in polyhedra.

[Bru88] R. A. Brualdi, *Some applications of doubly stochastic matrices*, Linear Algebra Appl. **107** (1988), 77–100.

[BWR90] S. Bosch, L. W., and M. Raynaud, *Néron models*, vol. 21, Springer-Verlag Berlin, 1990.

[Cam01] K. Cameron, *Thomason's algorithm for finding a second hamiltonian circuit through a given edge in a cubic graph is exponential on krawczyk's graphs*, Discrete Math. **235** (2001), no. 1-3, 69–77, Combinatorics (Prague, 1998).

[Cam04] P. G. Cameron, *Automorphisms of graphs*, Topics in Algebraic Graph Theory (L. W. Beineke and R. J. Wilson, eds.), Cambridge Univ. Press, 2004, pp. 203–221.

[CEI96] M. Clegg, J. Edmonds, and R. Impagliazzo, *Using the Groebner basis algorithm to find proofs of unsatisfiability*, STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (New York, New York, USA), ACM, 1996, pp. 174–183.

[CG97] A. Chan and C. Godsil, *Graph symmetry: Algebraic methods and applications*, ch. 4, pp. 75–106, Kluwer Academic Publishers, Montréal, QC, Canada., 1997.

[CKPS00] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, Advances in cryptology—EUROCRYPT 2000 (Bruges) (Berlin), Lecture Notes in Comput. Sci., vol. 1807, Springer, 2000, pp. 392–407.

[CLO07] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, 3 ed., Undergraduate Texts in Mathematics, Springer, 2007, An introduction to computational algebraic geometry and commutative algebra.

[CM09] E. R. Canfield and B. D. McKay, *The asymptotic volume of the Birkhoff polytope*, Online J. Anal. Comb. (2009), no. 4, Art. 2, 4.

[CP10] J. Collins and D. Perkinson, *Frobenius polytopes*, Available at http://arxiv.org/abs/1102.0988, 2010.

[CR99] C. S. Chan and D. P. Robbins, *On the volume of the polytope of doubly stochastic matrices*, Experiment. Math. **8** (1999), no. 3, 291–300.

[CW04] W. Cunningham and Y. Wang, *On the even permutation polytope*, Linear Algebra and its Applications **381** (2004), 269–281.

[DF04] D. Dummit and R. M. Foote, *Abstract algebra*, 3 ed., John Wiley & Sons Inc., 2004.

[DG95] P. Diaconis and A. Gangolli, *Rectangular arrays with fixed margins*, Discrete probability and algorithms (Minneapolis, MN, 1993), IMA Vol. Math. Appl., vol. 72, Springer, New York, 1995, pp. 15–41.

[Die10] R. Diestel, *Graph theory*, fourth ed., Graduate Texts in Mathematics, vol. 173, Springer, Heidelberg, 2010.

[DL95] J. A. De Loera, *Gröbner bases and graph colorings*, Beiträge Algebra Geom. **36** (1995), no. 1, 89–96.

[DLLMM08] J. De Loera, J. Lee, P. Malkin, and S. Margulies, *Hilbert's Nullstellensatz and an algorithm for proving combinatorial infeasibility*, Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation (ISSAC 2008), 2008.

[DLLMO09] J. De Loera, J. Lee, S. Margulies, and S. Onn, *Expressing combinatorial problems by systems of polynomial equations and Hilbert's Nullstellensatz*, Combin. Probab. Comput. **18** (2009), no. 4, 551–582.

[DLLY09] J. A. De Loera, F. Liu, and R. Yoshida, *A generating function for all semi-magic squares and the volume of the Birkhoff polytope*, J. Algebraic Combin. **30** (2009), no. 1, 113–139.

[DLMP09] J. De Loera, P. Malkin, and P. Parrilo, *Computation with polynomial equations and inequalities arising in combinatorial optimization*, http://arxiv.org/abs/0909.0808, 2009.

[DLRS10] J. A. De Loera, J. Rambau, and F. Santos, *Triangulations: Structures for algorithms and applications*, Algorithms and Computation in Mathematics, vol. 25, Springer, Berlin, 2010.

[Eli92] S. Eliahou, *An algebraic criterion for a graph to be four-colourable*, International Seminar on Algebra and its Applications (Spanish) (México City, 1991), Aportaciones Mat. Notas Investigación, vol. 6, Soc. Mat. Mexicana, México, 1992, pp. 3–27.

[Fau99] J. C. Faugére, *A new efficient algorithm for computing Gröbner bases* (F_4), J. Pure Appl. Algebra **139** (1999), no. 1-3, 61–88, Effective methods in algebraic geometry (Saint-Malo, 1998).

[Fis88] K. Fischer, *Symmetric polynomials and Hall's theorem*, Discrete Math. **69** (1988), no. 3, 225–234.

[Fri09] S. Friedland, *Graph isomorphism and volumes of convex bodies*, http://arxiv.org:0911.1739, 2009.

[GN10] J. Gouveia and T. Netzer, *Positive polynomials and projections of spectrahedra*, arXiv:0911.2750, 2010.

[GP06] R. M. Guralnick and D. Perkinson, *Permutation polytopes and indecomposable elements in permutation groups*, J. Combin. Theory Ser. A **113** (2006), no. 7, 1243–1256.

[GPT10] J. Gouveia, P. Parrilo, and R. R. Thomas, *Theta bodies for polynomial ideals*, SIAM Journal on Optimization **20** (2010), no. 4, 2097–2118.

[Gre66] M. Greenberg, *Rational points in Henselian discrete valuation rings*, Bull. Amer. Math. Soc. **72** (1966), no. 4, 713–714.

[GT11] J. Gouveia and R. R. Thomas, *Handbook of semidefinite, cone and polynomial optimization: Theory, algorithms, software and applications*, ch. Convex Hulls of Algebraic Sets, 2011.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hir64] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero: I*, Ann. of Math. **79** (1964), no. 1, 109–203.

[HL10] C. J. Hillar and L.-H. Lim, *Most tensor problems are NP hard*, Available at http://arxiv.org/abs/0911.1393, 2010.

[HP04] J. Hood and D. Perkinson, *Some facets of the polytope of even permutation matrices*, Linear Algebra and its Applications **381** (2004), 237–244.

[HW08] C. J. Hillar and T. Windfeldt, *Algebraic characterization of uniquely vertex colorable graphs*, J. Combin. Theory Ser. B **98** (2008), no. 2, 400–414.

[KK05] A. Kehrein and M. Kreuzer, *Characterizations of border bases*, J. Pure Appl. Algebra **196** (2005), no. 2-3, 251–270.

[KKY84] M. M. Kovalëv, M. K. Kravtsov, and V. Yemelichev, *Polytopes, graphs and optimisation*, Cambridge University Press, Cambridge, 1984, Translated from the Russian by G. H. Lawden.

[Kol88] J. Kollár, *Sharp effective Nullstellensatz*, J. Amer. Math. Soc. **1** (1988), no. 4, 963–975.

[Las02] J. B. Lasserre, *An explicit equivalent positive semidefinite program for nonlinear* 0-1 *programs*, SIAM J. Optim. **12** (2002), no. 3, 756–769 (electronic).

[Lau07] M. Laurent, *Semidefinite representations for finite varieties*, Math. Program. **109** (2007), no. 1, Ser. A, 1–26.

[LL81] S.-Y. Li and W. Li, *Independence numbers of graphs and generators of ideals*, Combinatorica **1** (1981), no. 1, 55–61.

[LLR08] J. B. Lasserre, M. Laurent, and P. Rostalski, *Semidefinite characterization and computation of zero- dimensional real radical ideals*, Found. Comput. Math. **8** (2008), no. 5, 607–647.

[Lov94] L. Lovász, *Stable sets and polynomials*, Discrete Math. **124** (1994), no. 1-3, 137–153, Graphs and combinatorics (Qawra, 1990).

[LR05] M. Laurent and F. Rendl, *Semidefinite programming & integer programming*, Handbook on Discrete Optimization (K. Aardal, G. Nemhauser, and R. Weismantel, eds.), Elsevier B.V., 2005, pp. 393–514.

[Mar08] S. Margulies, *Computer algebra, combinatorics, and complexity: Hilbert's Nullstellensatz and NP-complete problems*, Ph.D. thesis, UC Davis, 2008.

[Mat74] Y. Matiyasevich, *A criteria for colorability of vertices stated in terms of edge orientations*, Discrete Analysis **26** (1974), 65–71.

[Mat01] ———, *Some algebraic methods for calculation of the number of colorings of a graph*, Zapiski Nauchnykh Seminarov POMI **293** (2001), 193–205.

[MT08] B. Mourrain and P. Trébuchet, *Stable normal forms for polynomial system solving*, Theoret. Comput. Sci. **409** (2008), no. 2, 229–240.

[Mur08] M. Murray, *Positive polynomials and sums of squares*, Mathematical Surveys and Monographs, vol. 146, American Mathematical Society, 2008.

[Onn93] S. Onn, *Geometry, complexity, and combinatorics of permutation polytopes*, Journal of Combinatorial Theory, Series A **64** (1993), 31–49.

[Onn04] ———, *Nowhere-zero flow polynomials*, Journal of Combinatorial Theory, Series A **108** (2004), 205–215.

[Pak00] I. Pak, *Four questions on Birkhoff polytope*, Ann. Comb. **4** (2000), no. 1, 83–90.

[Par02] P. Parrilo, *An explicit construction of distinguished representations of polynomials nonnegative over finite sets*, IfA AUT02-02, ETH Zürich, 2002.

[Par03] P. A. Parrilo, *Semidefinite programming relaxations for semialgebraic problems*, Math. Program. **96** (2003), no. 2, Ser. B, 293–320, Algebraic and geometric methods in discrete optimization.

[Pos09] A. Postnikov, *Permutohedra, associahedra, and beyond*, Int. Math. Res. Not. IMRN (2009), no. 6, 1026–1106.

[PS10] S. Pokutta and A. Schulz, *On the connection of the Sherali-Adams Closure and Border Bases*, Available at http://www.optimization-online.org/DBHTML/2009/08/2378.html, 2010.

[Sch91] K. Schmüdgen, *The k-moment problem for compact semi-algebraic sets*, Math. Ann **289** (1991), no. 2, 203–206.

[Sey79] P. D. Seymour, *Sums of circuits*, Graph Theory and Related Topics (1979), 341–355.

[SFB11] R. Sanyal, S. F., and S. B., *Orbitopes*, Available at http://front.math.ucdavis.edu/0911.5436, 2011.

[She75] J. Sheehan, *The multiplicity of hamiltonian circuits in a graph*, 1975, pp. 477–480.

[Ste99] H. Steinkamp, *Convex polytopes and permutation matrices*, Master's thesis, Reed College, Portland, Oregon, 1999.

[Ste04] H. J. Stetter, *Numerical polynomial algebra*, Society for Industrial and Applied Mathematics (SIAM), 2004.

[Stu96] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, 1996.

[Sul06] S. Sullivant, *Compressed polytopes and statistical disclosure limitation*, Tohoku Math. J. (2) **58** (2006), no. 3, 433–445.

[SVV94] A. Simis, W. Vasconcelos, and R. Villarreal, *On the ideal theory of graphs*, J. Algebra **167** (1994), no. 2, 389–416.

[Sze73] G. Szekeres, *Polyhedral decompositions of cubic graphs*, Bull. Austral. Math. Soc. **8** (1973), 367–387.

[Tin86] G. Tinhofer, *Graph isomorphism and theorems of birkhoff type*, Computing **36** (1986), 285–300.

[Tru69] V. A. Trubin, *A method of solution of a special form of integer linear programming problems*, Dokl. Akad. Nauk SSSR **189** (1969), 952–954.

[Wie64] H. Wielandt, *Finite permutation groups*, Translated from the German by R. Bercov, Academic Press, New York, 1964.

[Yap00] C. K. Yap, *Fundamental problems of algorithmic algebra*, Oxford University Press, New York, 2000.