1-1-2010

Recognizing Graph Theoretic Properties with Polynomial Ideals

Jesus A. De Loera
University of California - Davis

Christopher J. HIllar
Mathematical Sciences Research Institute

Peter N. Malkin
University of California - Davis

Mohamed Omar
Harvey Mudd College

Recognizing Graph Theoretic Properties with Polynomial Ideals

Jesús A. De Loera*
University of California, Davis, Davis, CA 95616
deloera@math.ucdavis.edu

Christopher J. Hillar*
Mathematical Sciences Research Institute, Berkeley, CA 94120
chillar@msri.org

Peter N. Malkin*
University of California, Davis, Davis, CA 95616
malkin@math.ucdavis.edu

Mohamed Omar†
University of California, Davis, Davis, CA 95616
momar@math.ucdavis.edu

Submitted: Mar 10, 2010; Accepted: Jul 15, 2010; Published: Aug 16, 2010
Mathematics Subject Classification: 05C25, 05E40, 52B55

Abstract

Many hard combinatorial problems can be modeled by a system of polynomial equations. N. Alon coined the term *polynomial method* to describe the use of nonlinear polynomials when solving combinatorial problems. We continue the exploration of the polynomial method and show how the algorithmic theory of polynomial ideals can be used to detect k-colorability, unique Hamiltonicity, and automorphism rigidity of graphs. Our techniques are diverse and involve Nullstellensatz certificates, linear algebra over finite fields, Gröbner bases, toric algebra, convex programming, and real algebraic geometry.

[1]The first and third author are partially supported by NSF grant DMS-0914107 and an IBM OCR award.

*The second author is partially supported by an NSA Young Investigator Grant and an NSF All-Institutes Postdoctoral Fellowship administered by the Mathematical Sciences Research Institute through its core grant DMS-0441170.

†The fourth author is partially supported by NSERC Postgraduate Scholarship 281174.

1 Introduction

In his well-known survey [1], Noga Alon used the term *polynomial method* to refer to the use of nonlinear polynomials when solving combinatorial problems. Although the polynomial method is not yet as widely used as its linear counterpart, increasing numbers of researchers are using the algebra of multivariate polynomials to solve interesting problems (see for example [2, 12, 13, 17, 19, 23, 24, 32, 31, 35, 36, 38, 43] and references therein). In the concluding remarks of [1], Alon asked whether it is possible to modify algebraic proofs to yield efficient algorithmic solutions to combinatorial problems. In this paper, we explore this question further. We use polynomial ideals and zero-dimensional varieties to study three hard recognition problems in graph theory. We show that this approach can be fruitful both theoretically and computationally, and in some cases, result in efficient recognition strategies.

Roughly speaking, our approach is to associate to a combinatorial question (e.g., is a graph 3-colorable?) a system of polynomial equations J such that the combinatorial problem has a positive answer if and only if system J has a solution. These highly structured systems of equations (see Propositions 1.1, 1.3, and 1.4), which we refer to as *combinatorial systems of equations*, are then solved using various methods including linear algebra over finite fields, Gröbner bases, or semidefinite programming. As we shall see below this methodology is applicable in a wide range of contexts.

In what follows, $G = (V, E)$ denotes an undirected simple graph on vertex set $V = \{1, \ldots, n\}$ and edges E. Similarly, by $G = (V, A)$ we mean that G is a *directed* graph 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 for each edge in G. We study three classical graph problems.

First, in Section 2, we explore k-colorability using techniques from commutative algebra and algebraic geometry. The following polynomial formulation of k-colorability is well-known [5].

Proposition 1.1. *Let $G = (V, E)$ be an undirected simple graph on vertices $V = \{1, \ldots, n\}$. 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 common zero over $\overline{\mathbb{K}}$ (the algebraic closure of $\mathbb{K}$) if and only if the graph G is k-colorable.

Remark 1.2. *Depending on the context, the fields $\mathbb{K}$ we use in this paper 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 [11, Theorem 2, Chapter 4] states that a system of polynomial equations $\{f_1(x) = 0, \ldots, f_r(x) = 0\}$ with coefficients in $\mathbb{K}$ has no solution with entries

in its algebraic closure $\overline{\mathbb{K}}$ if and only if

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

Thus, if the system has no solution, there 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 $D := \max_{1 \leqslant i \leqslant r}\{\deg(\beta_i)\}$ or determine that no such certificate exists by solving a system of *linear equations* whose variables are in bijection with the coefficients of the monomials of $\beta_1, \ldots, \beta_r$ (see [15] and the many references therein). The number of variables in this linear system grows with the number $\binom{n+D}{D}$ of monomials of degree at most D. Crucially, the linear system, 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 [34, Theorem 4.1.3] or the survey [15]). The degree D of a Nullstellensatz certificate of an infeasible polynomial system cannot be more than known bounds [26], 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 [34, 14, 13]). The philosophy of "linearizing" a system of arbitrary polynomials has also been applied in other contexts besides combinatorics, including computer algebra [18, 25, 37, 44], logic and complexity [9], cryptography [10], and optimization [30, 28, 29, 39, 40, 41].

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 2.1, we give a combinatorial characterization of non-3-colorable graphs whose polynomial system encoding has a degree one Nullstellensatz certificate of infeasibility. Essentially, a graph has a degree one certificate 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. This result is reminiscent of the cycle double cover conjecture of Szekeres (1973) [47] and Seymour (1979) [42]. The class of non-3-colorable graphs with degree one certificates is far from trivial; it includes graphs that contain an odd-wheel or a 4-clique [34] and experimentally it has been shown to include more complicated graphs (see [34, 13, 15]).

In our second application of the polynomial method, we use tools from the theory of Gröbner bases to investigate (in Section 3) the detection of Hamiltonian cycles of a directed graph G. The following ideals algebraically encode Hamiltonian cycles (see Lemma 3.8 for a proof).

Proposition 1.3. *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. Consider the following system in $\mathbb{K}[x_1, \ldots, x_n]$:*

$$H_G = \{x_i^n - 1 = 0, \quad \prod_{j \in \delta^+(i)} (\omega x_i - x_j) = 0 : \ i \in V\}.$$

Here, $\delta^+(i)$ denotes those vertices j which are connected to i by an arc going from i to j in G. The system H has a solution over $\overline{\mathbb{K}}$ if and only if G has a Hamiltonian cycle.

We prove a decomposition theorem for the ideal H_G generated by the above polynomials, and based on this structure, we give an algebraic characterization of *uniquely Hamiltonian graphs* (reminiscent of the one for k-colorability in [24]). Our results also provide an algorithm to decide this property. These findings are related to a well-known theorem of Smith [50] which states that if a 3-regular graph has one Hamiltonian cycle then it has at least three. It is still an open question to decide the complexity of finding a second Hamiltonian cycle knowing that it exists [6].

Finally, in Section 4 we explore the problem of determining the automorphisms $Aut(G)$ of an undirected graph G. Recall that the elements of $Aut(G)$ are those permutations of the vertices of G which preserve edge adjacency. Of particular interest for us in that section is when graphs are *rigid*; that is, $|Aut(G)| = 1$. The complexity of this decision problem is still wide open [7]. The combinatorial object $Aut(G)$ will be viewed as an algebraic variety in $\mathbb{R}^{n\times n}$ as follows.

Proposition 1.4. *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 from the equations:*

$$\begin{gathered}(PA_G - A_GP)_{i,j} = 0, \;\; 1 \leqslant i, j \leqslant n; \quad \sum_{i=1}^{n} P_{i,j} = 1, \;\; 1 \leqslant j \leqslant n; \\ \sum_{j=1}^{n} P_{i,j} = 1, \;\; 1 \leqslant i \leqslant n; \quad P_{i,j}^2 - P_{i,j} = 0, \;\; 1 \leqslant i, j \leqslant n.\end{gathered} \tag{1}$$

Proof. The last three sets of equations say that P is a permutation matrix, while the first one ensures that this permutation preserves adjacency of edges ($PA_GP^\top = A_G$). □

In what follows, we shall interchangeably refer to $Aut(G)$ as a group or the variety of Proposition 1.4. This real variety can be studied from the perspective of convexity. Indeed, from Proposition 1.4, $Aut(G)$ consists of the integer vertices of the polytope of doubly stochastic matrices commuting with A_G. By replacing the equations $P_{i,j}^2 - P_{i,j} = 0$ in (1) with the linear inequalities $P_{ij} \geqslant 0$, we obtain a polyhedron P_G which is a convex relaxation of the automorphism group of the graph. This polytope and its integer hull have been investigated by Friedland and Tinhofer [48, 20], where they gave conditions for it to be integral. Here, we uncover more properties of the polyhedron P_G and its integer vertices $Aut(G)$.

Our first result is that P_G is *quasi-integral*; that is, the graph induced by the integer points in the 1-skeleton of P_G is connected (see Definition 7.1 in Chapter 4 of [27]). It follows that one can decide rigidity of graphs by inspecting the vertex neighbors of the identity permutation. Another application of this result is an output-sensitive algorithm for enumerating all automorphisms of any graph [3]. The problem of determining the triviality of the automorphism group of a graph can be solved efficiently when P_G is integral. Such graphs have been called *compact* and a fair amount of research has been dedicated to them (see [8, 48] and references therein).

Next, we use the theory of Gouveia, Parrilo, and Thomas [21], applied to the ideal I_G of Proposition 1.4, to approximate the integer hull of P_G by projections of semidefinite programs (the so-called *theta bodies*). In their work, the authors of [21] generalize the Lovász theta body for 0/1 polyhedra to generate a sequence of semidefinite programming relaxations computing the convex hull of the zeroes of a set of real polynomials [33, 32]. The paper [21] provides some applications to finding maximum stable sets [33] and maximum cuts [21]. We study the theta bodies of the variety of automorphisms of a graph. In particular, we give sufficient conditions on $Aut(G)$ for which the first theta body is already equal to P_G (in much the same way that stable sets of perfect graphs are theta-1 exact [21, 33]). Such graphs will be called *exact*. Establishing these conditions for exactness requires an interesting generalization of properties of the symmetric group (see Theorem 4.6 for details). In addition, we prove that compact graphs are a proper subset of exact graphs (see Theorem 4.4). This is interesting because we do not know of an example of a graph that is not exact, and the connection with semidefinite programming may open interesting approaches to understanding the complexity of the graph automorphism problem.

Below, we assume the reader is familiar with the basic properties of polynomial ideals and commutative algebra as introduced in the elementary text [11]. A quick, self-contained review can also be found in Section 2 of [24].

2 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 1.1:

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

This polynomial system 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

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

Our characterization involves two types of substructures on the graph G (see Figure 1). 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).

Theorem 2.1. *For a given simple undirected graph $G = (V, E)$ the following two conditions are equivalent:*

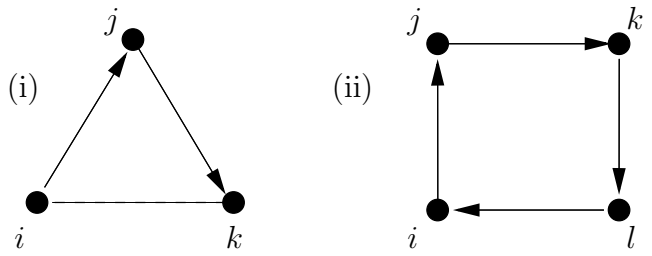

Figure 1: (i) partial 3-cycle, (ii) chordless 4-cycle

1. *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.

2. *There exists a set* C *of oriented partial* 3*-cycles and oriented chordless* 4*-cycles from* $Arcs(G)$ *such that*

   (a) $|C_{(i,j)}| + |C_{(j,i)}| \equiv 0 \pmod 2$ *for all* $\{i,j\} \in E$ *and*
   (b) $\sum_{(i,j)\in Arcs(G), i<j} |C_{(i,j)}| \equiv 1 \pmod 2$,

   where $C_{(i,j)}$ *denotes the set of cycles in* C *in which the arc* $(i,j) \in Arcs(G)$ *appears.*

Moreover, such graphs are non-3-colorable and can be recognized in polynomial time.

We can consider the set C in Theorem 2.1 as a covering of E by directed edges. From this perspective, Condition 1 in Theorem 2.1 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.

Note that the 3-cycles and 4-cycles in G that correspond to the partial 3-cycles and chordless 4-cycles in C give an edge-covering of a non-3-colorable subgraph of G. Also, note that if a graph G has a non-3-colorable subgraph whose polynomial encoding has a degree one infeasibility certificate, then the encoding of G will also have a degree one infeasibility certificate.

The class of graphs with encodings that have degree one infeasibility certificates includes all graphs containing odd wheels as subgraphs (e.g., a 4-clique) [34].

Corollary 2.2. *If a graph* $G = (V,E)$ *contains an odd wheel, then the encoding of* 3*-colorability of* G *from Theorem 2.1 has a degree one Nullstellensatz certificate of infeasibility.*

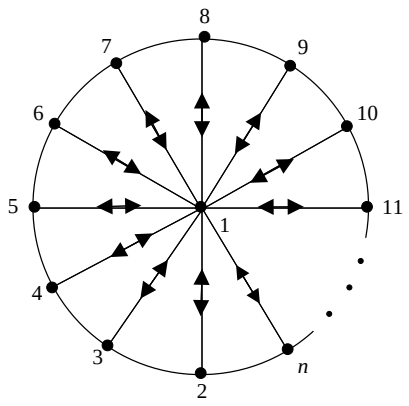

Figure 2: Odd wheel

Proof. Assume G contains an odd wheel with vertices labelled as in Figure 2 below. Let

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

Figure 2 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 2.1. 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 2.1. □

A non-trivial example of a non-3-colorable graph with a degree one Nullstellensatz certicate is the Grötzsch graph.

Example 2.3. *Consider the Grötzsch graph in Figure 3, which has no 3-cycles. The following set of oriented chordless 4-cycles gives a certificate of non-3-colorability by Theorem 2.1:*

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

Figure 3 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 2.1. Moreover, one can check that Condition 2 is also satisfied. It follows that the graph has no proper 3-coloring. □

We now prove Theorem 2.1 using ideas from polynomial algebra. First, notice that we can simplify a degree one certificate as follows: Expanding the left-hand side of (3) 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:

$$\sum_{i \in V} a_i (x_i^3 + 1) + \sum_{\{i,j\} \in E} (\sum_{k \in V} b_{ijk} x_k)(x_i^2 + x_i x_j + x_j^2) = 1. \tag{4}$$

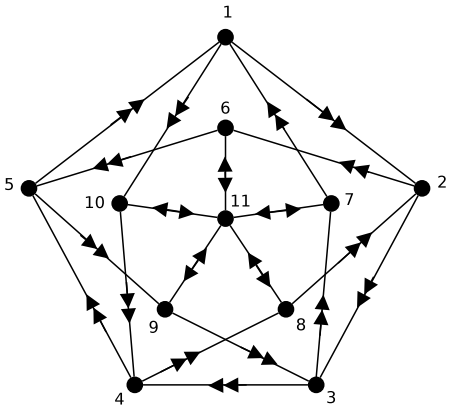

Figure 3: Grötzsch graph.

Now, consider the following set F of polynomials:

$$x_i^3 + 1 \qquad \forall i \in V, \tag{5}$$

$$x_k(x_i^2 + x_i x_j + x_j^2) \qquad \forall \{i,j\} \in E,\ k \in V. \tag{6}$$

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:

$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \forall \{i,j\} \in E, \tag{7}$$

$$x_i x_j^2 + x_j x_k^2 \qquad \forall (i,j),(j,k),(k,i) \in Arcs(G), \tag{8}$$

$$x_i x_j^2 + x_j x_k^2 + x_k x_l^2 + x_l x_i^2 \quad \forall (i,j),(j,k),(k,l),(l,i) \in Arcs(G), (i,k),(j,l) \notin Arcs(G). \tag{9}$$

If we identify the monomials $x_i x_j^2$ as the arcs (i,j), then the polynomials (8) correspond to oriented partial 3-cycles and the polynomials (9) 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 2.4. *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 (6) 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

$$x_i^3 + 1 \qquad \forall i \in V, \tag{10}$$

$$x_i(x_i^2 + x_i x_j + x_j^2) = x_i^3 + x_i^2 x_j + x_i x_j^2 \qquad \forall \{i,j\} \in E, \tag{11}$$

$$x_k(x_i^2 + x_i x_j + x_j^2) = x_i^2 x_k + x_i x_j x_k + x_j^2 x_k \qquad \forall \{i,j\} \in E,\ k \in V, i \neq k \neq j. \tag{12}$$

Using polynomials (10) to eliminate the x_i^3 terms from (11), we arrive at the following set of polynomials, which we label F':

$$x_i^3 + 1 \qquad \forall i \in V, \tag{13}$$

$$x_i^2 x_j + x_i x_j^2 + 1 = (x_i^3 + x_i^2 x_j + x_i x_j^2) + (x_i^3 + 1) \qquad \forall \{i,j\} \in E, \tag{14}$$

$$x_i^2 x_k + x_i x_j x_k + x_j^2 x_k \qquad \forall \{i,j\} \in E,\ k \in V, i \neq k \neq j. \tag{15}$$

Observe that $\langle F \rangle_{\mathbb{F}_2} = \langle F' \rangle_{\mathbb{F}_2}$. We can eliminate the polynomials (13) 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''.

$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \forall \{i,j\} \in E, \tag{16}$$

$$x_i^2 x_k + x_i x_j x_k + x_j^2 x_k \qquad \forall \{i,j\} \in E, k \in V, i \neq k \neq j. \tag{17}$$

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 $x_i x_j x_k$. 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 $x_i x_j x_k$ appears in only one polynomial, $x_k(x_i^2 + x_i x_j + x_j^2) = x_i^2 x_k + x_i x_j x_k + x_j^2 x_k$, so we can eliminate all such polynomials.

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

$$x_k(x_i^2 + x_i x_j + x_j^2) = x_i^2 x_k + x_i x_j x_k + x_j^2 x_k, \tag{18}$$

$$x_j(x_i^2 + x_i x_k + x_k^2) = x_i^2 x_j + x_i x_j x_k + x_j x_k^2, \tag{19}$$

$$x_i(x_j^2 + x_j x_k + x_k^2) = x_i x_j^2 + x_i x_j x_k + x_i x_k^2. \tag{20}$$

Using the first polynomial, we can eliminate $x_i x_j x_k$ from the other two:

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

We can now eliminate the polynomial (18). Moreover, we can use the polynomials (16) to rewrite the above two polynomials as follows.

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

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

$$x_k(x_i^2 + x_i x_j + x_j^2) = x_i^2 x_k + x_i x_j x_k + x_j^2 x_k, \tag{21}$$
$$x_i(x_j^2 + x_j x_k + x_k^2) = x_i x_j^2 + x_i x_j x_k + x_i x_k^2. \tag{22}$$

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 (21); thus, the original system has been reduced to the following one, which we label as F''':

$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \forall \{i,j\} \in E, \tag{23}$$
$$x_i x_j^2 + x_j x_k^2 \qquad \forall (i,j),(i,k),(j,k) \in Arcs(G), \tag{24}$$
$$x_i x_j^2 + x_j x_k^2 + (x_i^2 x_k + x_i x_k^2 + 1) \qquad \forall (i,j),(j,k) \in Arcs(G), (k,i) \notin Arcs(G). \tag{25}$$

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 (25) 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 (25) 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 (25), we have system H (polynomials (7), (8), and (9)):

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

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 2.1.

Lemma 2.5. *There exists a set C of oriented partial 3-cycles and oriented chordless 4-cycles satisfying Conditions 1. and 2. of Theorem 2.1 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 (8) or (9) 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 (8) or (9) 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 2.1. 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 2.4 and 2.5, we arrive at the characterization stated in Theorem 2.1. 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 [34, Theorem 4.1.3]).

Finally, we pose as open problems the construction of a variant of Theorem 2.1 for general k-colorability and also combinatorial characterizations for larger certificate degrees D.

Problem 2.6. *Characterize those graphs with a given k-colorability Nullstellensatz certificate of degree D.*

3 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. Let us denote by H_G the *Hamiltonian ideal* generated by the polynomials from Proposition 1.3. 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 3.8). 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:

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

We can also use the cyclotomic polynomial $\Phi_n(\omega)$ [16], 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 3.9 below). In the particular case when G has a unique Hamiltonian cycle, we get a specific algebraic criterion which can be algorithmically verified. These results are Hamiltonian analogues to the algebraic k-colorability characterizations of [24]. We first turn our attention more generally to cycle ideals 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).

When 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*. When $G = (V, E)$ is presented as an undirected graph, we shall always view it as the doubly covered directed graph on vertices V with arcs $Arcs(G)$.

Let C be a cycle of length $k > 2$ in G, expressed as a sequence of arcs,

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

For the purpose of this work, 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 3.1 (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 $\mathbb{K}[x_{v_1}, \ldots, x_{v_k}]$:*

$$g_i = \begin{cases} x_{v_i} + \frac{(\omega^{2+i} - \omega^{2-i})}{(\omega^3 - \omega)} x_{v_{k-1}} + \frac{(\omega^{1-i} - \omega^{3+i})}{(\omega^3 - \omega)} x_{v_k} & i = 1, \ldots, k-2, \\ (x_{v_{k-1}} - \omega x_{v_k})(x_{v_{k-1}} - \omega^{-1} x_{v_k}) & i = k-1, \\ x_{v_k}^k - 1 & i = k. \end{cases} \tag{26}$$

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:

$$g_i = \begin{cases} x_{v_{k-i}} - \omega^{k-i} x_{v_k} & i = 1, \ldots, k-1, \\ x_{v_k}^k - 1 & i = k. \end{cases} \tag{27}$$

Definition 3.2 (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_is are the cycle encoding of C given by (26) or (27).

The polynomials g_i are computationally useful generators for cycle ideals. (Once again, see [11] for the relevant background on Gröbner bases and term orders.)

Lemma 3.3. *The set of cycle encoding polynomials $F = \{g_1, \ldots, g_k\}$ is 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:

$$\{x_{v_1}, \ldots, x_{v_{k-2}}, x_{v_{k-1}}^2, x_{v_k}^k\} \text{ or } \{x_{v_1}, \ldots, x_{v_{k-2}}, x_{v_{k-1}}, x_{v_k}^k\} \tag{28}$$

are relatively prime, the polynomials g_i form a Gröbner basis for $H_{G,C}$ (see Theorem 3 and Proposition 4 in [11, Section 2]). That F is reduced follows from inspection of (26) and (27). □

Remark 3.4. *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 3.6).*

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

Corollary 3.5. *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 [11, Chapter 9, §3]. The form of the Hilbert series is now immediate from (28). □

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

1. *$H_{G,C}$ is radical,*
2. *$|V(H_{G,C})| = k$ if C is directed, and $|V(H_{G,C})| = 2k$ 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 3.3, 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 [24, Lemma 2.1], if we can prove that $|V(H_{G,C})| \geqslant k$ (resp. $|V(H_{G,C})| \geqslant 2k$), then both statements 1. and 2. follow.

When C is directed, this follows easily from the form of (27), 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 3.7. *Conversely, it is easy to see that points in $V(H_{G,C})$ 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 stating our decomposition theorem (Theorem 3.9), we need to explain how the Hamiltonian ideal encodes all Hamiltonian cycles of the graph G.

Lemma 3.8. *Let G be a connected directed graph on n vertices. Then,*

$$V(H_G) = \bigcup_C V(H_{G,C}),$$

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

Proof. We only need to verify that points in $V(H_G)$ 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 $V(H_G)$ 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 nth root of unity, this cycle must have length n, and thus is Hamiltonian. □

Combining all of these ideas, we can prove the following result.

Theorem 3.9. *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.

Proof. Since H_G contains a square-free univariate polynomial in each indeterminate, it is radical (see for instance [24, Lemma 2.1]). It follows that

$$\begin{aligned} H_G &= I(V(H_G)) \\ &= I\left(\bigcup_C V(H_{G,C})\right) \\ &= \bigcap_C I(V(H_{G,C})) \\ &= \bigcap_C H_{G,C}, \end{aligned} \tag{29}$$

where the second inequality comes from Lemma 3.8 and the last one from $H_{G,C}$ being a radical ideal (Lemma 3.6). □

We call a directed graph (resp. doubly covered graph) *uniquely Hamiltonian* if it contains n cycles of length n (resp. $2n$ cycles of length n).

Corollary 3.10. *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.*

This corollary 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 bases 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 [51, p. 400].

We close this section with a directed and an undirected example of Theorem 3.9.

Example 3.11. *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, $\{x_i^5 - 1 : 1 \leqslant i \leqslant 5\}$ union with the polynomials*

$$\{(\omega x_1 - x_2)(\omega x_1 - x_3)(\omega x_1 - x_4), \omega x_2 - x_3, \omega x_3 - x_4, \omega x_4 - x_5, \omega x_5 - x_1\}.$$

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 3.9 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 the two cycles

$$\{(v_1,v_2),(v_2,v_3),\ldots,(v_{n-1},v_n),(v_n,v_1)\}, \{(v_2,v_1),(v_3,v_2),\ldots,(v_n,v_{n-1}),(v_1,v_n)\}$$

are Hamiltonian cycles of $\tilde{G}$.

Example 3.12. *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:*

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

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 $i = 1,\ldots,12$.

4 Permutation Groups as Algebraic Varieties and their Convex Approximations

In this section, we study convex hulls of permutations groups viewed as permutation matrices. We begin by studying the convex hull of automorphism groups of undirected simple graphs; these have a natural polynomial presentation using Proposition 1.4 from the introduction. For background material on graph automorphism groups see [7, 8].

We write $Aut(G)$ for the automorphism group of a graph $G = (V, E)$. Elements of $Aut(G)$ are naturally represented as $|V| \times |V|$ permutation matrices; they are the *integer* vertices of the rational polytope P_G defined in the discussion following Proposition 1.4. The polytope P_G was first introduced by Tinhofer [48]. Since we are primarily interested in the integer vertices of P_G, we investigate IP_G, the *integer hull* of P_G (i.e. $IP_G = conv(P_G \cap \mathbb{Z}^{n\times n})$). In the fortunate case that P_G is already integral ($P_G = IP_G$), we say that the graph G is *compact*, a term coined in [48]. This occurs, for example, in the special case that G is an independent set on n vertices. In this case $Aut(G) = S_n$ and P_G is the well-studied Birkhoff polytope, the convex hull of all doubly-stochastic matrices (see Chapter 5 of [27]). 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. Nevertheless, we can prove the following related result.

Proposition 4.1. *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.*

Proof. We claim that there exists a 0/1 matrix A such that P_G is the set of points $\{x \in \mathbb{R}^{n\times n} \ : \ Ax = \mathbf{1}, x \geqslant 0\}$ (where $\mathbf{1}$ is the all 1s vector). By the main theorem of Trubin [49] and independently [4], polytopes given by such systems are quasi-integral (see also Theorem 7.2 in Chapter 4 of [27]). Therefore, we need to rewrite the defining equations presented in Proposition 1.4 to fit this desired shape. Fix indices $1 \leqslant i, j \leqslant n$ 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 $\sum_{r=1}^{n} P_{rj} = 1$ to both sides of this expression yields

$$\sum_{r\in\delta(j)} P_{ir} + \sum_{k\notin\delta(i)} P_{kj} = 1. \tag{30}$$

We can therefore replace the original n^2 equations defining P_G by (30) over all $1 \leqslant i, j \leqslant n$. 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 1.4 and its real variety $V_{\mathbb{R}}(I_G)$. We approximate a tighter description of IP_G using a hierarchy of projected semidefinite relaxations of $conv(V_{\mathbb{R}}(I_G))$. When these relaxations are tight, we obtain a full description of IP_G that allows us to optimize and determine feasibility via semidefinite programming.

We begin with some preliminary definitions from [21] and motivated by Lovász & Schrijver [33]. Let $I \subset \mathbb{R}[x_1, \ldots, x_n]$ be a *real radical ideal* ($I = \mathcal{I}(V_{\mathbb{R}}(I))$). A polynomial

f is said to be *nonnegative* mod I (written $f \geqslant 0 \pmod{I}$) if $f(p) \geqslant 0$ 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 the $h_1, \ldots, h_m$ are bounded by some positive integer k, we say f is k-sos mod I.

The *k-th theta body* of I, denoted $TH_k(I)$, is the subset of $\mathbb{R}^n$ that is nonnegative on each $f \in I$ that is k-sos mod I. We say that a real variety $V_{\mathbb{R}}(I)$ is *theta k-exact* if $\overline{conv(V_{\mathbb{R}}(I))} = TH_k(I)$. When the ideal I is real radical, theta bodies provide a hierarchy of semidefinite relaxations of $\overline{conv(V_{\mathbb{R}}(I))}$:

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

because in this case theta bodies can be expressed as projections of feasible regions of semidefinite programs (such regions are called *spectrahedra*). In order to exploit this theory, we must establish that I_G is indeed real radical.

Lemma 4.2. *The ideal $I_G \subseteq \mathbb{R}[x_1, \ldots, x_n]$ is real radical.*

Proof. Let J_G be the ideal in $\mathbb{C}[x_1, \ldots, x_n]$ generated by the same polynomials that generate I_G, and $\sqrt[\mathbb{R}]{I_G}$ be the real radical of I_G. Since the polynomial $x_i^2 - x_i \in J_G$ for each $1 \leqslant i \leqslant n$, Lemma 2.1 of [24] implies $J_G = \sqrt{J_G}$ (where $\sqrt{J_G}$ is the radical of J_G). Together with the fact that $V_{\mathbb{C}}(J_G) = V_{\mathbb{R}}(I_G)$, this implies $J_G \supseteq \sqrt[\mathbb{R}]{I_G}$. Since $I_G = J_G \cap \mathbb{R}[x_1, \ldots, x_n]$, we conclude $I_G \supseteq \sqrt[\mathbb{R}]{I_G}$. The result follows since trivially, $I_G \subseteq \sqrt[\mathbb{R}]{I_G}$. □

From Lemma 4.2, we conclude that if I_G is theta k-exact, linear optimization over the automorphisms can be performed using semidefinite programming provided that one first computes a basis for the quotient ring $\mathbb{R}[P_{11}, P_{12}, \ldots, P_{nn}]/I_G$ (e.g., obtained from the standard monomials of a Gröbner basis). Using such a basis one can set up the necessary semidefinite programs (see Section 2 of [21] for details). In fact, for k-exact ideals, one only needs those elements of the basis up to degree $2k$. This motivates the need for characterizing those graphs for which I_G is k-exact.

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 4.3. *[21] 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 $g(x) \geqslant 0$, 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 [46]) 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 4.3. Putting these ideas together we can prove compactness implies exactness. Furthermore, the class of exact graphs properly extends the class of compact graphs. The proof of this latter fact is an extension of a result in [48].

Theorem 4.4. *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 $1 \leqslant i, j \leqslant n$.*

Proof. If G is compact, then the integer hull of P_G is precisely the affine space

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

intersected with the cube $[0,1]^{n\times n}$. That G is exact follows from Theorem 2.4 of [46].

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 [48, 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 $I\tilde{P}_G$):

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

where $n_i = |V(G_i)|$ with $n_1 \leqslant n_2$. Statement 2 then follows again from Theorem 2.4 of [46].

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 $\tilde{IP}_G$. 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 $\tilde{IP}_G$.

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 $1 \leqslant i \leqslant n$. 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 [8], 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 exactness is really a property of the set of permutation matrices representing an automorphism group. This discussion motivates the following question.

Question 4.5. *Which permutation subgroups of S_n are exact?*

Here we view a permutation subgroup of S_n through its natural permutation representation in $\mathbb{R}^{n\times n}$. In this light, a permutation subgroup can be considered as a variety, and we say the permutation subgroup is *exact* if this variety is exact. As an example, consider the alternating group A_n as a subgroup of S_n. It is known (see [7]) that A_n is never the automorphism group of a graph on n vertices, so it cannot be presented as the integer points of a polytope of the form P_G with $|V(G)| = n$. However, there is a description of A_n as a variety whose points are vertices of the $n \times n$ Birkhoff polytope:

$$\sum_{j=1}^{n} P_{i,j} = 1, \quad 1 \leqslant i \leqslant n; \quad \sum_{i=1}^{n} P_{i,j} = 1, \quad 1 \leqslant j \leqslant n;$$
$$\det(P) = 1; \qquad\qquad P_{i,j}^2 - P_{i,j} = 0, \quad 1 \leqslant i, j \leqslant n.$$

More generally, when a finite permutation group has a description as a variety, we can apply the theory of theta bodies to obtain descriptions of convex hulls. Using the algebraic-geometric ideas outlined in [45] we give a sufficient condition for exactness of permutation groups.

Let $A = \{\sigma_1, \ldots, \sigma_d\}$ be a subgroup of S_n. We consider A as the set of matrices $\{P_{\sigma_1}, \ldots, P_{\sigma_d}\} \subseteq \mathbb{Z}^{n\times n}$, where P_{σ_i} is the permutation matrix corresponding to σ_i. Let $\mathbb{C}[\mathbf{x}] := \mathbb{C}[x_{\sigma_1}, \ldots, x_{\sigma_d}]$ be the polynomial ring in d indeterminates indexed by permutations in A, and let $\mathbb{C}[\mathbf{t}] := \mathbb{C}[t_{ij} : 1 \leqslant i, j \leqslant n]$.

The algebra homomorphism induced by the map

$$\pi : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{t}], \ \pi(x_{\sigma_i}) = \prod_{1\leqslant j,k\leqslant n} t_{jk}^{(P_{\sigma_i})_{jk}} \tag{31}$$

has kernel I_A, which is a prime *toric ideal* [45]. By Theorem 4.3, Corollary 8.9 in [45], and Corollary 2.5 in [46], the group A is exact if and only if for every reverse lexicographic term ordering $\prec$ on $\mathbb{C}[x]$, the initial ideal $in_\prec(I_A)$ is generated by square-free monomials. We now describe a family of permutation groups that are exact.

Let $A \subseteq \mathbb{Z}^{n\times n}$ be a subgroup of S_n. We say that A is *permutation summable* if for any permutations $P_1, \ldots, P_m \in A$ satisfying the inequality $\sum_{i=1}^m P_i - I \geqslant 0$ (entry-wise), we have that $\sum_{i=1}^m P_i - I$ is also a sum of permutation matrices in A. For example, Birkhoff's Theorem (see e.g., Theorem 1.1 in Chapter 5 of [27]) implies S_n is permutation summable. Note that in this case P_{S_n} is the Birkhoff polytope which is known to be exact by the results in [21]. We prove the following result.

Theorem 4.6. *Let $A = \{\sigma_1, \ldots, \sigma_d\}$ be a permutation group that is a subgroup of S_n.*

(1) If A is permutation summable, then A is exact.

(2) Suppose I_A, the toric ideal associated to A, has a quadratically generated Gröbner basis with respect to any reverse lexicographic ordering $\prec$, then A is exact.

Proof. Let I_A be the kernel of the algebra homomorphism induced by (31). We shall abbreviate the action of π on x_σ by $\pi(x_\sigma) = t^{P_\sigma}$ for any $\sigma \in A$.

Let $\mathfrak{G}$ be a reduced Gröbner basis for I_A with respect to some reverse lexicographic order $\prec$ on $\{x_{\sigma_1}, \ldots, x_{\sigma_d}\}$. Let $x^u - x^v \in \mathfrak{G}$ with leading term x^u. By Theorem 4.3, Corollary 8.9 in [45] and Corollary 2.5 in [46], Statement (1) follows if we can find a square-free monomial $x^{u'} \in in_\prec(I_A)$ such that $x^{u'}$ divides x^u.

Let x_τ be the smallest variable dividing x^v with respect to $\prec$. Then x_τ is smaller than any variable appearing in x^u by the choice of a reverse lexicographic ordering. Since $x^u - x^v \in \mathfrak{G}$, we have $\pi(x^u) = \pi(x^v)$. It follows that $\pi(x_\tau)$ divides $\pi(x^u)$, so letting $x^u = x_{\sigma_{i_1}} \cdots x_{\sigma_{i_k}}$ for some $\{\sigma_{i_1}, \ldots, \sigma_{i_k}\} \subseteq A$, we have

$$\frac{\pi(x^u)}{\pi(x_\tau)} = t^{P_{\sigma_{i_1}} + \cdots + P_{\sigma_{i_k}}} t^{-P_\tau},$$

in which $\sum_{j=1}^k P_{\sigma_{i_j}} - P_\tau$ is a matrix with nonnegative integer entries. Choose a subset $\{\rho_1, \ldots, \rho_r\} \subset \{\sigma_{i_1}, \ldots, \sigma_{i_k}\}$ such that $\{P_{\rho_1}, \ldots, P_{\rho_r}\}$ minimally supports P_τ with $P_{\rho_i} \neq P_{\rho_j}$ for all i, j, and let $x^{u'} = x_{\rho_1} \cdots x_{\rho_r}$. We claim that $x^{u'}$ is a square-free monomial that divides x^u and lies in $in_\prec(I_A)$, which will prove Statement (1).

By construction, all indeterminates $x_{\rho_1}, \ldots, x_{\rho_r}$ are distinct, so $x^{u'}$ is square-free. Moreover, since $\{\rho_1, \ldots, \rho_r\} \subset \{\sigma_{i_1}, \ldots, \sigma_{i_k}\}$, we have that $x^{u'}$ divides x^u. It remains to show that $x^{u'}$ lies in $in_\prec(I_A)$. To see this, note that $\sum_{i=1}^r P_{\rho_i} - P_\tau$ has nonnegative integer entries, and hence so does

$$M = \sum_{i=1}^r (P_\tau)^{-1} P_{\rho_i} - I$$

(multiplying by P_τ^{-1} permutes matrix entries, and therefore does not effect nonnegativity). Since A is permutation summable, the matrix M is a sum of matrices in A, and hence so is $P_\tau M = \sum_{i=1}^r P_{\rho_i} - P_\tau$. It follows that

$$\sum_{i=1}^r P_{\rho_i} - P_\tau = \sum_{j=1}^{r-1} P_{\sigma_{l_j}}$$

for some $\{\sigma_{l_1}, \ldots, \sigma_{l_{r-1}}\} \subset A$. In particular, $\pi(x^{u'}) = \pi(x_\tau) \cdot \pi(x^{v'})$ and so $x^{u'} - x_\tau x^{v'} \in I_A$. Since x_τ is smaller than any term in $x^{u'}$ (the monomial $x^{u'}$ divides x^u and the same holds for x^u), the leading term of $x^{u'} - x_\tau x^{v'}$ is $x^{u'}$; hence, $x^{u'} \in in_\prec(I_A)$. This proves Statement (1).

For Statement (2), since any Gröbner basis is quadratically generated, by part (1) it suffices to show that if $P_1, P_2, Q \in A$ with all entries of $P_1 + P_2 - Q$ nonnegative, then $P_1 + P_2 - Q$ is a permutation matrix. Since $supp(Q) \subset supp(P_1) \cup supp(P_2)$, the permutation Q is a vertex of a face containing P_1 and P_2. By Theorem 3.5 of [22], Q is on the smallest face containing P_1 and P_2, and this face is centrally symmetric. Thus, there is a vertex R such that $Q + R = P_1 + P_2$, and the result follows.

□

In light of Theorem 4.6, we would like to find permutation groups A that are permutation summable. As we have seen, Birkhoff's Theorem (see [45]) implies that S_n is permutation summable. We can use this fact to construct more permutation summable groups. For instance, $S_{n_1} \times \cdots \times S_{n_m}$ is permutation summable, simply by applying the permutation summability condition on each S_{n_i} and taking direct sums. More generally, if $H_1, \ldots, H_m$ are permutation summable, then so is $H_1 \times \cdots \times H_m$. We present another class of permutation summable groups that contains familiar groups.

Definition 4.7. *Let A be a permutation subgroup of S_n. We say A is strongly fixed-point free if for every $\sigma \in A \backslash \{1\}$, we have $\sigma(i) \neq i$ for any $i \in \{1, \ldots, n\}$.*

Corollary 4.8. *Let A be a strongly fixed-point free subgroup of S_n. Then A is exact.*

Proof. Let A be strongly fixed-point free. Consider any subset $\{P_{\sigma_1}, \ldots, P_{\sigma_k}\}$ of A and assume $\sum_{i=1}^{k} P_{\sigma_i} - I$ is a matrix with nonnegative entries. Then one of the matrices in A contains a fixed point. Without loss of generality, assume P_{σ_1} is one such matrix. Since A is strongly fixed-point free, we have $P_{\sigma_1} = I$. Hence,

$$\sum_{i=1}^{k} P_{\sigma_i} - I = \sum_{i=2}^{k} P_{\sigma_i},$$

and thus A is permutation summable. The result now follows from Theorem 4.6. □

There are many well-known families of permutation groups that are strongly fixed-point free, and hence exact. These include the group generated by any n cycle in S_n, and even dihedral groups (dihedral groups of order $4n$ as subgroups of S_{2n}).

Acknowledgements

We would like to thank the referee for his or her truly valuable suggestions and corrections. We would also like to thank Joao Gouveia for his help.

References

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

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

[3] 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).

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

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

[6] 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).

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

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

[9] 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, NY, USA), ACM, 1996, pp. 174–183.

[10] 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.

[11] 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.

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

[13] J.A. De Loera, J. Lee, P.N. 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.

[14] J.A. 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.

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

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

[17] 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.

[18] 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).

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

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

[21] J. Gouveia, P.A. Parrilo, and R.R. Thomas, *Theta bodies for polynomial ideals*, http://arxiv.org:0809.3480, 2008.

[22] 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.

[23] C. J. Hillar and L-H. Lim, *Most tensor problems are NP hard*, preprint, 2010.

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

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

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

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

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

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

[30] 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.

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

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

[33] L. Lovász and A. Schrijver, *Cones of matrices and set-functions and* 0-1 *optimization*, SIAM J. Optim. **1** (1991), no. 2, 166–190.

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

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

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

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

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

[39] 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.

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

[41] S. Pokutta and A.S. Schulz, *On the connection of the Sherali-Adams Closure and Border Bases*, 2009, Working Paper, Technische Universität Darmstadt / Massachusetts Institute of Technology.

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

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

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

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

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

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

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

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

[50] W. T. Tutte, *On hamiltonian circuits*, J. London Math. Soc. **21** (1946), 98–101.

[51] C. K. Yap, *Fundamental problems of algorithmic algebra*, Oxford University Press, New York, 2000. MR MR1740761 (2000m:12014)