Computational Aspects of Graph Coloring and the Quillen–Suslin Theorem

Troels Windfeldt

Department of Mathematical Sciences
University of Copenhagen
Denmark

Preface

This thesis is the result of research I have carried out during my time as a PhD student at the University of Copenhagen. It is based on four papers, the overall topics of which are: Graph Coloring, The Quillen–Suslin Theorem, and Symmetric Ideals. The thesis is organized as follows.

Graph Coloring

Part 1 is, except for a few minor corrections, identical to the paper ”Fibonacci Identities and Graph Colorings” (joint with C. Hillar, see page 61), which has been accepted for publication in *The Fibonacci Quarterly.* The paper introduces a simple idea that relates graph coloring with certain integer sequences including the Fibonacci and Lucas numbers. It demonstrates how one can produce identities involving these numbers by decomposing different classes of graphs in different ways. The treatment is by no means exhaustive, and there should be many ways to expand on the results presented in the paper.

Part 2 is an extended and improved version of the paper ”Algebraic Characterization of Uniquely Vertex Colorable Graphs” (joint with C. Hillar, see page 67), which has appeared in *Journal of Combinatorial Theory, Series B.* The paper deals with graph coloring from a computational algebraic point of view. It collects a series of results in the literature regarding graphs that are not k-colorable, and provides a refinement to uniquely k-colorable graphs. It also gives algorithms for testing (unique) vertex colorability. These algorithms are then used to verify a counterexample to a conjecture of Xu concerning uniquely 3-colorable graphs without triangles.

The Quillen–Suslin Theorem

Part 3 is the manuscript ”Revisiting an Algorithm for the Quillen–Suslin Theorem”, which is still work in progress. It provides a new algorithm for the Quillen–Suslin Theorem in case of an infinite ground field. The new algorithm follows the lines of an algorithm by Logar and Sturmfels, however, both theoretical and experimental evidence that the new algorithm produces a much simpler output, is presented. This will hopefully facilitate its implementation in a computer algebra system.

Symmetric Ideals

Part 4 is an extended version of the short paper ”Minimal Generators for Symmetric Ideals” (joint with C. Hillar, see page 82), which has appeared in *Proceedings of the American Mathematical Society.* The paper settles a question regarding the minimal number of generators for symmetric ideals in polynomial rings with infinitely many indeterminates.

I would like to take this opportunity to thank my supervisor Henrik Schlichtkrull for accepting me as his PhD student, for letting me pursue my own mathematical interests, and for supporting me all the way.

It has been a thrill working with my colleague and dear friend, Chris Hillar, who deserves a special thanks. I would also like to thank Niels Lauritzen and David Cox for many inspirational discussions on computational algebra.

Last, but not least, I thank my wife Gitte and daughter Emma for their continuous love and support.

Allerød,
February 27, 2009, *Troels Windfeldt.*

Contents

I

Graph Coloring

Part 1

Fibonacci Identities and Graph Colorings

We generalize both the Fibonacci and Lucas numbers to the context of graph colorings, and prove some identities involving these numbers. As a corollary we obtain new proofs of some known identities involving Fibonacci numbers such as

$$F_{r+s+t} = F_{r+1}F_{s+1}F_{t+1} + F_rF_sF_t - F_{r-1}F_{s-1}F_{t-1}.$$

1.1 Introduction

In graph theory, it is natural to study vertex colorings, and more specifically, those colorings in which adjacent vertices have different colors. In this case, the number of such colorings of a graph G is encoded by the chromatic polynomial of G. This object can be computed using the method of "deletion and contraction", which involves the recursive combination of chromatic polynomials for smaller graphs. The purpose of this note is to show how the Fibonacci and Lucas numbers (and other integer recurrences) arise naturally in this context, and in particular, how identities among these numbers can be generated from the different choices for decomposing a graph into smaller pieces.

We first introduce some notation. Let G be a undirected graph (possibly containing loops and multiple edges) with vertices $V = \{1, \ldots, n\}$ and edges E. Given nonnegative integers k and ℓ, a (k, ℓ)-*coloring* of G is a map

$$\varphi : V \to \{c_1, \ldots, c_{k+\ell}\},$$

in which $\{c_1, \ldots, c_{k+\ell}\}$ is a fixed set of $k+\ell$ "colors". The map φ is called *proper* if whenever i is adjacent to j and $\varphi(i), \varphi(j) \in \{c_1, \ldots, c_k\}$, we have $\varphi(i) \neq \varphi(j)$. Otherwise, we say that the map φ is *improper*. In somewhat looser terminology, one can think of $\{c_{k+1}, \ldots, c_{k+\ell}\}$ as coloring "wildcards".

Let $\chi_G(x, y)$ be a function such that $\chi_G(k, \ell)$ is the number of proper (k, ℓ)-colorings of G. This object was introduced by the authors of [DPT03] and can be given as a polynomial in x and y (see Lemma 1.1.1). It simultaneously generalizes the chromatic, independence, and matching polynomials of G. For instance, $\chi_G(x, 0)$ is the usual chromatic polynomial while $\chi_G(x, 1)$ is the independence polynomial for G (see [DPT03] for more details).

We next state a simple rule that enables one to calculate the polynomial $\chi_G(x, y)$ recursively. In what follows, $G\backslash e$ denotes the graph obtained by removing the edge e from G, and for a subgraph H of G, the graph $G\backslash H$ is gotten from G by removing H and all the edges of G that are adjacent to vertices of H. Additionally, the *contraction* of an edge e in G is the graph G/e obtained by removing e and identifying as equal the two vertices sharing this edge.

Lemma 1.1.1. *Let e be an edge in G, and let v be the vertex to which e contracts in G/e. Then,*

$$\chi_G(x, y) = \chi_{G\backslash e}(x, y) - \chi_{G/e}(x, y) + y \cdot \chi_{(G/e)\backslash v}(x, y). \tag{1.1.1}$$

Proof. The number of proper (k, ℓ)-colorings of $G\backslash e$ which have distinct colors for the vertices sharing edge e is given by $\chi_{G\backslash e}(k, \ell) - \chi_{G/e}(k, \ell)$; these colorings are also proper for G. The remaining proper (k, ℓ)-colorings of G are precisely those for which the vertices sharing edge e have the same color. This color must be one of the wildcards $\{c_{k+1}, \dots, c_{k+\ell}\}$, and so the number of remaining proper (k, ℓ)-colorings of G is counted by $\ell \cdot \chi_{(G/e)\backslash v}(k, \ell)$. □

With such a recurrence, we need to specify initial conditions. When G simply consists of one vertex and has no edges, we have $\chi_G(x, y) = x + y$, and when G is the empty graph, we set $\chi_G(x, y) = 1$ (consider G with one edge joining two vertices in (1.1.1)). Moreover, χ is multiplicative on disconnected components. This allows us to compute χ_G for any graph recursively.

In the special case when $k = 1$, there is also a way to calculate $\chi_G(1, y)$ by removing vertices from G. Define the *link* of a vertex v to be the subgraph $\mathrm{link}(v)$ of G consisting of v, the edges touching v, and the vertices sharing one of these edges with v. Also if u and v are joined by an edge e, we define $\mathrm{link}(e)$ to be $\mathrm{link}(u) \cup \mathrm{link}(v)$ in G, and also we set $\deg(e)$ to be $\deg(u) + \deg(v) - 2$. We then have the following rules.

Lemma 1.1.2. *Let v be any vertex of G, and let e be any edge. Then,*

$$\chi_G(1, y) = y \cdot \chi_{G\backslash v}(1, y) + y^{\deg(v)} \cdot \chi_{G\backslash \mathrm{link}(v)}(1, y), \tag{1.1.2}$$

$$\chi_G(1, y) = \qquad \chi_{G\backslash e}(1, y) - y^{\deg(e)} \cdot \chi_{G\backslash \mathrm{link}(e)}(1, y). \tag{1.1.3}$$

Proof. The number of proper $(1, \ell)$-colorings of G with vertex v colored with a wildcard is $\ell \cdot \chi_{G\backslash v}(1, \ell)$. Moreover, in any proper coloring of G with v colored c_1, each vertex among the $\deg(v)$ ones adjacent to v can only be one of the ℓ wildcards. This explains the first equality in the lemma.

Let v be the vertex to which e contracts in G/e. From equation (1.1.2), we have

$$\chi_{G/e}(1, y) = y \cdot \chi_{(G/e)\backslash v}(1, y) + y^{\deg(v)} \cdot \chi_{(G/e)\backslash \mathrm{link}(v)}(1, y).$$

Subtracting this equation from (1.1.1) with $x = 1$, and noting that $\deg(e) = \deg(v)$ and $G\backslash \mathrm{link}(e) = (G/e)\backslash \mathrm{link}(v)$, we arrive at the second equality in the lemma. □

Let P_n be the path graph on n vertices and let C_n be the cycle graph, also on n vertices (C_1 is a vertex with a loop attached while C_2 is two vertices joined by two edges). Fixing nonnegative integers k and ℓ not both zero, we define the following sequences of numbers ($n \geq 1$):

$$\begin{aligned} a_n &= \chi_{P_n}(k, \ell), \\ b_n &= \chi_{C_n}(k, \ell). \end{aligned} \tag{1.1.4}$$

As we shall see, these numbers are natural generalizations of both the Fibonacci and Lucas numbers to the context of graph colorings. The following lemma uses graph decomposition to give simple recurrences for these sequences.

Lemma 1.1.3. *The sequences a_n and b_n satisfy the following linear recurrences with initial conditions:*

$$a_1 = k + \ell, \qquad a_2 = (k+\ell)^2 - k, \qquad a_n = (k+\ell-1)a_{n-1} + \ell a_{n-2}; \tag{1.1.5}$$

$$b_1 = \ell, \qquad b_2 = (k+\ell)^2 - k, \qquad b_3 = a_3 - b_2 + \ell a_1, \tag{1.1.6}$$

$$b_n = (k+\ell-2)b_{n-1} + (k+2\ell-1)b_{n-2} + \ell b_{n-3}. \tag{1.1.7}$$

Moreover, the sequence b_n satisfies a shorter recurrence if and only if $k = 0$, $k = 1$, or $\ell = 0$. When $k = 0$, this recurrence is given by $b_n = \ell b_{n-1}$, and when $k = 1$, it is

$$b_n = \ell b_{n-1} + \ell b_{n-2}. \tag{1.1.8}$$

Proof. The first recurrence follows from deleting an outer edge of the path graph P_n and using Lemma 1.1.1. To verify the second one, we first use Lemma 1.1.1 (picking any edge in C_n) to give

$$b_n = a_n - b_{n-1} + \ell a_{n-2}. \tag{1.1.9}$$

Let $c_n = b_n + b_{n-1} = a_n + \ell a_{n-2}$ and notice that c_n satisfies the same recurrence as a_n; namely,

$$\begin{aligned} c_n &= a_n + \ell a_{n-2} \\ &= (k+\ell-1)a_{n-1} + \ell a_{n-2} + \ell\left((k+\ell-1)a_{n-3} + \ell a_{n-4}\right) \\ &= (k+\ell-1)(a_{n-1} + \ell a_{n-3}) + \ell(a_{n-2} + \ell a_{n-4}) \\ &= (k+\ell-1)c_{n-1} + \ell c_{n-2}. \end{aligned} \tag{1.1.10}$$

It follows that b_n satisfies the third order recurrence given in the statement of the lemma. Additionally, the initial conditions for both sequences a_n and b_n are easily worked out to be the ones shown.

Finally, suppose that the sequence b_n satisfies a shorter recurrence,

$$b_n + rb_{n-1} + sb_{n-2} = 0,$$

and let

$$B = \begin{bmatrix} b_3 & b_2 & b_1 \\ b_4 & b_3 & b_2 \\ b_5 & b_4 & b_3 \end{bmatrix}.$$

Since the nonzero vector $[1, r, s]^T$ is in the kernel of B, we must have that

$$0 = \det(B) = -k^2(k-1)\ell((k+\ell-1)^2 + 4\ell).$$

It follows that for b_n to satisfy a smaller recurrence, we must have $k = 0$, $k = 1$, or $\ell = 0$. It is clear that when $k = 0$, we have $b_n = \ell^n = \ell b_{n-1}$. When $k = 1$, we can use Lemma 1.1.2 to see that

$$b_{n+1} = \ell(a_n + \ell a_{n-2}),$$

and combining this with (1.1.9) gives the recurrence stated in the lemma. □

When $k = 1$ and $\ell = 1$, the recurrences given by Lemma 1.1.3 when applied to the families of path graphs and cycle graphs are the Fibonacci and Lucas numbers, respectively. This observation is well-known (see [Kos01, Examples 4.1 and 5.3]) and was brought to our attention by Cox [Cox]:

$$\chi_{P_n}(1,1) = F_{n+2} \qquad \text{and} \qquad \chi_{C_n}(1,1) = L_n. \tag{1.1.11}$$

Moreover, when $k = 2$ and $\ell = 1$, the recurrence given by Lemma 1.1.3 when applied to the family of path graphs is the one associated to the Pell numbers:

$$\chi_{P_n}(2,1) = Q_{n+1},$$

where $Q_0 = 1$, $Q_1 = 1$, and $Q_n = 2Q_{n-1} + Q_{n-2}$.

1.2 Identities

In this section, we derive some identities involving the generalized Fibonacci and Lucas numbers a_n and b_n using the graph coloring interpretation found here.

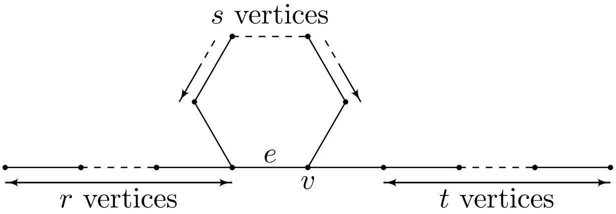
In what follows, we fix $k = 1$. In this case, the a_n and b_n satisfy the following recurrences:

$$a_n = \ell a_{n-1} + \ell a_{n-2} \qquad \text{and} \qquad b_n = \ell b_{n-1} + \ell b_{n-2}.$$

Theorem 1.2.1. *The following identities hold:*

$$\begin{aligned} b_n &= \ell a_{n-1} + \ell^2 a_{n-3}, &(1.2.1)\\ b_n &= a_n - \ell^2 a_{n-4}, &(1.2.2)\\ a_{r+s} &= \ell a_r a_{s-1} + \ell^2 a_{r-1} a_{s-2}, &(1.2.3)\\ a_{r+s} &= a_r a_s - \ell^2 a_{r-2} a_{s-2}, &(1.2.4)\\ a_{r+s+t+1} &= \ell a_r a_s a_t + \ell^3 a_{r-1} a_{s-1} a_{t-1} - \ell^4 a_{r-2} a_{s-2} a_{t-2}. &(1.2.5) \end{aligned}$$

Proof. All of the above identities follow from Lemma 1.1.2 when applied to different graphs (with certain choices of vertices and edges). To see the first two equations, consider the cycle graph C_n and pick any vertex and any edge. To see the next two equations, consider the path graph P_{r+s} with $v = r + 1$ and $e = \{r, r + 1\}$.



In order to prove the final equation in the statement of the theorem, consider the graph G in the above figure. It follows from Lemma 1.1.2 that

$$\ell a_{r+s} a_t + \ell^3 a_{r-1} a_{s-1} a_{t-1} = a_{r+s+t+1} - \ell^4 a_{r-2} a_{s-2} a_{t-1}.$$

Rearranging the terms and applying (1.2.4), we see that

$$\begin{aligned}
a_{r+s+t+1} &= \ell a_{r+s}a_t + \ell^3 a_{r-1}a_{s-1}a_{t-1} + \ell^4 a_{r-2}a_{s-2}a_{t-1} \\
&= \ell(a_r a_s - \ell^2 a_{r-2}a_{s-2})a_t + \ell^3 a_{r-1}a_{s-1}a_{t-1} + \ell^4 a_{r-2}a_{s-2}a_{t-1} \\
&= \ell a_r a_s a_t - \ell^3 a_{r-2}a_{s-2}(\ell a_{t-1} + \ell a_{t-2}) \\
&\qquad + \ell^3 a_{r-1}a_{s-1}a_{t-1} + \ell^4 a_{r-2}a_{s-2}a_{t-1} \\
&= \ell a_r a_s a_t + \ell^3 a_{r-1}a_{s-1}a_{t-1} - \ell^4 a_{r-2}a_{s-2}a_{t-2}.
\end{aligned}$$

This completes the proof of the theorem. □

Corollary 1.2.2. *The following identities hold:*

$$\begin{aligned}
L_n &= F_{n+1} + F_{n-1}, \\
L_n &= F_{n+2} - F_{n-2}, \\
F_{r+s} &= F_{r+1}F_s + F_r F_{s-1}, \\
F_{r+s} &= F_{r+1}F_{s+1} - F_{r-1}F_{s-1}, \\
F_{r+s+t} &= F_{r+1}F_{s+1}F_{t+1} + F_r F_s F_t - F_{r-1}F_{s-1}F_{t-1}.
\end{aligned}$$

Proof. The identities follow from the corresponding ones in Theorem 1.2.1 with $\ell = 1$ by making suitable shifts of the indices and using (1.1.11). □

1.3 Further Exploration

In this note, we have produced recurrences and identities by decomposing different classes of graphs in different ways. Our treatment is by no means exhaustive, and there should be many ways to expand on what we have done here. For instance, is there a graph coloring proof of Cassini's identity?

Part 2

Algebraic Characterization of Uniquely Vertex Colorable Graphs

The study of graph vertex colorability from an algebraic perspective has introduced novel techniques and algorithms into the field. For instance, it is known that k-colorability of a graph G is equivalent to the condition $1 \in I_{G,k}$ for a certain ideal $I_{G,k} \subseteq \Bbbk[x_1, \ldots, x_n]$. In this paper, we extend this result by proving a general decomposition result for $I_{G,k}$. This will allow us to give an algebraic characterization of uniquely k-colorable graphs. Our results also give algorithms for testing (unique) vertex colorability. As an application, we verify a counterexample to a conjecture of Xu concerning uniquely 3-colorable graphs without triangles.

2.1 Introduction

Let G be a simple, undirected graph with vertices $V = \{1, \ldots, n\}$ and edges E. Fix a positive integer $k \leq n$, and let $C_k = \{c_1, \ldots, c_k\}$ be a k-element set. Each element of C_k is called a *color*. A (vertex) *k-coloring* of G is a map $\gamma : V \to C_k$. We say that a k-coloring γ is *proper* if adjacent vertices receive different colors; otherwise γ is *improper*. The graph G is said to be *k-colorable* if there exists a proper k-coloring of G.

Let $\Bbbk$ be an algebraically closed field of characteristic not dividing k. We will be interested in the following ideals of the polynomial ring $\Bbbk[x_1, \ldots, x_n]$ over $\Bbbk$ in indeterminates $x_1, \ldots, x_n$:

$$I_{n,k} = \left\langle x_i^k - 1 : i \in V \right\rangle, \tag{2.1.1}$$

and

$$I_{G,k} = I_{n,k} + \left\langle x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} : \{i,j\} \in E \right\rangle. \tag{2.1.2}$$

One should think of (the zeros of) $I_{n,k}$ and $I_{G,k}$ as representing k-colorings and proper k-colorings of the graph G, respectively (see Section 2.3). The idea of using roots of unity and ideal theory to study graph coloring problems seems to originate in Bayer's thesis [Bay82], although it has appeared in many other places. The following theorem establishes an important connection between the *graph ideal* $I_{G,k}$ and the number of proper k-colorings of G.

Theorem 2.1.1. *The vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$ equals the number of proper k-colorings of G.*

This key theorem seems to have gone unnoticed in the literature. We present a proof of it in Section 2.3.

The ideals $I_{n,k}$ and $I_{G,k}$ are also important because they, together with the *graph polynomial* of G given by

$$f_G = \prod_{\substack{\{i,j\} \in E, \\ i<j}} (x_i - x_j),$$

allow for an algebraic formulation of k-colorability. The following theorem collects some of the results in the series of works [AT92, Bay82, dL95].

Theorem 2.1.2. *The following statements are equivalent:*

(1) *The graph G is not k-colorable.*
(2) *The vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$ is zero.*
(3) *The constant polynomial 1 belongs to the graph ideal $I_{G,k}$.*
(4) *The graph polynomial f_G belongs to the ideal $I_{n,k}$.*

The equivalence between (1) and (2) follows from Theorem 2.1.1. The equivalence between (1) and (3) is due to Bayer [Bay82, pp. 109–112] (see also Chapter 2.7 of [AL94]). Alon and Tarsi [AT92] proved that (1) and (4) are equivalent, but also de Loera [dL95] have proved this using Gröbner basis methods. We give a self-contained and simplified proof of Theorem 2.1.2 in Section 2.3, in part to collect the many facts we need here.

We say that a graph is *uniquely k-colorable* if there is a unique proper k-coloring up to permutation of the colors. In this case, partitions of the vertices into subsets having the same color are the same for each of the $k!$ proper k-colorings of G. A natural refinement of Theorem 2.1.2 would be an algebraic characterization of when a k-colorable graph is uniquely k-colorable. We provide such a characterization.

Theorem 2.1.3. *The following statements are equivalent:*

(1) *The graph G is uniquely k-colorable.*
(2) *The vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$ is $k!$.*
(3) *The polynomials $g_1, \ldots, g_n$ belong to the graph ideal $I_{G,k}$.*
(4) *The graph polynomial f_G belongs to the ideal $I_{n,k} : \langle g_1, \ldots, g_n \rangle$.*

The polynomials $g_1, \ldots, g_n$ in (3) and (4) are given by (2.4.3) *in Lemma 2.4.4 for some proper k-coloring of G, and some complete set of representatives of the color classes.*

Remark 2.1.4. It is important to point out that one need not have a proper k-coloring of a given graph G (nor the polynomials $g_1, \ldots, g_n$) in order to test if G is uniquely k-colorable using (2) of Theorem 2.1.3. This is only necessary when using (3) or (4).

The organization of this paper is as follows. In Section 2.2 we discuss some of the algebraic tools that will go into the proofs of our main results. Section 2.3 is devoted to proofs of Theorems 2.1.1 and 2.1.2. In Section 2.4 we develop the concept of coloring ideals, and use it to prove Theorem 2.1.3. Theorems 2.1.2 and 2.1.3 give algorithms for testing k-colorability and unique k-colorability of graphs, and we discuss an implementation of them in Section 2.5. These algorithms we then use in Section 2.6 to verify a counterexample [AMS01] to a conjecture [Xu90] by Xu concerning uniquely 3-colorable graphs without triangles. In this section we also discuss the tractability of our algorithms. We hope that they might be used to perform experiments for raising and settling problems in the theory of (unique) vertex colorability.

2.2 Algebraic Preliminaries

We briefly review the basic concepts of commutative algebra that will be useful for us here. We refer to [AL94, CLO07, CLO05, KR00] for more details.

Let I be an ideal of $\Bbbk[x_1, \ldots, x_n]$. The *variety* $V(I)$ of I is the set of points in $\Bbbk^n$ that are zeros of all the polynomials in I. Conversely, the *vanishing ideal* $I(V)$ of a set $V \subseteq \Bbbk^n$ is the ideal of those polynomials vanishing on all of V. These two definitions are related by way of $V(I(V)) = V$ and $I(V(I)) = \sqrt{I}$ (the latter equality is known as Hilbert's Nullstellensatz), in which

$$\sqrt{I} = \{f : f^n \in I \text{ for some } n\}$$

is the *radical* of I. The ideal I is said to be a radical ideal if it is equal to its radical. The ideal I is said to be *zero-dimensional* if $V(I)$ is finite.

Many arguments in commutative algebra and algebraic geometry are simplified when restricted to radical, zero-dimensional ideals (resp. multiplicity-free, finite varieties), and those found in this paper are not exceptions. The following two facts are useful in this regard.

Lemma 2.2.1. *Let $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be a zero-dimensional ideal. If I contains a non-zero univariate square-free polynomial in each indeterminate then I is a radical ideal.*

Proof. See [KR00, p. 250, Proposition 3.7.15]. □

Lemma 2.2.2. *Let $I \subseteq \Bbbk[x_1, \dots, x_n]$ be a zero-dimensional ideal. The vector space dimension of $\Bbbk[x_1, \dots, x_n]/I$ over $\Bbbk$ is greater than or equal to the number of points in the variety $V(I)$. Furthermore, equality occurs if and only if I is a radical ideal.*

Proof. See [CLO05, pp. 43–44, Theorem 2.10]. □

A *term order* $\prec$ for the monomials of $\Bbbk[x_1, \dots, x_n]$ is a well-ordering which is multiplicative ($u \prec v \implies wu \prec wv$ for monomials u, v, w) and for which the constant monomial 1 is smallest. The *leading monomial* $\mathrm{lm}_\prec(f)$ of a polynomial $f \in \Bbbk[x_1, \dots, x_n]$ is the largest monomial in f with respect to $\prec$. The *standard monomials* of I are those monomials which are not the leading monomial of any polynomial in I.

Lemma 2.2.3. *Let $I \subseteq \Bbbk[x_1, \dots, x_n]$ be an ideal, and let $\prec$ be a term order. The vector space $\Bbbk[x_1, \dots, x_n]/I$ over $\Bbbk$ is isomorphic to the vector space over $\Bbbk$ spanned by the standard monomials of I.*

Proof. See [CLO07, p. 232, Proposition 4]. □

A finite subset $\mathcal{G}$ of an ideal I is said to be a *Gröbner basis* for I (with respect to the term order $\prec$) if the *leading ideal*,

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

is generated by the leading monomials of elements of $\mathcal{G}$. It is called *minimal* if no leading monomial of $g \in \mathcal{G}$ divides any other leading monomial of polynomials in $\mathcal{G}$. Many of the properties of I and $V(I)$ can be calculated by finding a Gröbner basis for I, and such generating sets are fundamental for computation (including the algorithms presented in Section 2.5).

Finally, a useful operation on two ideals I and J is the construction of the *colon ideal* $I : J = \{f \in \Bbbk[x_1, \dots, x_n] : fJ \subseteq I\}$. If V and W are two varieties, then the colon ideal

$$I(V) : I(W) = I(V \backslash W) \qquad (2.2.1)$$

corresponds to a set difference. We conclude this section by noticing that

$$K \subseteq I : J \iff J \subseteq I : K \qquad (2.2.2)$$

for ideals I, J, and K. The reader is referred to [CLO07, pp. 194–196] for proofs of these facts.

2.3 Characterization of Vertex Colorability

In what follows, the set $C_k = \{c_1, \dots, c_k\}$ of colors will be the set of kth roots of unity, and we shall freely speak of points in $\Bbbk^n$ with all coordinates in C_k as k-colorings of G. In this case, a point $\gamma = (\gamma_1, \dots, \gamma_n) \in \Bbbk^n$ corresponds to a coloring of vertex i with color γ_i for $i = 1, \dots, n$. Furthermore, let $\Gamma_{n,k} \subseteq \Bbbk^n$ be the set of all k-colorings of G, and let $\Gamma_{G,k} \subseteq \Bbbk^n$ be the set of all proper k-colorings of G.

The next result will prove useful in simplifying many of the proofs in this section and the next one.

Lemma 2.3.1. *$I_{n,k}$ and $I_{G,k}$ are zero-dimensional radical ideals.*

Proof. Equations (2.1.1) and (2.1.2) show that $V(I_{G,k}) \subseteq V(I_{n,k}) = \Gamma_{n,k}$, which means that $I_{n,k}$ and $I_{G,k}$ are zero-dimensional.

If we let $f_i = x_i^k - 1$ then $f_i' = kx_i^{k-1} \neq 0$, since the characteristic of $\Bbbk$ does not divide k. This shows that $\gcd(f_i, f_i') = 1$ and so f_i is square-free. It now follows from Lemma 2.2.1 that $I_{n,k}$ is a radical ideal. The same argument works for $I_{G,k}$, since $I_{n,k} \subseteq I_{G,k}$. □

Lemma 2.3.2. *$I_{n,k}$ and $I_{G,k}$ are the vanishing ideals of the set of all k-colorings of G and the set of all proper k-colorings of G, respectively.*

Proof. From Equation (2.1.1) it is clear that $V(I_{n,k}) = \Gamma_{n,k}$. Hilbert's Nullstellensatz then tells us that $I_{n,k} = I(\Gamma_{n,k})$, since $I_{n,k}$ is a radical ideal.

From Equation (2.1.2) it is not quite so obvious that $V(I_{G,k}) = \Gamma_{G,k}$. To see this, first notice that $V(I_{G,k}) \subseteq V(I_{n,k}) = \Gamma_{n,k}$. Next, let

$$h_{\{i,j\}}^{k-1} = x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1},$$

and let $\gamma = (\gamma_1, \dots, \gamma_n) \in \Gamma_{n,k}$ be any k-coloring of G. If γ is improper there exists an edge $\{i,j\} \in E$ for which $\gamma_i = \gamma_j$. Then $h_{\{i,j\}}^{k-1}(\gamma) = k\gamma_i^{k-1} \neq 0$, since the characteristic of $\Bbbk$ does not divide k. This shows that $V(I_{G,k}) \subseteq \Gamma_{G,k}$. To get the reverse direction, notice that

$$(\gamma_i - \gamma_j)h^{k-1}_{\{i,j\}}(\gamma) = \gamma_i^k - \gamma_j^k = 1 - 1 = 0.$$

Hence, if γ is proper, we have $h^{k-1}_{\{i,j\}}(\gamma) = 0$ for all $\{i, j\} \in E$. This shows that $\Gamma_{G,k} \subseteq V(I_{G,k})$. As before, Hilbert's Nullstellensatz tells us that $I_{G,k} = I(\Gamma_{G,k})$, since $I_{G,k}$ is also a radical ideal. □

We are now in a position to prove our first main theorem.

Proof of Theorem 2.1.1. According to Lemma 2.2.2, the vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$ equals the number of points in the variety $V(I_{G,k})$, since $I_{G,k}$ is a radical ideal. The result now follows since $V(I_{G,k})$ is the set of all proper k-colorings of G as a result of Lemma 2.3.2. □

The next result describes a simple relationship between the ideals $I_{n,k}$ and $I_{G,k}$, and the graph polynomial f_G.

Lemma 2.3.3. $I_{n,k} : \langle f_G \rangle = I_{G,k}$.

Proof. The first step is to note that $\langle f_G \rangle$ is a radical ideal. This follows from [CLO07, p. 180, Proposition 9], since f_G is square-free. Hilbert's Nullstellensatz then implies that

$$\langle f_G \rangle = I(V(\langle f_G \rangle)). \tag{2.3.1}$$

Next, let $\gamma = (\gamma_1, \ldots, \gamma_n) \in \Gamma_{n,k}$ be any k-coloring of G. It is clear that $f_G(\gamma) = 0$ if and only if γ is improper. Hence, we see that

$$\Gamma_{n,k} \backslash V(\langle f_G \rangle) = \Gamma_{G,k}. \tag{2.3.2}$$

The result now follows from the string of equations:

$$\begin{aligned}
I_{n,k} : \langle f_G \rangle &= I(\Gamma_{n,k}) : \langle f_G \rangle && \text{by Lemma 2.3.2} \\
&= I(\Gamma_{n,k}) : I(V(\langle f_G \rangle)) && \text{by Equation (2.3.1)} \\
&= I(\Gamma_{n,k} \backslash V(\langle f_G \rangle)) && \text{by Equation (2.2.1)} \\
&= I(\Gamma_{G,k}) && \text{by Equation (2.3.2)} \\
&= I_{G,k} && \text{by Lemma 2.3.2.}
\end{aligned}$$

□

We now prove Theorem 2.1.2. We feel that it is the most efficient proof of this result.

Proof of Theorem 2.1.2.

(1) $\iff$ (2)**:** The graph G is not k-colorable if and only if the number of proper k-colorings of G is zero. Theorem 2.1.1 shows that this happens if and only if the vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$ is zero.

(2) $\iff$ (3)**:** The vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ is zero if and only if $I_{G,k} = \Bbbk[x_1, \ldots, x_n]$, which is the case if and only if the constant polynomial 1 belongs to the graph ideal $I_{G,k}$.

(3) $\iff$ (4)**:** Recall that $I_{n,k} : \langle f_G \rangle = I_{G,k}$ according to Lemma 2.3.3, and notice that $I_{n,k} : \langle 1 \rangle = I_{n,k}$ by definition. The equivalence now follows from (2.2.2) with $I = I_{n,k}$, $J = \langle f_G \rangle$, and $K = \langle 1 \rangle$.

□

2.4 Characterization of Unique Vertex Colorability

Let γ be any k-coloring of G. Any k-coloring of G that arises from γ by a permutation of the colors is said to be *essentially identical* to γ. Let $\Gamma_{G,\gamma} \subseteq \Bbbk^n$ be the set of all k-colorings of G that are essentially identical to γ. The vanishing ideal $I(\Gamma_{G,\gamma})$ is said to be the *coloring ideal* $I_{G,\gamma}$ associated to γ.

Our first result about coloring ideals is the following simple lemma, which is an analogue of Lemma 2.3.1.

Lemma 2.4.1. *$I_{G,\gamma}$ is a zero-dimensional radical ideal.*

Proof. The variety $V(I_{G,\gamma}) = \Gamma_{G,\gamma}$ is finite since there is only a finite number of permutations of the k colors. Any vanishing ideal is a radical ideal. □

In fact, it is not difficult to determine the exact number of k-colorings of G that are essentially identical to γ. If γ uses $\ell \leq k$ of the available colors, then the number of such k-colorings is

$$|\Gamma_{G,\gamma}| = \binom{k}{\ell}\ell!. \tag{2.4.1}$$

The next result is similar to Lemma 2.3.3, but instead it decomposes the graph ideal $I_{G,k}$ in terms of coloring ideals.

Lemma 2.4.2. $\bigcap_{\gamma\in\Gamma_{G,k}} I_{G,\gamma} = I_{G,k}$.

Proof. If $\gamma \in \Gamma_{G,k}$ is a proper k-colorings of G, then all essentially identical k-colorings of G are proper too. Hence, we see that

$$\bigcup_{\gamma\in\Gamma_{G,k}} \Gamma_{G,\gamma} = \Gamma_{G,k}. \tag{2.4.2}$$

The result now follows from the string of equations:

$$\begin{aligned}
\bigcap_{\gamma\in\Gamma_{G,k}} I_{G,\gamma} &= \bigcap_{\gamma\in\Gamma_{G,k}} I(\Gamma_{G,\gamma}) && \text{by definition} \\
&= I(\Gamma_{G,k}) && \text{by Equation (2.4.2)} \\
&= I_{G,k} && \text{by Lemma 2.3.2.}
\end{aligned}$$

□

For a subset $U \subseteq V$ of vertices and a positive integer d, let h_U^d be the sum of all monomials of degree d in the indeterminates $\{x_\ell : \ell \in U\}$. Also, let $h_U^0 = 1$. The polynomial h_U^d is obviously homogeneous of degree d, and symmetric in the indeterminates $\{x_\ell : \ell \in U\}$.

The following lemma is a very important ingredient in the proof of Lemma 2.4.4.

Lemma 2.4.3. *If $\{i,j\} \subseteq U$, then*

$$(x_i - x_j)h_U^d = h_{U\setminus\{j\}}^{d+1} - h_{U\setminus\{i\}}^{d+1},$$

for all non-negative integers d.

Proof. The first step is to note that the polynomial $x_i h_U^d + h_{U\setminus\{i\}}^{d+1}$ is symmetric in the indeterminates $\{x_\ell : \ell \in U\}$. This follows from the polynomial identity

$$h_U^{d+1} - h_{U\setminus\{i\}}^{d+1} = x_i h_U^d,$$

and the fact that h_U^{d+1} is symmetric in the indeterminates $\{x_\ell : \ell \in U\}$. Let σ be the transposition $(i\ j)$, and note that

$$x_i h_U^d + h_{U\setminus\{i\}}^{d+1} = \sigma\left(x_i h_U^d + h_{U\setminus\{i\}}^{d+1}\right) = x_j h_U^d + h_{U\setminus\{j\}}^{d+1}.$$

This concludes the proof. □

The next result is an important technical lemma that describes special sets of generators for coloring ideals.

Lemma 2.4.4. *Let γ be any k-coloring of G, and let $\{v_1, \dots, v_\ell\} \subseteq V$ be any complete set of representatives of the color classes in which γ partitions V. For any vertex $i \in V$, denote by $v(i)$ the representative having the same color as i. The coloring ideal $I_{G,\gamma}$ associated to γ is generated by the polynomials $g_1, \dots, g_n$ defined by*

$$g_i = \begin{cases} x_{v_1}^k - 1 & \textit{if } i = v_1, \\ h_{\{v_1,\dots,v_j\}}^{k+1-j} & \textit{if } i = v_j \textit{ for any } j > 1, \\ x_i - x_{v(i)} & \textit{otherwise.} \end{cases} \tag{2.4.3}$$

Moreover, the set $\mathcal{G} = \{g_1, \dots, g_n\}$ of polynomials form a minimal Gröbner basis for the ideal $I_{G,\gamma}$ with respect to any term order $\prec$ satisfying $x_{v_1} \prec \cdots \prec x_{v_\ell}$, and $x_{v(i)} \prec x_i$ for all vertices $i \in V \setminus \{v_1, \dots, v_\ell\}$.

Proof. We begin by proving that $I = \langle g_1, \dots, g_n\rangle$ vanishes on all the k-colorings of G that are essentially identical to γ. Suppose $\delta = (\delta_1, \dots, \delta_n) \in \Gamma_{G,\gamma}$ is such a k-coloring of G. First of all, it is obvious that

$$g_{v_1}(\delta) = \delta_{v_1}^k - 1 = 1 - 1 = 0.$$

We will prove that also $g_{v_2}, \dots, g_{v_\ell}$ vanish on δ by establishing the following stronger statement using induction on $|U|$:

$$h_U^{k+1-|U|}(\delta) = 0 \text{ for all subsets } U \subseteq \{v_1, \dots, v_\ell\} \text{ with } |U| > 1. \tag{$*$}$$

In the case $|U| = 2$, we have $U = \{u_1, u_2\}$. It is easily verified that

$$(\delta_{u_1} - \delta_{u_2})h_U^{k-1}(\delta) = \delta_{u_1}^k - \delta_{u_2}^k = 1 - 1 = 0.$$

Since $U \subseteq \{v_1, \ldots, v_\ell\}$, we have $\delta_{u_1} \neq \delta_{u_2}$ and so $h_U^{k-1}(\delta) = 0$. This shows that $(*)$ holds for all subsets $U \subseteq \{v_1, \ldots, v_\ell\}$ with $|U| = 2$. In the general case, we have $\{u_1, u_2\} \subset U$. It now follows from Lemma 2.4.3 and the induction hypothesis, that

$$(\delta_{u_1} - \delta_{u_2})h_U^{k+1-|U|}(\delta) = h_{U\setminus\{u_2\}}^{k+1-|U\setminus\{u_2\}|}(\delta) - h_{U\setminus\{u_1\}}^{k+1-|U\setminus\{u_1\}|}(\delta) = 0.$$

As before, we have $h_U^{k+1-|U|}(\delta) = 0$, and this completes the proof of $(*)$. Finally we need to show that the remaining generators of I also vanish on δ. This follows immediately from that fact that

$$g_i(\delta) = \delta_i - \delta_{v(i)} = 0,$$

since δ partitions V into the same color classes as γ does, and $v(i)$ is the representative having the same color as $i \in V$. We have therefore now proved that I vanishes on all the k-colorings of G that are essentially identical to γ, that is, $I \subseteq I_{G,\gamma}$. It now follows immediately that

$$V(I) \supseteq V(I_{G,\gamma}). \tag{2.4.4}$$

We continue the proof by showing that the ideals I and $I_{G,\gamma}$ give rise to the same variety. Let $\prec$ be any term order satisfying $x_{v_1} \prec \cdots \prec x_{v_\ell}$, and $x_{v(i)} \prec x_i$ for all vertices $i \in V\setminus\{v_1, \ldots, v_\ell\}$. By inspecting (2.4.3) we see that the leading monomial of g_i is given by

$$\mathrm{lm}_\prec(g_i) = \begin{cases} x_i^{k+1-j} & \text{if } i = v_j \text{ for any } j \geq 1, \\ x_i & \text{otherwise.} \end{cases}$$

The leading monomials of $g_1, \ldots, g_n$ are therefore pairwise relatively prime. It follows that the set $\mathcal{G} = \{g_1, \ldots, g_n\}$ of polynomials form a minimal Gröbner basis for the ideal I with respect to the term order $\prec$ (see [AL94, Theorem 1.7.4 and Lemma 3.3.1]). Furthermore, for each $i = 1, \ldots, n$ there is a $g \in \mathcal{G}$ with leading monomial that is a power of x_i. This implies that $V(I)$ is finite, that is, I is a zero-dimensional ideal (see [AL94, Theorem 2.2.7]).

The set of standard monomials of I with respect to $\prec$ is readily seen to be the set

$$S = \left\{x_{v_j}^{\alpha_j} : \alpha_j < k + 1 - j \text{ for } j = 1, \ldots, \ell\right\}. \tag{2.4.5}$$

The vector space $\Bbbk[x_1, \ldots, x_n]/I$ is, according to Lemma 2.2.3, isomorphic to the vector space over $\Bbbk$ spanned by S, that is,

$$\Bbbk[x_1, \ldots, x_n]/I \simeq \operatorname{span}_{\Bbbk} S. \tag{2.4.6}$$

We may now write

$$\begin{aligned} k(k-1)\cdots(k+1-\ell) &= |\Gamma_{G,\gamma}| && \text{by Equation (2.4.1)} \\ &= |V(I_{G,\gamma})| && \text{by definition} \\ &\leq |V(I)| && \text{by (2.4.4)} \\ &\leq \dim \Bbbk[x_1, \ldots, x_n]/I && \text{by Lemma 2.2.2} \\ &= \dim \operatorname{span}_{\Bbbk} S && \text{by (2.4.6)} \\ &= k(k-1)\cdots(k+1-\ell) && \text{by (2.4.5).} \end{aligned}$$

Hence, equality holds throughout. In particular, we have $|V(I_{G,\gamma})| = |V(I)|$ which, together with (2.4.4), shows that the ideals I and $I_{G,\gamma}$ give rise to the same variety, that is,

$$V(I) = V(I_{G,\gamma}). \tag{2.4.7}$$

Furthermore, we also see that the vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I$ over $\Bbbk$ equals the number of points in the variety $V(I)$, and so I is a radical ideal according to Lemma 2.2.2. Since $I_{G,\gamma}$, by Lemma 2.4.1, is also a radical ideal, Equation (2.4.7) and Hilbert's Nullstellensatz finally imply that $I = I_{G,\gamma}$, which then concludes the proof. □

We present three examples that demonstrate Lemma 2.4.4.

Example 2.4.5. Let G be the complete graph on n vertices, and let γ be any proper n-coloring of G. The color classes each consist of a single vertex, and so we may choose the representative $v_j = j$ for $j = 1, \ldots, n$. The coloring ideal associated to γ is therefore given by

$$I_{G,\gamma} = \left\langle x_1^n - 1, x_1^{n-1} + x_1^{n-2}x_2 + \cdots + x_1x_2^{n-2} + x_2^{n-1}, \ldots, x_1 + \cdots + x_n \right\rangle.$$

Example 2.4.6. Let G be the graph in Figure 2.1, and let γ be the indicated 3-coloring of G. We may choose the set $v_1 = 12$, $v_2 = 11$, and $v_3 = 10$ as representatives of the color classes in which γ partitions V. The coloring ideal

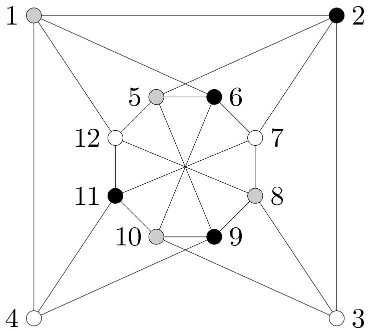


Figure 2.1: A uniquely 3-colorable graph without triangles [CC93].

associated to γ is therefore given by

$$\begin{aligned}I_{G,\gamma} = \langle & \underline{x_{12}^3} - 1,\ \underline{x_7} - x_{12},\ \underline{x_4} - x_{12},\ \underline{x_3} - x_{12},\\ & \underline{x_{11}^2} + x_{11}x_{12} + x_{12}^2,\ \underline{x_9} - x_{11},\ \underline{x_6} - x_{11},\ \underline{x_2} - x_{11},\\ & \underline{x_{10}} + x_{11} + x_{12},\ \underline{x_8} - x_{10},\ \underline{x_5} - x_{10},\ \underline{x_1} - x_{10}\rangle.\end{aligned}$$

The generators form a minimal Gröbner basis for the ideal $I_{G,\gamma}$ with respect to any term ordering with e.g. $x_{12} \prec \cdots \prec x_1$. The leading term (with respect to such a term order) of each polynomial is underlined. Notice that the leading terms of the polynomials in each line correspond to the different color classes of this coloring of G.

The third example also demonstrates Lemma 2.4.2.

Example 2.4.7. Let $G = (\{1, 2, 3\}, \{\{1, 2\}, \{2, 3\}\})$ be the path graph on three vertices. There are essentially two proper 3-colorings of G: the one where vertices 1 and 3 receive the same color, and the one where all the vertices receive different colors. If we denote by γ_1 the former, and by γ_2 the latter, it follows from Lemma 2.4.4 that

$$\begin{aligned}I_{G,\gamma_1} &= \left\langle x_1^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_3 - x_1\right\rangle,\\ I_{G,\gamma_2} &= \left\langle x_1^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_1 + x_2 + x_3\right\rangle.\end{aligned}$$

Lemma 2.4.2 predicts that the intersection $I_{G,\gamma_1} \cap I_{G,\gamma_2}$ is equal to the graph ideal

$$I_{G,3} = \left\langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_2^2 + x_2x_3 + x_3^2 \right\rangle .$$

It is possible to verify this using the computer algebra system Singular as shown by the following piece of code. For more information about Singular and the libraries `graph.lib` and `ideals.lib` that are being used, the reader is referred to Section 2.7.

```
> int n = 3;
> ring R = 0, x(1..n), lp;
> list G = pathgraph(n);
> list gamma1 = 3, list(intvec(1,3), 2);
> ideal I1 = I(G, gamma1);
> I1;
I1[1]=x(1)^3-1
I1[2]=x(1)^2+x(1)*x(2)+x(2)^2
I1[3]=-x(1)+x(3)
> list gamma2 = 3, list(1, 2, 3);
> ideal I2 = I(G, gamma2);
> I2;
I2[1]=x(1)^3-1
I2[2]=x(1)^2+x(1)*x(2)+x(2)^2
I2[3]=x(1)+x(2)+x(3)
> groebner(intersect(I1, I2));
_[1]=x(3)^3-1
_[2]=x(2)^2+x(2)*x(3)+x(3)^2
_[3]=x(1)^2+x(1)*x(2)-x(2)*x(3)-x(3)^2
> groebner(I(G, 3));
_[1]=x(3)^3-1
_[2]=x(2)^2+x(2)*x(3)+x(3)^2
_[3]=x(1)^2+x(1)*x(2)-x(2)*x(3)-x(3)^2
```

The two Gröbner basis computations yield the same result, which means the two ideals $I_{G,\gamma_1} \cap I_{G,\gamma_2}$ and $I_{G,3}$ are the same.

We are now ready to prove our characterization of uniquely k-colorable graphs. Before we begin though, we need the following elementary observation.

Lemma 2.4.8. *If a graph G is k-colorable, then there exists a proper k-coloring of G that uses all k colors.*

Proof. Suppose γ is a proper k-coloring of a graph G. If γ uses all k colors, then we are done. Now suppose γ uses only $\ell < k$ colors. Then $\ell < n$ so there must be two vertices with the same color. Give one of these one of the unused colors. The resulting k-coloring of G is still proper but uses $\ell + 1$ colors. Continue this way until a proper k-coloring of G that uses all k colors is reached. □

Proof of Theorem 2.1.3.

(1) $\Longleftrightarrow$ (2)**:** Suppose the graph G is uniquely k-colorable. By Lemma 2.4.8 there exists a proper k-coloring of G that uses all k colors. Since G is uniquely k-colorable, all other proper k-colorings of G are essentially identical to this one. Thus, the number of proper k-colorings of G is $k!$ and so, the result now follows from Theorem 2.1.1.

Conversely, suppose the vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$ is $k!$. Theorem 2.1.1 implies that G is k-colorable, and that the number of proper k-colorings of G is $k!$. Lemma 2.4.8 then yields a proper k-coloring of G that uses all k colors and so, all other proper k-colorings of G must be essentially identical to this one. This means that the graph G is uniquely k-colorable.

(2) $\Longleftrightarrow$ (3)**:** Suppose the vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$ is $k!$. Theorem 2.1.1 implies that G is k-colorable, and that the number of proper k-colorings of G is $k!$. Lemma 2.4.8 then yields a proper k-coloring γ of G that uses all k colors. Furthermore, all other proper k-colorings of G must be essentially identical to γ. Let the polynomials $g_1, \ldots, g_n$ be given by (2.4.3) in Lemma 2.4.4 for some complete set $\{v_1, \ldots, v_\ell\} \subseteq V$ of representatives of the color classes. Lemma 2.4.4 now shows that the coloring ideal $I_{G,\gamma}$ is generated by the polynomials $g_1, \ldots, g_n$. The result now follows from Lemma 2.4.2 which tells us that $I_{G,\gamma} = I_{G,k}$.

Conversely, suppose polynomials $g_1, \ldots, g_n$ are given by (2.4.3) in Lemma 2.4.4 for some proper k-coloring γ of G, and some complete set of representatives of the color classes. Furthermore, suppose the polynomials $g_1, \ldots, g_n$ belongs to the graph ideal $I_{G,k}$. Lemma 2.4.4 implies that the coloring ideal $I_{G,\gamma}$ is generated by $g_1, \ldots, g_n$. Hence, we must have

$I_{G,\gamma} \subseteq I_{G,k}$. Now, according to Lemma 2.4.2, $\bigcap_{\gamma \in \Gamma_{G,k}} I_{G,\gamma} = I_{G,k}$, and so $I_{G,\gamma} = I_{G,k}$. This means that all proper k-colorings of G are essentially identical to γ, and so Lemma 2.4.8 implies that γ uses all k colors. Hence, the number of proper k-colorings of G is $k!$. The result now follows from Theorem 2.1.1.

(3) $\Longleftrightarrow$ (4): Recall that $I_{n,k} : \langle f_G \rangle = I_{G,k}$ according to Lemma 2.3.3. The equivalence now follows from (2.2.2) with $I = I_{n,k}$, $J = \langle f_G \rangle$, and $K = \langle g_1, \ldots, g_n \rangle$.

□

2.5 Algorithms for Testing (Unique) Vertex Colorability

In this section we describe the algorithms for testing (unique) vertex colorability implied by Theorems 2.1.2 and 2.1.3. We do so through a series of examples using the computer algebra system Singular. The reader is referred to Section 2.7 for more information on Singular and the libraries `graph.lib` and `ideals.lib` that are being used.

In the first three examples – the ones regarding vertex colorability – we use the non-uniquely 3-colorable graph $G_1 = (\{1,2,3,4\}, \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}\})$ as well as the not 3-colorable complete graph $G_2 = K_4$ on four vertices as examples.

Example 2.5.1 (Testing if a graph is k-colorable using (2) of Theorem 2.1.2)**.** The command `vdim(groebner(I(G, k)));` returns the vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$, which is zero if and only if the graph G is not k-colorable.

```
> int n = 4;
> ring R = 0, x(1..n), lp;
> list G1 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3)));
> vdim(groebner(I(G1, 3)));
12
> list G2 = completegraph(n);
> vdim(groebner(I(G2, 3)));
0
```

Example 2.5.2 (Testing if a graph is k-colorable using (3) of Theorem 2.1.2). The command `reduce(1, groebner(I(G, k)));` returns 0 if and only if the constant polynomial 1 belongs to the ideal $I_{G,k}$, that is, if and only if the graph G is not k-colorable.

```
> int n = 4;
> ring R = 0, x(1..n), lp;
> list G1 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3)));
> reduce(1, groebner(I(G1, 3)));
1
> list G2 = completegraph(n);
> reduce(1, groebner(I(G2, 3)));
0
```

Example 2.5.3 (Testing if a graph is k-colorable using (4) of Theorem 2.1.2). The command `reduce(f(G), I(n, k));` returns 0 if and only if the graph polynomial f_G belongs to the ideal $I_{n,k}$, that is, if and only if the graph G is not k-colorable.

```
> int n = 4;
> ring R = 0, x(1..n), lp;
> list G1 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3)));
> reduce(f(G1), I(n, 3));
-x(1)^2*x(2)^2-x(1)^2*x(2)*x(4)+x(1)^2*x(3)^2+x(1)^2*x(3)*x(4)
+x(1)*x(2)^2*x(3)+x(1)*x(2)^2*x(4)-x(1)*x(2)*x(3)^2
-x(1)*x(3)^2*x(4)-x(2)^2*x(3)*x(4)+x(2)*x(3)^2*x(4)+x(2)-x(3)
> list G2 = completegraph(n);
> reduce(f(G2), I(n, 3));
0
```

The reason we need not compute a Gröbner basis for the ideal $I_{n,k}$ before making the reductions, is that the generators $\mathcal{G} = \left\{x_1^k - 1, \ldots, x_n^k - 1\right\}$ already form a Gröbner basis for $I_{n,k}$ with respect to any term order. This follows easily since the leading terms of the polynomials of $\mathcal{G}$ are relatively prime, regardless of term order [AL94, Theorem 1.7.4 and Lemma 3.3.1].

In the last three examples – the ones regarding unique vertex colorability – we do not use the graph $G_2 = K_4$. Instead we replace it with the uniquely 3-colorable graph $G_2 = (\{1,2,3,4\}, \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}\})$.

Example 2.5.4 (Testing if a graph is uniquely k-colorable using (2) of Theorem 2.1.3). The command `vdim(groebner(I(G, k)));` returns the vector space dimension of $\Bbbk[x_1, \ldots, x_n]/I_{G,k}$ over $\Bbbk$, which is $k!$ if and only if the graph G is uniquely k-colorable.

```
> int n = 4;
> ring R = 0, x(1..n), lp;
> list G1 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3)));
> vdim(groebner(I(G1, 3)));
12
> list G2 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3),e(2,4)));
> vdim(groebner(I(G2, 3)));
6
```

Example 2.5.5 (Testing if a graph is uniquely k-colorable using (3) of Theorem 2.1.3). In this example we choose work with the proper 3-coloring γ of both G_1 and G_2 given by the partition $\{\{1\}, \{2\}, \{3,4\}\}$ of the set of vertices. Furthermore, the set $\{1,2,3\}$ is chosen as the complete set of representatives of the color classes when constructing the polynomials $g_1, \ldots, g_n$ given by (2.4.3) in Lemma 2.4.4.

The command `quotient(I(G, k), I(G, gamma));` returns a set of generators of the colon ideal $I_{G,k} : I_{G,\gamma}$. The colon ideal equals the polynomial ring $\Bbbk[x_1, \ldots, x_n]$ if and only if $I_{G,\gamma} \subseteq I_{G,k}$. Hence, the constant polynomial 1 belongs to the colon ideal $I_{G,k} : I_{G,\gamma}$ if and only if the polynomials $g_1, \ldots, g_n$ belong to the graph ideal $I_{G,k}$, that is, if and only if the graph G is uniquely k-colorable.

```
> int n = 4;
> ring R = 0, x(1..n), lp;
> list gamma = 3, list(1, 2, intvec(3, 4));
> list G1 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3)));
> quotient(I(G1, 3), I(G1, gamma));
_[1]=x(4)^3-1
_[2]=x(3)^2+x(3)*x(4)+x(4)^2
```

```
_[3]=x(2)-x(4)
_[4]=x(1)+x(3)+x(4)
> list G2 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3),e(2,4)));
> quotient(I(G2, 3), I(G2, gamma));
_[1]=1
```

Example 2.5.6 (Testing if a graph is uniquely k-colorable using (4) of Theorem 2.1.3)**.** In this example we choose work with the proper 3-coloring γ of both G_1 and G_2 given by the partition $\{\{1\},\{2\},\{3,4\}\}$ of the set of vertices. Furthermore, the set $\{1,2,3\}$ is chosen as the complete set of representatives of the color classes when constructing the polynomials $g_1,\ldots,g_n$ given by (2.4.3) in Lemma 2.4.4.

The command `reduce(f(G), groebner(quotient(I(n,k), I(G,gamma))));` returns 0 if and only if the graph polynomial f_G belongs to the ideal $I_{n,k} : I_{G,\gamma}$, that is, if and only if the graph G is uniquely k-colorable.

```
> int n = 4;
> ring R = 0, x(1..n), lp;
> list gamma = 3, list(1, 2, intvec(3, 4));
> list G1 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3)));
> reduce(f(G1), groebner(quotient(I(n, 3), I(G1, gamma))));
-x(1)^2*x(2)^2-x(1)^2*x(2)*x(4)+x(1)^2*x(3)^2+x(1)^2*x(3)*x(4)
+x(1)*x(2)^2*x(3)+x(1)*x(2)^2*x(4)-x(1)*x(2)*x(3)^2
-x(1)*x(3)^2*x(4)-x(2)^2*x(3)*x(4)+x(2)*x(3)^2*x(4)+x(2)-x(3)
> list G2 = list(1..n, list(e(1,2),e(1,3),e(1,4),e(2,3),e(2,4)));
> reduce(f(G2), groebner(quotient(I(n, 3), I(G2, gamma))));
0
```

2.6 Verification of a Counterexample to Xu's Conjecture

In [Xu90], Xu showed that if G is a uniquely k-colorable graph with $|V| = n$ and $|E| = m$, then $m \geq (k-1)n - k(k-1)/2$, and this bound is best possible. He went on to conjecture that if G is uniquely k-colorable with $|V| = n$ and $m = (k-1)n - k(k-1)/2$, then G contains a k-clique. In [AMS01], this conjecture was shown to be false for $k = 3$ and $|V| = 24$ using the graph in Figure 2.2; however, the proof is somewhat complicated. We verified that this graph is indeed a counterexample to Xu's conjecture using several of the methods described in Section 2.5. The fastest verification requires less than a second of processor time on a laptop PC with a 1.5 GHz Intel Pentium M processor and 1.5 GB of memory running Windows Vista.

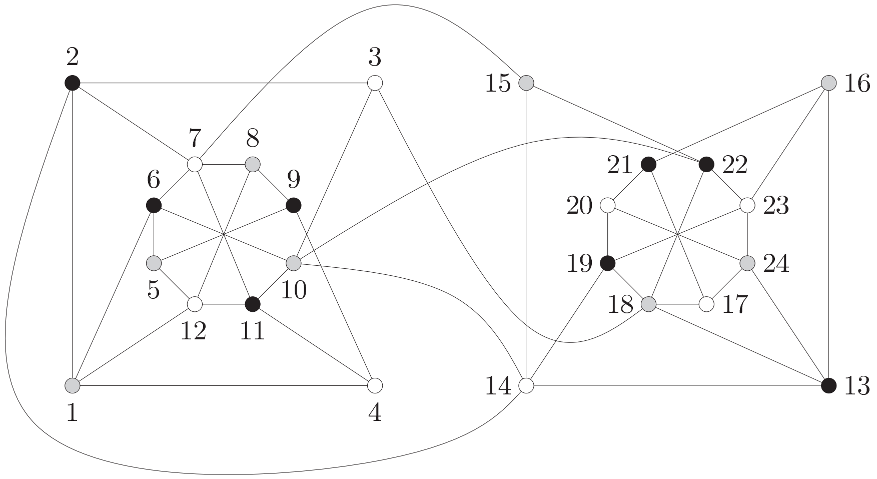


Figure 2.2: A counterexample to Xu's conjecture [AMS01].

Below are the runtimes for the graphs in Figures 1 and 2. The term orders used is given using the usual SINGULAR syntax: `lp` is the lexicographical ordering, `Dp` is the degree lexicographical ordering, and `dp` is the degree reverse lexicographical ordering. All term orders $\prec$ used had $x_1 \prec \cdots \prec x_n$. The symbol $\gg$ indicates that the computation did not finish within 10 minutes.

In order to speed up the computations, basically two types of optimizations were made to the algorithms described in Section 2.5:

(1) When computing a Gröbner basis for the graph ideal $I_{G,k}$ in Example 2.5.1, it helps to add the edges one at a time. This means that the command `vdim(groebner(I(G, k)));` was replaced with the following piece of code:

```
int i, j;
ideal A = I(n, k);
for (int l = 1; l <= size(E(G)); l++)
{
  i, j = E(G)[l];
  A = groebner(A + ideal(h(intvec(i,j), k - 1)));
}
vdim(A);
```

Similar optimizations were made to the algorithms described in Examples 2.5.2, 2.5.4, and 2.5.5.

(2) The number of terms in the graph polynomial f_G when fully expanded may be very large. In the algorithm described in Example 2.5.3, the reduction of the graph polynomial was therefore done iteratively. This means that command `reduce(f(G), I(n, k));` was replaced with the following piece of code:

```
int i, j;
poly p = 1;
for (int l = 1; l <= size(E(G)); l++)
{
  i, j = E(G)[l];
  p = reduce((x(i) - x(j)) * p, I(n, k));
}
p;
```

A similar optimization was made to the algorithm described in Example 2.5.6.

Characteristic of $\Bbbk$	0			2		
Term order	`lp`	`Dp`	`dp`	`lp`	`Dp`	`dp`
Theorem 2.1.2 (2)	0.406	0.187	0.156	0.282	0.109	0.109
Theorem 2.1.2 (3)	0.437	0.188	0.140	0.297	0.094	0.094
Theorem 2.1.2 (4)	148.750	$\gg$	$\gg$	43.797	558.844	$\gg$
Theorem 2.1.3 (2)	0.437	0.187	0.156	0.298	0.125	0.109
Theorem 2.1.3 (3)	0.453	0.204	0.171	0.297	0.157	0.108
Theorem 2.1.3 (4)	161.813	$\gg$	$\gg$	38.735	397.780	368.313

Runtimes in seconds for the graph in Figure 1.

Characteristic of $\Bbbk$	0			2		
Term order	`lp`	`Dp`	`dp`	`lp`	`Dp`	`dp`
Theorem 2.1.2 (2)	4.421	1.313	0.828	2.016	0.781	0.578
Theorem 2.1.2 (3)	4.312	1.266	0.828	2.016	0.781	0.562
Theorem 2.1.2 (4)	$\gg$	$\gg$	$\gg$	$\gg$	$\gg$	$\gg$
Theorem 2.1.3 (2)	4.375	1.265	0.844	2.032	0.781	0.593
Theorem 2.1.3 (3)	4.485	1.313	0.875	2.077	0.797	0.625
Theorem 2.1.3 (4)	$\gg$	$\gg$	$\gg$	$\gg$	$\gg$	$\gg$

Runtimes in seconds for the graph in Figure 2.

Another way one might prove that a graph G is uniquely k-colorable is by computing the chromatic polynomial $\chi_G(x)$ and testing if it equals $k!$ when evaluated at $x = k$. This is actually possible for the graph in Figure 1. MAPLE reports that it has chromatic polynomial

$$\begin{aligned} &x(x-2)(x-1)(x^9 - 20x^8 + 191x^7 - 1145x^6 + 4742x^5 \\ &\qquad\qquad - 14028x^4 + 29523x^3 - 42427x^2 + 37591x - 15563). \end{aligned}$$

When evaluated at $x = 3$ we get the expected result $6 = 3!$. Computing the above chromatic polynomial took 94.83 seconds. MAPLE, on the other hand, was not able to compute the chromatic polynomial of the graph in Figure 2 within 10 hours.

2.7 SINGULAR Libraries

The computer algebra system SINGULAR[1] is used extensively in this paper. SINGULAR is especially designed for doing symbolic computations in algebra. In particular, it has some of the fastest routines for doing Gröbner basis computations which are central to the algorithms presented in this paper (see Sections 2.5 and 2.6).

All the SINGULAR examples presented in this paper use the libraries `graph.lib` and `ideals.lib` described below. They are loaded with the commands:

```
LIB "graph.lib";
LIB "ideals.lib";
```

Furthermore, we used the options:

```
option(redSB);
option(noredefine);
```

The option `redSB` tells SINGULAR to compute so-called reduced Gröbner bases by default, while the option `noredefine` simply tells SINGULAR not to give any warning when variables are being redefined.

2.7.1 graph.lib

SINGULAR does not have any built-in structures or routines for doing computations with graphs. Hence, we have made our own structures.

A graph $G = (V, E)$ is being represented by a `list` with two entries: V and E. The first entry V is of type `intvec`, which is an integer vector, while the latter entry E is of type `list`, which is a list of integer vectors each containing exactly two elements. For example, the complete graph K_3 on three vertices is defined by:

[1] We used version 3–0–3 which is available free of charge at SINGULAR's homepage `http://www.singular.uni-kl.de/`.

```
intvec V = 1,2,3;
list E = intvec(1,2), intvec(1,3), intvec(2,3);
list K_3 = V, E;
```

A k-coloring of G is represented by a `list` with two entries: k, and a partition $P = \{U_1, \ldots, U_\ell\}$ of the set V of vertices, where $\ell \leq k$. The first entry k is simply an integer, while the latter entry P is a list of integer vectors. For example, the unique proper 2-coloring γ of the path graph on four vertices is defined by:

```
int k = 2;
list P = intvec(1,3), intvec(2,4);
list gamma = k, P;
```

The following code is the library `graph.lib`.

```
proc e(int i, int j)
{
  return(intvec(i, j));
}

proc graph(string G)
{
  if (G == "CC93")
  {
    intvec V = 1..12;
    list E = e(1,2), e(1,4), e(1,6), e(1,12), e(2,3), e(2,5),
             e(2,7), e(3,8), e(3,10), e(4,9), e(4,11), e(5,6),
             e(5,9), e(5,12), e(6,7), e(6,10), e(7,8), e(7,11),
             e(8,9), e(8,12), e(9,10), e(10,11), e(11,12);
    return(list(V, E));
  }
  if (G == "AMS01")
  {
    intvec V = 1..24;
    list E = e(1,2), e(1,4), e(1,6), e(1,12), e(2,3), e(2,7),
             e(2,14), e(3,10), e(3,18), e(4,9), e(4,11), e(5,6),
              e(5,9), e(5,12), e(6,7), e(6,10), e(7,8), e(7,11),
              e(7,15), e(8,9), e(8,12), e(10,11), e(10,14),
              e(10,22), e(11,12), e(13,14), e(13,16), e(13,18),
              e(13,24), e(14,15), e(14,19), e(15,22), e(16,21),
              e(16,23), e(17,18), e(17,21), e(17,24), e(18,19),
              e(18,22), e(19,20), e(19,23), e(20,21), e(20,24),
              e(22,23), e(23,24);
    return(list(V, E));
  }
}

proc f(list G)
{
  int i, j;
  poly p = 1;
  for (int l = 1; l <= size(E(G)); l++)
  {
    i, j = E(G)[l];
    p = p * (x(i) - x(j));
  }
  return(p);
}

proc V(list G)
{
  return(G[1]);
}

proc E(list G)
{
  return(G[2]);
}

proc pathgraph(int n)
{
  list E;
  for (int i = 1; i < n; i++) { E = E + list(e(i, i + 1)); }
  return(list(1..n, E));
}
```

```
proc completegraph(int n)
{
  list E;
  for (int i = 1; i < n; i++)
  {
    for (int j = i + 1; j <= n; j++) { E = E + list(e(i, j)); }
  }
  return(list(1..n, E));
}
```

2.7.2 ideals.lib

Recall that for a subset $U \subseteq V$ of vertices and a positive integer d, h_U^d is the sum of all monomials of degree d in the indeterminates $\{x_\ell : \ell \in U\}$. We may also express h_U^d as

$$h_U^d = \sum_{l=0}^{d} x_i^l h_{U\setminus\{i\}}^{d-l}$$

for any $i \in U$. This is the expression used to construct h_U^d recursively in the procedure `h` below. The following code is the library `ideals.lib`.

```
proc h(intvec U, int d)
{
  if (size(U) == 1) { return(x(U[1])^d); }
  poly p;
  for (int l = 0; l <= d; l++)
  {
    p = p + x(U[1])^l * h(intvec(U[2..size(U)]), d - l);
  }
  return(p);
}

proc v(list gamma, intvec U, int  i)
{
  int j1, j2, j3, j4;
  for (j1 = 1; j1 <= size(gamma[2]); j1++)
  {
    for (j2 = 1; j2 <= size(gamma[2][j1]); j2++)
    {
      if (i == gamma[2][j1][j2])
      {
        for (j3 = 1; j3 <= size(gamma[2][j1]); j3++)
        {
          for (j4 = 1; j4 <= size(U); j4++)
          {
            if (U[j4] == gamma[2][j1][j3]) { return(U[j4]); }
          }
        }
      }
    }
  }
}

proc g(list gamma, int i)
{
  int j;
  int k = gamma[1];
  int l = size(gamma[2]);
  intvec U;
  U[1] = gamma[2][1][1];
  for (j = 2; j <= l; j++) { U = U, gamma[2][j][1]; }
  if (i == U[1]) { return(x(U[1])^k - 1); }
  for (j = 2; j <= l; j++)
  {
    if (i == U[j]) { return(h(intvec(U[1..j]), k + 1 - j)); }
  }
  return(x(i) - x(v(gamma, U, i)));
}

proc I(expr1, expr2)
{
  int i, j;
  ideal A;
  if (typeof(expr1) == "int")
  {
    int n = expr1;
    int k = expr2;
    for (i = 1; i <= n; i++) { A[i] = x(i)^k - 1; }
    return(A);
  }
  list G = expr1;
  int n = size(V(G));
  if (typeof(expr2) == "int")
  {
    int k = expr2;
    for (int l = 1; l <= size(E(G)); l++)
    {
      i, j = E(G)[l];
      A[l] = (x(i)^k - x(j)^k) / (x(i) - x(j));
    }
    return(I(n, k) + A);
  }
  list gamma = expr2;
  for (i = 1; i <= n; i++) { A[i] = g(gamma, i); }
  return(A);
}
```

II

The Quillen–Suslin Theorem

Part 3

Revisiting an Algorithm for the Quillen–Suslin Theorem

We give a new constructive algorithm for the Quillen–Suslin Theorem in the important case of an infinite ground field. The new algorithm follows the lines of an algorithm by Logar and Sturmfels, but differs in the way it constructs sequences of polynomials and matrices that are central to the algorithm. The output of the two algorithms are not easily comparable, however, both theoretical and experimental evidence that the new algorithm produces a much simpler output, is presented. Some tricks that may potentially simplify the computations further as well as some drawbacks of the algorithms are also discussed.

3.1 Introduction

Let $\Bbbk$ be a field, and let $\Bbbk[x_1, \ldots, x_n]$ be the polynomial ring over $\Bbbk$ in indeterminates $x_1, \ldots, x_n$. The following theorem, known as Serre's Conjecture, is central in commutative algebra.

Theorem 3.1.1 (Serre's Conjecture)**.** *Every finitely generated projective module over $\Bbbk[x_1, \ldots, x_n]$ is free.*

It was proved independently by Quillen and Suslin in 1976. We refer to the book [Lam06] by Lam for more information on Serre's Conjecture and its history.

A matrix over a commutative ring is said to be *unimodular* if its maximal minors generate the unit ideal. Serre's Conjecture is equivalent to the following theorem.

Theorem 3.1.2 (Quillen–Suslin)**.** *For every unimodular $\ell \times m$ matrix F (with $\ell \leq m$) over $\Bbbk[x_1, \ldots, x_n]$, there exists a unimodular $m \times m$ matrix U over $\Bbbk[x_1, \ldots, x_n]$ such that*

$$FU = \begin{pmatrix} 1 & & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & & 1 & 0 & \cdots & 0 \end{pmatrix}.$$

For a commutative ring A, and a multiplicative closed subset $S \subseteq A$, let $S^{-1}A$ denote the ring $S^{-1}A = \{a/s : a \in A \text{ and } s \in S\}$. In case $S = \left\{s, s^2, \ldots\right\}$ for some $s \in A \setminus \{0\}$, we simply write $s^{-1}A$ instead of $S^{-1}A$.

In 1992, Logar and Sturmfels [LS92] gave a constructive algorithm for the Quillen–Suslin Theorem in case $\Bbbk = \mathbb{C}$. An analysis of the algorithm shows that what is central for the construction of such a unimodular $m \times m$ matrix U, is the ability to construct polynomials $r_1, \ldots, r_k \in \Bbbk[x_1, \ldots, x_{n-1}]$, and matrices U_i over $r_i^{-1}\Bbbk[x_1, \ldots, x_n]$ for each $i = 1, \ldots, k$ such that

1. the polynomials $r_1, \ldots, r_k$ generate $\Bbbk[x_1, \ldots, x_{n-1}]$,
2. the row fU_i is over $r_i^{-1}\Bbbk[x_1, \ldots, x_{n-1}]$, and
3. the matrix U_i is unimodular,

for any positive integer n, and any unimodular row $f = \begin{pmatrix} f_1 & \cdots & f_m \end{pmatrix}$ over $\Bbbk[x_1, \ldots, x_n]$.

The organization of this paper is as follows. In Section 3.2, we give a new constructive algorithm for the Quillen–Suslin Theorem in the important case of an infinite ground field $\Bbbk$. We do so by constructing sequences of polynomials $r_1, \ldots, r_k$ and matrices $U_1, \ldots, U_k$ with the above three properties. The output of the two algorithms are not easily comparable. The new algorithm, however, almost certainly produces a much simpler output. Theoretical and experimental evidence to support this claim, is presented in Section 3.3. Finally, in Section 3.4, we discuss some tricks that may potentially simplify the computations further as well as some drawbacks of the algorithms.

3.2 Algorithm for the Unimodular Row Problem

The problem of constructing a unimodular $m \times m$ matrix U as in Theorem 3.1.2 may be reduced to the following using induction (see [LS92] for details).

Problem 3.2.1 (Unimodular Row Problem)**.** *Given a unimodular row $f = \begin{pmatrix} f_1 & \cdots & f_m \end{pmatrix}$ over $\Bbbk[x_1, \ldots, x_n]$, find a unimodular $m \times m$ matrix U over $\Bbbk[x_1, \ldots, x_n]$ such that $fU = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$.*

Let A be a commutative ring, and suppose $f = \begin{pmatrix} f_1 & \cdots & f_m \end{pmatrix}$ is a unimodular row over $A[x]$ in which f_1 is monic. We begin by computing polynomials $g_1, \ldots, g_m \in A[x]$ such that

$$f_1 g_1 + \cdots + f_m g_m = 1.$$

In case $m = 2$, the matrix U over $A[x]$ defined by

$$U = \begin{pmatrix} g_1 & -f_2 \\ g_2 & f_1 \end{pmatrix}$$

satisfies $fU = \begin{pmatrix} 1 & 0 \end{pmatrix}$. Hence, from now on, we may assume that $m \geq 3$. We will need the following result by Lombardi and Yengui.

Theorem 3.2.2 (**[LY05, Corollary 3]**). *Let $k = \deg(f_1) + 1$ and suppose A contains a set $\{a_1, \ldots, a_k\}$ such that the difference between any two elements is invertible. Then $\langle r_1, \ldots, r_k \rangle = A$, where*

$$r_i = \operatorname{Res}\left(f_1, f_2 + a_i \sum_{j=3}^{m} f_j g_j \right) \in A.$$

For our application, A will be a polynomial ring over an infinite field. Hence, we may choose such a set $\{a_1, \ldots, a_k\}$, and compute the resultants $r_1, \ldots, r_k \in A$ defined in the theorem. If the resultant r_i is zero for some i, it may simply be discarded. Thus, we may assume, without loss of generality, that r_i is nonzero for $i = 1, \ldots, k$. Furthermore, find $s_1, \ldots, s_k \in A$ such that

$$r_1 s_1 + \cdots + r_k s_k = 1.$$

For each $i = 1, \ldots, k$ we now compute polynomials $p_i, q_i \in A[x]$ such that

$$p_i f_1 + q_i \left(f_2 + a_i \sum_{j=3}^{m} f_j g_j \right) = r_i,$$

and construct the following matrix M_i over $A[x]$:

$$M_i = \begin{pmatrix} f_1 & f_2 & f_3 & \cdots & f_m \\ -q_i & p_i & 0 & \cdots & 0 \\ 0 & -a_i g_3 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -a_i g_m & 0 & \cdots & 1 \end{pmatrix}.$$

An obvious property of M_i which will be important later on, is that

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} M_i = f. \tag{3.2.1}$$

We claim that M_i has determinant r_i. To see this, simply expand the determinant along the first row:

$$\det(M_i) = p_i f_1 - (-q_i) f_2 + \sum_{j=3}^{m} (-1)^{1+j} (-q_i) f_j ((-1)^{j-1} a_i g_j) = r_i.$$

Since r_i is nonzero, M_i is invertible when considered as a matrix over $r_i^{-1} A[x]$. Hence, we let $U_i = M_i^{-1}$ over $r_i^{-1} A[x]$.

Remark 3.2.3. Notice that in case r_i is invertible, the matrix U_i is in fact over $A[x]$, and satisfies $fU_i = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$.

It is straight forward to verify that $U_i = I_m - r_i^{-1} N_i$, where I_m is the $m \times m$ identity matrix, and N_i is the following matrix over $A[x]$:

$$N_i = \begin{pmatrix} r_i - p_i & f_2 + a_i \sum_{j=3}^{m} f_j g_j & p_i f_3 & \cdots & p_i f_m \\ -\, q_i & r_i - f_1 & q_i f_3 & \cdots & q_i f_m \\ -a_i q_i g_3 & -a_i f_1 g_3 & a_i q_i f_3 g_3 & \cdots & a_i q_i f_m g_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_i q_i g_m & -a_i f_1 g_m & a_i q_i f_3 g_m & \cdots & a_i q_i f_m g_m \end{pmatrix}.$$

This explicit expression of U_i may be useful when implementing the algorithm for the Unimodular Row Problem described below, but we shall not need it. We may now construct the matrix Δ_i over $r_i^{-1}A[y,z]$:

$$\Delta_i = U_i\,(y) \cdot U_i^{-1}(y+z).$$

It is clear that Δ_i has determinant 1, and that $\Delta_i(y,0) = I_m$. It follows from (3.2.1) that Δ_i has the property

$$f(y)\Delta_i = f(y+z). \tag{3.2.2}$$

Recall that the matrix M_i is defined over $A[x]$ and has determinant r_i. Since U_i equals the adjoint of M_i divided by the determinant of M_i, we see that r_i is a common denominator for all the entries of U_i. This means that r_i is also a common denominator for all the entries of Δ_i. Expanding the matrix

$$\Delta_i = I_m + \Delta_{i1} z + \Delta_{i2} z^2 + \cdots + \Delta_{id_i} z^{d_i}$$

as a polynomial in z with matrix coefficients over $r_i^{-1}A[y]$ shows that replacing z by $r_i z$ yields a matrix $\Delta_i(y, r_i z)$ over $A[y,z]$. We may now finally construct the matrix V over $A[x]$ as follows:

$$V = \Delta_1(x, -r_1 s_1 x) \prod_{i=2}^{k} \Delta_i \left(\left(1 - \sum_{t=1}^{i-1} r_t s_t \right) x, -r_i s_i x \right).$$

It is clear that V has determinant 1. Furthermore, it follows from (3.2.2) that V has the property that, when multiplied by the unimodular row f, it will evaluate

f at $x = 0$:

$$\begin{aligned} fV &= f(x - r_1 s_1 x) \prod_{i=2}^{k} \Delta_i \left(\left(1 - \sum_{t=1}^{i-1} r_t s_t \right) x, -r_i s_i x \right) \\ &= f \left(\left(1 - \sum_{t=1}^{k} r_t s_t \right) x \right) \\ &= f(0). \end{aligned}$$

The construction of V form the basis of the following algorithm for the Unimodular Row Problem. In what follows, $\Bbbk$ is an infinite field.

Algorithm 3.2.4. *With the above notation, we have the following algorithm for the Unimodular Row Problem:*

Input: *A unimodular row* $f = \begin{pmatrix} f_1 & \cdots & f_m \end{pmatrix}$ *over* $\Bbbk[x_1, \ldots, x_n]$ *with* $m \geq 3$.
Output: *A unimodular* $m \times m$ *matrix* U *over* $\Bbbk[x_1, \ldots, x_n]$ *such that*

$$fU = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}.$$

1. *Let* $U := I_m$ *be the* $m \times m$ *identity matrix.*

2. *Let* $A := \Bbbk[x_1, \ldots, x_{n-1}]$ *and* $x := x_n$, *and consider* f *as a row over* $A[x]$.

3. *Using Noether normalization, make a linear change of variables such that* f_1 *becomes monic, and update* U *accordingly.*

4. *Let* $k := \deg(f_1) + 1$, *and choose a set* $\{a_1, \ldots, a_k\} \subseteq A$ *such that the difference between any two elements is invertible.*

5. *Compute polynomials* $g_1, \ldots, g_m \in A[x]$ *such that* $f_1 g_1 + \cdots + f_m g_m = 1$.

6. *For each* $i = 1, \ldots, k$ *do:*

   (a) *Compute the resultant* $r_i = \operatorname{Res}\left(f_1, f_2 + a_i \sum_{j=3}^{m} f_j g_j\right) \in A$.

   (b) *Compute* $p_i, q_i \in A[x]$ *such that* $p_i f_1 + q_i \left(f_2 + a_i \sum_{j=3}^{m} f_j g_j\right) = r_i$.

   (c) *If* r_i *is invertible, let* $U := UU_i$ *and exit the algorithm.*

7. *Compute polynomials* $s_1, \ldots, s_k \in A$ *such that* $r_1 s_1 + \cdots + r_k s_k = 1$.

8. *Let $U := UV$, and let $f := fV$.*

9. *Let $n := n - 1$, and go to step 2.*

Proof. The algorithm will terminate once an invertible r_i has been found. This will happen sooner or later, since if $n = 1$ is reached, then $r_1, \ldots, r_k \in \Bbbk$ will generate $\Bbbk$ by Theorem 3.2.2. Hence, there is some nonzero r_i. It follows from the above construction of V and Remark 3.2.3 that the algorithm produces a unimodular $m \times m$ matrix such that $fU = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$. We note that the new row f in step 8 is again unimodular since $fV = f(0)$, and

$$f_1(0)g_1(0) + \cdots + f_m(0)g_m(0) = 1(0) = 1.$$

This completes the proof. □

3.3 Complexity

We have seen that r_i is a common denominator for all the entries of Δ_i, which implies that by replacing z by $r_i z$, we get a matrix $\Delta_i(y, r_i z)$ over $A[y, z]$. In the algorithm by Logar and Sturmfels we, however, need to replace z by $r_i^m z$ in order to get rid of the denominators. This has a huge impact on the resulting unimodular $m \times m$ matrix U. Not only because z in Δ_i, when constructing V, gets replaced by $r_i^m s_i' x$ instead of $r_i s_i x$, but also because the polynomials $s_1', \ldots, s_k'$ needed in order for

$$r_1^m s_1' + \cdots + r_k^m s_k' = 1$$

also get much more complicated with bigger coefficients and higher degrees as a result. We shall now see an example of this.

Example 3.3.1. Let $f = \begin{pmatrix} x_2^2 & x_1^2 + x_2 & x_1x_2 + x_1 + x_2 + 1 \end{pmatrix}$ be a row over $\Bbbk[x_1, x_2]$. We verify that f is indeed unimodular and compute the polynomials $g_1, g_2, g_3 \in \Bbbk[x_1, x_2]$ using a Gröbner basis computation in Maple:

```
[> with(LinearAlgebra):
[> with(Groebner):
[> f := [x[2]^2, x[1]^2+x[2], x[1]*x[2]+x[1]+x[2]+1];
[> g := Basis(f, plex(x[1],x[2]), output=extended)[2][];
```

We get the row $g = \begin{pmatrix} 2 + x_2x_1^2 - x_2 - x_1^2 & -x_2 + 1 & -(x_2 - 1)^2(-1 + x_1) \end{pmatrix}$, and may verify that f (and g) is unimodular since $f_1g_1 + f_2g_2 + f_3g_3 = 1$. We let $k = 3$, and choose $a_1 = 0$, $a_2 = 1$, and $a_3 = 2$. Next we compute the resultant r_1, and the polynomials p_1, and q_1:

```
[> a := [0, 1, 2];
[> r[1] := resultant(f[1], f[2]+a[1]*f[3]*g[3], x[2]);
[> pq := Basis([f[1], f[2]+a[1]*f[3]*g[3]],
               plex(x[2]), output=extended)[2][];
[> p[1] := pq[1]*r[1];
[> q[1] := pq[2]*r[1];
```

This yields $r_1 = x_1^4$, $p_1 = 1$, and $q_1 = -x_2 + x_1^2$. Since r_1 is not invertible, we compute the resultant r_2, and the polynomials p_2, and q_2:

```
[> r[2] := resultant(f[1], f[2]+a[2]*f[3]*g[3], x[2]);
[> pq := Basis([f[1], f[2]+a[2]*f[3]*g[3]],
               plex(x[2]), output=extended)[2][];
[> p[2] := pq[1]*r[2];
[> q[2] := pq[2]*r[2];
```

This then yields $r_2 = 1$, $p_2 = x_1^4 - x_1^4x_2^2 + x_2^2x_1^2 + x_1^4x_2 - x_2 - x_1^2 + 1$, and $q_2 = -x_2x_1^2 + 1$. Since r_2 is invertible, it follows from Remark 3.2.3 that U_2 satisfies $fU_2 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$. We therefore compute U_2:

```
[> M[2] := Matrix(3, 3, [[f[1], f[2], f[3]],
                         [-q[2], p[2], 0], [0, -a[2]*g[3], 1]]);
[> U[2] := M[2]^(-1);
```

The result is the 3×3 matrix $U_2 = (u_{ij})$ in which

$$\begin{aligned}
u_{11} &= x_1^4 - x_1^4x_2^2 + x_2^2x_1^2 + x_1^4x_2 - x_2 - x_1^2 + 1,\\
u_{21} &= -x_2x_1^2 + 1,\\
u_{31} &= (-1 + x_2x_1^2)(x_2^2x_1 - 2x_1x_2 + 2x_2 - x_2^2 - 1 + x_1),\\
u_{12} &= x_1^2x_2^3 - x_2^2x_1^2 - x_2x_1^2 + x_2^2 - x_2^3 - 1,\\
u_{22} &= x_2^2,\\
u_{32} &= -x_2^2(x_2^2x_1 - 2x_1x_2 + 2x_2 - x_2^2 - 1 + x_1),\\
u_{13} &= (x_1x_2 + x_1 + x_2 + 1)(-x_1^4 + x_1^4x_2^2 - x_2^2x_1^2 - x_1^4x_2 + x_2 + x_1^2 - 1),\\
u_{23} &= (x_1x_2 + x_1 + x_2 + 1)(-1 + x_2x_1^2),\\
u_{33} &= x_1^4x_2^2 - x_2^4x_1^4 + x_2^4x_1^2 + x_2^3x_1^4 - x_2^3 - 2x_2^2x_1^2 + x_2^2 + x_1^2 + x_2 - x_1^4x_2.
\end{aligned}$$

One may also verify that this matrix has determinant 1, and so is indeed unimodular. Notice that the entries of U_2 have degree ranging from 2 to 8.

If we assume that $\Bbbk$ has characteristic zero, the algorithm by Logar and Sturmfels, given the same input as before, produces another unimodular 3×3 matrix with entries

$$\begin{aligned}
u_{11} &= c_1x_1^{91}x_2^4 + (635\text{ terms}),\\
u_{21} &= -c_1x_1^{89}x_2^6 + (714\text{ terms}),\\
u_{31} &= c_1x_1^{89}x_2^6 + (719\text{ terms}),\\
u_{12} &= c_1x_1^{92}x_2^4 + (645\text{ terms}),\\
u_{22} &= -c_1x_1^{90}x_2^6 + (727\text{ terms}),\\
u_{32} &= c_1x_1^{90}x_2^6 + (729\text{ terms}),\\
u_{13} &= -c_2x_1^{67}x_2^3 + (394\text{ terms}),\\
u_{23} &= c_2x_1^{65}x_2^5 + (303\text{ terms}),\\
u_{33} &= -c_2x_1^{65}x_2^5 + (303\text{ terms}),
\end{aligned}$$

in which

$$\begin{aligned}
c_1 &= 7534679545549067711721222011 4576\\
&\qquad\qquad + 33696111280109816482971698230272\sqrt{5},\\
c_2 &= 1780395043182825433742028\\
&\qquad\qquad + 796216849068911274481428\sqrt{5}.
\end{aligned}$$

The degree of the entries of the above matrix range from 70 to 96. Thus, the algorithm by Logar and Sturmfels leads to a tremendous growth in both the coefficients as well as the degrees. Another unfortunate aspect is the introduction of $\sqrt{5}$ in the solution keeping in mind that we may view f as a row over $\mathbb{Q}[x_1, x_2]$. This is due to the fact the algorithm by Logar and Sturmfels only works for an algebraically closed field $\Bbbk$.

3.4 Tricks and Drawbacks

We conclude with some tricks that may potentially simplify the computations needed to find a unimodular $m \times m$ matrix U as in Theorem 3.1.2, when given a concrete unimodular row $f = \begin{pmatrix} f_1 & \cdots & f_m \end{pmatrix}$ over $\Bbbk[x_1, \ldots, x_n]$. Some drawbacks of the algorithms are also discussed.

(1) If we compute polynomials $g_1, \ldots, g_m$ such that $f_1 g_1 + \cdots + f_m g_m = 1$, and one of the g_j is a nonzero element of $\Bbbk$, then U may easily be constructed as a product of elementary column operations matrices.

(2) Given f, we may try to divide each f_j by $\{f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_m\}$ using the division algorithm. Suppose, for instance,

$$f_1 = h_2 f_2 + \cdots + h_m f_m + r$$

for polynomials $h_2, \ldots, h_m$ not all zero, and a remainder r. The row f may then easily be replaced by $\begin{pmatrix} r & f_2 & \cdots & f_m \end{pmatrix}$ using elementary column operations. We may then try to divide f_2, and so on. In the end we are left with a unimodular row $f' = \begin{pmatrix} f'_1 & \cdots & f'_m \end{pmatrix}$ which may hopefully lead to a simpler output of Algorithm 3.2.4.

(3) For an elementary column operation matrix E, let U_f and U_{fE} be the output produced by Algorithm 3.2.4 for the unimodular rows f and fE, respectively. It would be desirable to have $U_{fE} = U_f E$, however, this is not the case. As an example we may interchange the first two columns of f in Example 3.3.1. Algorithm 3.2.4 now produces a unimodular 3×3 matrix the entries of which have degree ranging from 25 to 28. This is also a drawback of the algorithm by Logar and Sturmfels.

(4) The output of Algorithm 3.2.4 strongly depends on the choice of subset $\{a_1, \ldots, a_k\}$ made in each iteration. It is natural to prefer small values for the a_i in order to prevent coefficient growth. However, for a given unimodular row, there might be some other choice for the a_i that yields particularly simple resultants. If so, Algorithm 3.2.4 may terminate sooner, hopefully producing a simpler output.

III

Symmetric Ideals

Part 4

Minimal Generators for Symmetric Ideals

Let $R = \Bbbk[X]$ be the polynomial ring in infinitely many indeterminates X over a field $\Bbbk$, and let $\mathfrak{S}_X$ be the symmetric group of X. The group $\mathfrak{S}_X$ acts naturally on R, and this in turn gives R the structure of a module over the group ring $R[\mathfrak{S}_X]$. A recent theorem of Aschenbrenner and Hillar states that the module R is Noetherian. We address whether submodules of R can have any number of minimal generators, answering this question positively.

4.1 Introduction

Let $R = \Bbbk[X]$ be the polynomial ring in infinitely many indeterminates X over a field $\Bbbk$, and let $\mathfrak{S}_X$ be the symmetric group of X. The group $\mathfrak{S}_X$ acts naturally on R: if $\sigma \in \mathfrak{S}_X$ and $f \in \Bbbk[x_1, \ldots, x_\ell]$ where $x_i \in X$, then

$$\sigma f(x_1, x_2, \ldots, x_\ell) = f(\sigma x_1, \sigma x_2, \ldots, \sigma x_\ell) \in R. \tag{4.1.1}$$

We say that an ideal $I \subseteq R$ is *symmetric* if I is invariant under $\mathfrak{S}_X$, that is, if

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

The action (4.1.1) naturally gives R the structure of a (left) module over the (left) group ring $R[\mathfrak{S}_X]$ defined by

$$R[\mathfrak{S}_X] = \left\{ \sum_{\sigma \in \mathfrak{S}_X}^{\text{finite}} r_\sigma \sigma : r_\sigma \in R \right\}.$$

Symmetric ideals are then simply the submodules of R. Aschenbrenner and Hillar recently proved the following.

Theorem 4.1.1. *Every symmetric ideal of R is finitely generated as an $R[\mathfrak{S}_X]$-module. In other words, R is a Noetherian $R[\mathfrak{S}_X]$-module.*

Theorem 4.1.1 was motivated by finiteness questions in chemistry and algebraic statistics (see the references in [AH07]).

The basic question whether a symmetric ideal is always cyclic (already asked by J. Schicho[1]) was left unanswered in [AH07]. Our result addresses a generalization of this important issue.

Theorem 4.1.2. *For every positive integer n, there are symmetric ideals of R generated by n polynomials which cannot have fewer than n $R[\mathfrak{S}_X]$-generators.*

At first glance, Theorem 4.1.2 is a bit surprising. If one picks even a single polynomial $g \in R$, the cyclic submodule $\langle g \rangle$ is very large, and it is not clear that every submodule of R doesn't arise in this way. Given a finite list of

[1] Private communication, 2006.

polynomials $f_1, \ldots, f_n$, one could conceivably choose a sufficiently large enough positive integer N so that the number of unknowns in a system

$$\begin{aligned} f_1 &= \sum_{\sigma \in \mathfrak{S}_N} r_{1\sigma} \sigma g, \qquad r_{1\sigma} \in R \\ &\vdots \\ f_n &= \sum_{\sigma \in \mathfrak{S}_N} r_{n\sigma} \sigma g, \qquad r_{n\sigma} \in R \end{aligned}$$

greatly outnumbers the number of equations, thereby (presumably) ensuring a solution for the $r_{i\sigma}$. Here $\mathfrak{S}_N$ denotes the set of permutations of $\{1, \ldots, N\}$.

In what follows, we work with the set $X = \{x_1, x_2, x_3, \ldots\}$, although as remarked in [AH07], this is not really a restriction. In this case, $\mathfrak{S}_X$ is naturally identified with $\mathfrak{S}_\infty$, the permutations of the set of positive integers, and $\sigma x_i = x_{\sigma i}$ for $\sigma \in \mathfrak{S}_\infty$.

4.2 Multisets and monomials

In this section, we provide the basic notation used in the proof of Theorem 4.1.2 as well as the proof itself.

Formally, a *multiset* $M = (A, m)$ is a set A along with a *multiplicity function* $m : A \to \mathbb{Z}$ which assigns to each element $a \in A$ a nonnegative *multiplicity* $m(a)$.

In what follows, the set A will always be the set of positive integers and m will be a function with finite support; that is, m will be nonzero for only finitely many elements of A. For notational simplicity, we will frequently view M as a finite set of positive integers with repetitions allowed as in $M = \{1, 1, 1, 2, 3, 3\}$.

Multisets are in natural bijection with monomials of R. Given a multiset $M = (A, m)$, we can construct the monomial:

$$\mathbf{x}_M = \prod_{a \in A} x_a^{m(a)}.$$

Conversely, given a monomial, the associated multiset is the set of indices appearing in it, along with multiplicities.

Let $M = (A, m)$ be a multiset and let $a_1, \ldots, a_k$ be the list elements of A with positive multiplicity, arranged so that $m(a_1) \geq \cdots \geq m(a_k)$. The *type* of a multiset M (or the corresponding monomial) is the vector

$$\lambda(M) = (m(a_1), \ldots, m(a_k)).$$

For instance, the multiset $M = \{1, 1, 1, 2, 3, 3\}$ has type $\lambda(M) = (3, 2, 1)$. The action of $\mathfrak{S}_\infty$ on monomials coincides with the natural action of $\mathfrak{S}_\infty$ on multisets $M = (A, m)$: $\sigma M = (A, \sigma m)$, in which $\sigma m : A \to \mathbb{Z}$ is the function $i \mapsto m(\sigma^{-1} i)$. It easy to see that the action of $\mathfrak{S}_\infty$ preserves the type of a monomial.

We also note that an infinite permutation acting on a polynomial may be replaced with a finite one.

Lemma 4.2.1. *Let $\sigma \in \mathfrak{S}_\infty$ and $f \in R$. Then there exists a positive integer N and $\tau \in \mathfrak{S}_N$ such that $\tau f = \sigma f$.*

Proof. Let S be the set of indices appearing in the monomials of f and let N be the largest integer in $\sigma S \cup S$. The injective function $\sigma|_S : S \to \{1, \ldots, N\}$ extends (nonuniquely) to a permutation $\tau \in \mathfrak{S}_N$ such that $\tau f = \sigma f$. □

We will derive Theorem 4.1.2 is a direct corollary of the following result.

Theorem 4.2.2. *Let $G = \{g_1, \ldots, g_n\}$ be a set of monomials of degree d with distinct types and fix an $n \times n$ matrix $C = (c_{ij})$ over $\Bbbk$ of rank r. Then the submodule $I = \langle f_1, \ldots, f_n \rangle$ of R generated by the n polynomials*

$$f_j = \sum_{i=1}^{n} c_{ij} g_i, \qquad j = 1, \ldots, n$$

cannot have fewer than r $R[\mathfrak{S}_\infty]$-generators.

Proof. Suppose that $p_1, \ldots, p_k$ are generators for $I = \langle f_1, \ldots, f_n \rangle$ with the f_j as in the statement of the theorem; we prove that $k \geq r$. Note that each nonzero f_j is homogeneous of degree d. Since each $p_l \in I$, it follows that each is a linear combination, over $R[\mathfrak{S}_\infty]$, of monomials in G. Therefore, each monomial occurring in p_l has degree at least d, and, moreover, any degree d monomial in p_l has the same type as one of the monomials in G.

Write each of the monomials in G in the form $g_i = \mathbf{x}_{M_i}$ for multisets $M_1, \ldots, M_n$ with corresponding distinct types $\lambda_1, \ldots, \lambda_n$. Then we can express each generator p_l in the following form:

$$p_l = \sum_{i=1}^{n} \sum_{\lambda(M)=\lambda_i} u_{ilM}\mathbf{x}_M + q_l, \tag{4.2.1}$$

in which $u_{ilM} \in \Bbbk$ with only finitely many of them nonzero, each monomial appearing in q_l has degree greater than d, and the inner sum is over all multisets M with type λ_i.

Since each polynomial in $\{f_1, \ldots, f_n\}$ is a finite linear combination of the p_l, and since only finitely many positive integers are indices of monomials appearing in $p_1, \ldots, p_k$, it follows that we may pick a positive integer N large enough so that all of these linear combinations can be expressed with coefficients in the subring $R[\mathfrak{S}_N]$ (c.f. Lemma 4.2.1). Therefore, we have

$$f_j = \sum_{l=1}^{k} \sum_{\sigma\in\mathfrak{S}_N} s_{lj\sigma}\sigma p_l, \tag{4.2.2}$$

for some polynomials $s_{lj\sigma} \in R$. Substituting the expressions found in (4.2.1) into (4.2.2) produces

$$\begin{aligned} f_j &= \sum_{l=1}^{k} \sum_{\sigma\in\mathfrak{S}_N} s_{lj\sigma} \left(\sum_{i=1}^{n} \sum_{\lambda(M)=\lambda_i} u_{ilM}\mathbf{x}_{\sigma M} \; + \; \sigma q_l \right) \\ &= \sum_{l=1}^{k} \sum_{\sigma\in\mathfrak{S}_N} \sum_{i=1}^{n} \sum_{\lambda(M)=\lambda_i} v_{lj\sigma} u_{ilM}\mathbf{x}_{\sigma M} \; + h_j, \end{aligned}$$

in which each monomial appearing in $h_j \in R$ has degree greater than d and $v_{lj\sigma}$ is the constant term of $s_{lj\sigma}$. Since each f_j has degree d, we must have that $h_j = 0$. It follows that

$$\sum_{i=1}^{n} c_{ij}\mathbf{x}_{M_i} = \sum_{l=1}^{k} \sum_{\sigma\in\mathfrak{S}_N} \sum_{i=1}^{n} \sum_{\lambda(M)=\lambda_i} v_{lj\sigma} u_{ilM}\mathbf{x}_{\sigma M}.$$

Next, for a fixed i, take the sum on each side in this last equation of the coefficients of monomials with the type λ_i. This produces the n^2 equations:

$$\begin{aligned} c_{ij} &= \sum_{l=1}^{k} \sum_{\sigma \in \mathfrak{S}_N} \sum_{\lambda(M)=\lambda_i} v_{lj\sigma} u_{ilM} \\ &= \sum_{l=1}^{k} \left(\sum_{\lambda(M)=\lambda_i} u_{ilM} \right) \left(\sum_{\sigma \in \mathfrak{S}_N} v_{lj\sigma} \right) \\ &= \sum_{l=1}^{k} U_{il} V_{lj}, \end{aligned} \tag{4.2.3}$$

in which

$$U_{il} = \sum_{\lambda(M)=\lambda_i} u_{ilM} \qquad \text{and} \qquad V_{lj} = \sum_{\sigma \in \mathfrak{S}_N} v_{lj\sigma}.$$

Let U be the $n \times k$ matrix (U_{il}) and similarly let V be the $k \times n$ matrix (V_{lj}). The n^2 equations (4.2.3) can be viewed compactly as matrix multiplication:

$$\begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{bmatrix} = \begin{bmatrix} U_{11} & \cdots & U_{1k} \\ \vdots & \ddots & \vdots \\ U_{n1} & \cdots & U_{nk} \end{bmatrix} \begin{bmatrix} V_{11} & \cdots & V_{1n} \\ \vdots & \ddots & \vdots \\ V_{k1} & \cdots & V_{kn} \end{bmatrix}.$$

Considering the rank of both sides of the equation $C = UV$ leads to the following chain of inequalities:

$$r = \operatorname{rank}(C) = \operatorname{rank}(UV) \leq \min\{\operatorname{rank}(U), \operatorname{rank}(V)\} \leq \min\{n, k\} \leq k.$$

Therefore, we have $k \geq r$, and this completes the proof. □

Example 4.2.3. According to Theorem 4.2.2, the submodule $I = \langle x_1 x_2, x_1^2 \rangle$ of R cannot have fewer than two $R[\mathfrak{S}_\infty]$-generators. Thus, I is an example of a noncyclic symmetric ideal.

Proof of Theorem 4.1.2. Let $g_i = x_1^i x_2 \cdots x_{n+1-i}$ and apply Theorem 4.2.2 with C being the $n \times n$ identity matrix. □

Bibliography

[AH07] Matthias Aschenbrenner and Christopher J. Hillar. Finite generation of symmetric ideals. *Trans. Amer. Math. Soc.*, 359(11):5171–5192, 2007.

[AL94] William W. Adams and Philippe Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 1994.

[AMS01] S. Akbari, V. S. Mirrokni, and B. S. Sadjad. K_r-free uniquely vertex colorable graphs with minimum possible edges. *J. Combin. Theory Ser. B*, 82(2):316–318, 2001.

[AT92] N. Alon and M. Tarsi. Colorings and orientations of graphs. *Combinatorica*, 12(2):125–134, 1992.

[Bay82] David Allen Bayer. *The Division Algorithm and the Hilbert Scheme.* PhD thesis, Harvard University, Department of Mathematics, June 1982.

[CC93] Chong-Yun Chao and Zhibo Chen. On uniquely 3-colorable graphs. *Discrete Math.*, 112(1-3):21–27, 1993.

[CLO05] David A. Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics.* Springer, New York, second edition, 2005.

[CLO07] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[Cox] David Cox. Private communication, 2007.

[dL95] Jesús A. de Loera. Gröbner bases and graph colorings. *Beiträge Algebra Geom.*, 36(1):89–96, 1995.

[DPT03] Klaus Dohmen, André Pönitz, and Peter Tittmann. A new two-variable generalization of the chromatic polynomial. *Discrete Math. Theor. Comput. Sci.*, 6(1):69–89 (electronic), 2003.

[Kos01] Thomas Koshy. *Fibonacci and Lucas numbers with applications.* Pure and Applied Mathematics (New York). Wiley-Interscience, New York, 2001.

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra. 1.* Springer-Verlag, Berlin, 2000.

[Lam06] T. Y. Lam. *Serre's problem on projective modules.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[LS92] Alessandro Logar and Bernd Sturmfels. Algorithms for the Quillen-Suslin theorem. *J. Algebra*, 145(1):231–239, 1992.

[LY05] Henri Lombardi and Ihsen Yengui. Suslin's algorithms for reduction of unimodular rows. *J. Symbolic Comput.*, 39(6):707–717, 2005.

[Xu90] Shao Ji Xu. The size of uniquely colorable graphs. *J. Combin. Theory Ser. B*, 50(2):319–320, 1990.

Summary in English

Part 1 introduces a simple idea that relates graph coloring with certain integer sequences including the Fibonacci and Lucas numbers. It demonstrates how one can produce identities involving these numbers by decomposing different classes of graphs in different ways. Part 2 deals with graph coloring from a computational algebraic point of view. It collects a series of results in the literature regarding graphs that are not k-colorable, and provides a refinement to uniquely k-colorable graphs. It also gives algorithms for testing (unique) vertex colorability. Part 3 provides a new algorithm for the Quillen–Suslin Theorem in case of an infinite ground field. The new algorithm follows the lines of an algorithm by Logar and Sturmfels, however, both theoretical and experimental evidence that the new algorithm produces a much simpler output, is presented. Part 4 settles a question regarding the minimal number of generators for symmetric ideals in polynomial rings with infinitely many indeterminates.

Summary in Danish

Del 1 introducerer en simpel ide som skaber en forbindelse mellem graffarvning og udvalgte følger af heltal herunder Fibonacci og Lucas tallene. Den demonstrerer hvorledes man kan producere identiteter, som involverer disse tal, ved at dekomponere forskellige familier af grafer på forskellige måder. Del 2 omhandler graffarvning fra et beregningsmæssigt algebraisk synspunkt. Den samler en række resultater fra litteraturen vedrørende grafer der ikke er k-farvbare, og giver en specialicering til entydigt k-farvbare grafer. Den giver ligeledes algoritmer til at teste om en graf er (entydig) knudefarvbar. Del 3 giver en ny algoritme for Quillen–Suslins sætning i tilfældet af et uendeligt grundlegeme. Den nye algoritme følger konstruktionen af en algoritme af Logar og Sturmfels, men både teoretiske og eksperimentielle argumenter der indikerer at den nye algoritme producerer et meget simplere output, bliver præsenteret. Del 4 giver svaret på et spørgsmål vedrørende det minimale antal frembringere for symmetriske idealer i polynomiumsringe med uendeligt mange variable.

Papers to appear

FIBONACCI IDENTITIES AND GRAPH COLORINGS

CHRISTOPHER J. HILLAR AND TROELS WINDFELDT

Abstract. We generalize both the Fibonacci and Lucas numbers to the context of graph colorings, and prove some identities involving these numbers. As a corollary we obtain new proofs of some known identities involving Fibonacci numbers such as

$$F_{r+s+t} = F_{r+1}F_{s+1}F_{t+1} + F_rF_sF_t - F_{r-1}F_{s-1}F_{t-1}.$$

1. Introduction

In graph theory, it is natural to study vertex colorings, and more specifically, those colorings in which adjacent vertices have different colors. In this case, the number of such colorings of a graph G is encoded by the chromatic polynomial of G. This object can be computed using the method of "deletion and contraction", which involves the recursive combination of chromatic polynomials for smaller graphs. The purpose of this note is to show how the Fibonacci and Lucas numbers (and other integer recurrences) arise naturally in this context, and in particular, how identities among these numbers can be generated from the different choices for decomposing a graph into smaller pieces.

We first introduce some notation. Let G be a undirected graph (possibly containing loops and multiple edges) with vertices $V = \{1, \ldots, n\}$ and edges E. Given nonnegative integers k and ℓ, a (k, ℓ)-*coloring* of G is a map

$$\varphi\colon V \to \{c_1, \ldots, c_{k+\ell}\},$$

in which $\{c_1, \ldots, c_{k+\ell}\}$ is a fixed set of $k+\ell$ "colors". The map φ is called *proper* if whenever i is adjacent to j and $\varphi(i), \varphi(j) \in \{c_1, \ldots, c_k\}$, we have $\varphi(i) \neq \varphi(j)$. Otherwise, we say that the map φ is *improper*. In somewhat looser terminology, one can think of $\{c_{k+1}, \ldots, c_{k+\ell}\}$ as coloring "wildcards".

Let $\chi_G(x, y)$ be a function such that $\chi_G(k, \ell)$ is the number of proper (k, ℓ)-colorings of G. This object was introduced by the authors of [2] and can be given as a polynomial in x and y (see Lemma 1.1). It simultaneously generalizes the chromatic, independence, and matching polynomials of G. For instance, $\chi_G(x, 0)$ is the usual chromatic polynomial while $\chi_G(x, 1)$ is the independence polynomial for G (see [2] for more details).

We next state a simple rule that enables one to calculate the polynomial $\chi_G(x, y)$ recursively. In what follows, $G\backslash e$ denotes the graph obtained by removing the edge e from G, and for a subgraph H of G, the graph $G\backslash H$ is gotten from G by removing H and all the edges of G that are adjacent to vertices of H. Additionally, the *contraction* of an edge e in G is the graph G/e obtained by removing e and identifying as equal the two vertices sharing this edge.

The first author is supported under a National Science Foundation Postdoctoral Fellowship.

Lemma 1.1. *Let e be an edge in G, and let v be the vertex to which e contracts in G/e. Then,*

$$\chi_G(x,y) = \chi_{G\backslash e}(x,y) - \chi_{G/e}(x,y) + y \cdot \chi_{(G/e)\backslash v}(x,y). \tag{1.1}$$

Proof. The number of proper (k,ℓ)-colorings of $G\backslash e$ which have distinct colors for the vertices sharing edge e is given by $\chi_{G\backslash e}(k,\ell) - \chi_{G/e}(k,\ell)$; these colorings are also proper for G. The remaining proper (k,ℓ)-colorings of G are precisely those for which the vertices sharing edge e have the same color. This color must be one of the wildcards $\{c_{k+1},\ldots,c_{k+\ell}\}$, and so the number of remaining proper (k,ℓ)-colorings of G is counted by $\ell \cdot \chi_{(G/e)\backslash v}(k,\ell)$. □

With such a recurrence, we need to specify initial conditions. When G simply consists of one vertex and has no edges, we have $\chi_G(x,y) = x+y$, and when G is the empty graph, we set $\chi_G(x,y) = 1$ (consider G with one edge joining two vertices in (1.1)). Moreover, χ is multiplicative on disconnected components. This allows us to compute χ_G for any graph recursively.

In the special case when $k=1$, there is also a way to calculate $\chi_G(1,y)$ by removing vertices from G. Define the *link* of a vertex v to be the subgraph link(v) of G consisting of v, the edges touching v, and the vertices sharing one of these edges with v. Also if u and v are joined by an edge e, we define link(e) to be link$(u) \cup$ link(v) in G, and also we set deg(e) to be deg(u) + deg$(v) - 2$. We then have the following rules.

Lemma 1.2. *Let v be any vertex of G, and let e be any edge. Then,*

$$\chi_G(1,y) = y \cdot \chi_{G\backslash v}(1,y) + y^{\deg(v)} \cdot \chi_{G\backslash \mathrm{link}(v)}(1,y), \tag{1.2}$$
$$\chi_G(1,y) = \quad \chi_{G\backslash e}(1,y) - y^{\deg(e)} \cdot \chi_{G\backslash \mathrm{link}(e)}(1,y). \tag{1.3}$$

Proof. The number of proper $(1,\ell)$-colorings of G with vertex v colored with a wildcard is $\ell \cdot \chi_{G\backslash v}(1,\ell)$. Moreover, in any proper coloring of G with v colored c_1, each vertex among the deg(v) ones adjacent to v can only be one of the ℓ wildcards. This explains the first equality in the lemma.

Let v be the vertex to which e contracts in G/e. From equation (1.2), we have

$$\chi_{G/e}(1,y) = y \cdot \chi_{(G/e)\backslash v}(1,y) + y^{\deg(v)} \cdot \chi_{(G/e)\backslash \mathrm{link}(v)}(1,y).$$

Subtracting this equation from (1.1) with $x=1$, and noting that deg(e) = deg(v) and $G\backslash$link$(e) = (G/e)\backslash$link(v), we arrive at the second equality in the lemma. □

Let P_n be the path graph on n vertices and let C_n be the cycle graph, also on n vertices (C_1 is a vertex with a loop attached while C_2 is two vertices joined by two edges). Fixing nonnegative integers k and ℓ, not both zero, we define the following sequences of numbers ($n \geq 1$):

$$\begin{aligned} a_n &= \chi_{P_n}(k,\ell), \\ b_n &= \chi_{C_n}(k,\ell). \end{aligned} \tag{1.4}$$

As we shall see, these numbers are natural generalizations of both the Fibonacci and Lucas numbers to the context of graph colorings. The following lemma uses graph decomposition to give simple recurrences for these sequences.

Lemma 1.3. *The sequences a_n and b_n satisfy the following linear recurrences with initial conditions:*

$$a_1 = k + \ell, \qquad a_2 = (k+\ell)^2 - k, \qquad a_n = (k+\ell-1)a_{n-1} + \ell a_{n-2}; \tag{1.5}$$

$$b_1 = \ell, \qquad b_2 = (k+\ell)^2 - k, \qquad b_3 = a_3 - b_2 + \ell a_1, \tag{1.6}$$

$$b_n = (k+\ell-2)b_{n-1} + (k+2\ell-1)b_{n-2} + \ell b_{n-3}. \tag{1.7}$$

Moreover, the sequence b_n satisfies a shorter recurrence if and only if $k = 0$, $k = 1$, or $\ell = 0$. When $k = 0$, this recurrence is given by $b_n = \ell b_{n-1}$, and when $k = 1$, it is

$$b_n = \ell b_{n-1} + \ell b_{n-2}. \tag{1.8}$$

Proof. The first recurrence follows from deleting an outer edge of the path graph P_n and using Lemma 1.1. To verify the second one, we first use Lemma 1.1 (picking any edge in C_n) to give

$$b_n = a_n - b_{n-1} + \ell a_{n-2}. \tag{1.9}$$

Let $c_n = b_n + b_{n-1} = a_n + \ell a_{n-2}$ and notice that c_n satisfies the same recurrence as a_n; namely,

$$\begin{aligned} c_n &= a_n + \ell a_{n-2} \\ &= (k+\ell-1)a_{n-1} + \ell a_{n-2} + \ell\left((k+\ell-1)a_{n-3} + \ell a_{n-4}\right) \\ &= (k+\ell-1)(a_{n-1} + \ell a_{n-3}) + \ell(a_{n-2} + \ell a_{n-4}) \\ &= (k+\ell-1)c_{n-1} + \ell c_{n-2}. \end{aligned} \tag{1.10}$$

It follows that b_n satisfies the third order recurrence given in the statement of the lemma. Additionally, the initial conditions for both sequences a_n and b_n are easily worked out to be the ones shown.

Finally, suppose that the sequence b_n satisfies a shorter recurrence,

$$b_n + rb_{n-1} + sb_{n-2} = 0,$$

and let

$$B = \begin{bmatrix} b_3 & b_2 & b_1 \\ b_4 & b_3 & b_2 \\ b_5 & b_4 & b_3 \end{bmatrix}.$$

Since the nonzero vector $[1, r, s]^T$ is in the kernel of B, we must have that

$$0 = \det(B) = -k^2(k-1)\ell((k+\ell-1)^2 + 4\ell).$$

It follows that for b_n to satisfy a smaller recurrence, we must have $k = 0$, $k = 1$, or $\ell = 0$. It is clear that when $k = 0$, we have $b_n = \ell^n = \ell b_{n-1}$. When $k = 1$, we can use Lemma 1.2 to see that

$$b_{n+1} = \ell(a_n + \ell a_{n-2}),$$

and combining this with (1.9) gives the recurrence stated in the lemma. □

When $k = 1$ and $\ell = 1$, the recurrences given by Lemma 1.3 when applied to the families of path graphs and cycle graphs are the Fibonacci and Lucas numbers, respectively. This observation is well-known (see [3, Examples 4.1 and 5.3]) and was brought to our attention by Cox [1]:

$$\chi_{P_n}(1,1) = F_{n+2} \qquad \text{and} \qquad \chi_{C_n}(1,1) = L_n. \tag{1.11}$$

Moreover, when $k = 2$ and $\ell = 1$, the recurrence given by Lemma 1.3 when applied to the family of path graphs is the one associated to the Pell numbers:

$$\chi_{P_n}(2,1) = Q_{n+1},$$

where $Q_0 = 1$, $Q_1 = 1$, and $Q_n = 2Q_{n-1} + Q_{n-2}$.

2. Identities

In this section, we derive some identities involving the generalized Fibonacci and Lucas numbers a_n and b_n using the graph coloring interpretation found here. In what follows, we fix $k = 1$. In this case, the a_n and b_n satisfy the following recurrences:

$$a_n = \ell a_{n-1} + \ell a_{n-2} \qquad \text{and} \qquad b_n = \ell b_{n-1} + \ell b_{n-2}.$$

Theorem 2.1. *The following identities hold:*

$$b_n = \ell a_{n-1} + \ell^2 a_{n-3}, \tag{2.1}$$

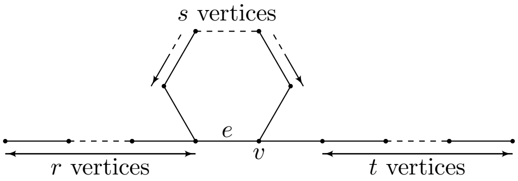
$$b_n = a_n - \ell^2 a_{n-4}, \tag{2.2}$$

$$a_{r+s} = \ell a_r a_{s-1} + \ell^2 a_{r-1} a_{s-2}, \tag{2.3}$$

$$a_{r+s} = a_r a_s - \ell^2 a_{r-2} a_{s-2}, \tag{2.4}$$

$$a_{r+s+t+1} = \ell a_r a_s a_t + \ell^3 a_{r-1} a_{s-1} a_{t-1} - \ell^4 a_{r-2} a_{s-2} a_{t-2}. \tag{2.5}$$

Proof. All the identities in the statement of the theorem follow from Lemma 1.2 when applied to different graphs (with certain choices of vertices and edges). To see the first two equations, consider the cycle graph C_n and pick any vertex and any edge. To see the next two equations, consider the path graph P_{r+s} with $v = r + 1$ and $e = \{r, r + 1\}$.



In order to prove the final equation in the statement of the theorem, consider the graph G in the above figure. It follows from Lemma 1.2 that

$$\ell a_{r+s} a_t + \ell^3 a_{r-1} a_{s-1} a_{t-1} = a_{r+s+t+1} - \ell^4 a_{r-2} a_{s-2} a_{t-1}.$$

Rearranging the terms and applying (2.4), we see that

$$\begin{aligned} a_{r+s+t+1} &= \ell a_{r+s} a_t + \ell^3 a_{r-1} a_{s-1} a_{t-1} + \ell^4 a_{r-2} a_{s-2} a_{t-1} \\ &= \ell(a_r a_s - \ell^2 a_{r-2} a_{s-2}) a_t + \ell^3 a_{r-1} a_{s-1} a_{t-1} + \ell^4 a_{r-2} a_{s-2} a_{t-1} \\ &= \ell a_r a_s a_t - \ell^3 a_{r-2} a_{s-2} (\ell a_{t-1} + \ell a_{t-2}) \\ &\qquad + \ell^3 a_{r-1} a_{s-1} a_{t-1} + \ell^4 a_{r-2} a_{s-2} a_{t-1} \\ &= \ell a_r a_s a_t + \ell^3 a_{r-1} a_{s-1} a_{t-1} - \ell^4 a_{r-2} a_{s-2} a_{t-2}. \end{aligned}$$

This completes the proof of the theorem. □

Corollary 2.2. *The following identities hold:*

$$\begin{aligned}
L_n &= F_{n+1} + F_{n-1}, \\
L_n &= F_{n+2} - F_{n-2}, \\
F_{r+s} &= F_{r+1}F_s + F_rF_{s-1}, \\
F_{r+s} &= F_{r+1}F_{s+1} - F_{r-1}F_{s-1}, \\
F_{r+s+t} &= F_{r+1}F_{s+1}F_{t+1} + F_rF_sF_t - F_{r-1}F_{s-1}F_{t-1}.
\end{aligned}$$

Proof. The identities follow from the corresponding ones in Theorem 2.1 with $\ell = 1$ by making suitable shifts of the indices and using (1.11). □

3. Further Exploration

In this note, we have produced recurrences and identities by decomposing different classes of graphs in different ways. Our treatment is by no means exhaustive, and there should be many ways to expand on what we have done here. For instance, is there a graph coloring proof of Cassini's identity?

References

[1] D. Cox, Private communication, 2007.

[2] K. Dohmen, A. Pönitz, and P. Tittmann, *A New Two-Variable Generalization of the Chromatic Polynomial*, Discrete Math. Theor. Comput. Sci., **6.1** (2003) 69–89.

[3] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Pure and Applied Mathematics (New York), Wiley Interscience, NY, 2001.

MSC2000: 05C15, 05A19, 05C38

Department of Mathematics, Texas A&M University, College Station, TX 77843
E-mail address: chillar@math.tamu.edu

Department of Mathematical Sciences, University of Copenhagen, Denmark
E-mail address: windfeldt@math.ku.dk

Published papers

Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Journal of Combinatorial Theory, Series B 98 (2008) 400–414

Journal of Combinatorial Theory

Series B

www.elsevier.com/locate/jctb

Algebraic characterization of uniquely vertex colorable graphs [☆]

Christopher J. Hillar [a], Troels Windfeldt [b]

[a] *Department of Mathematics, Texas A&M University, College Station, TX 77843, USA*
[b] *Department of Mathematical Sciences, University of Copenhagen, Denmark*

Received 22 June 2006

Available online 27 September 2007

Abstract

The study of graph vertex colorability from an algebraic perspective has introduced novel techniques and algorithms into the field. For instance, it is known that k-colorability of a graph G is equivalent to the condition $1 \in I_{G,k}$ for a certain ideal $I_{G,k} \subseteq \Bbbk[x_1, \ldots, x_n]$. In this paper, we extend this result by proving a general decomposition theorem for $I_{G,k}$. This theorem allows us to give an algebraic characterization of uniquely k-colorable graphs. Our results also give algorithms for testing unique colorability. As an application, we verify a counterexample to a conjecture of Xu concerning uniquely 3-colorable graphs without triangles.

Keywords: Vertex coloring; Gröbner basis; Colorability algorithm; Uniquely colorable graph

1. Introduction

Let G be a simple, undirected graph with vertices $V = \{1, \ldots, n\}$ and edges E. The *graph polynomial* of G is given by

$$f_G = \prod_{\substack{\{i,j\} \in E, \\ i<j}} (x_i - x_j).$$

[☆] The work of the first author was supported under a National Science Foundation Graduate Research Fellowship. The work of the second author was partially supported by Rejselegat for Matematikere. This work was conducted during the Special Semester on Gröbner Bases, February 1–July 31, 2006, organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria.

E-mail addresses: chillar@math.tamu.edu (C.J. Hillar), windfeldt@math.ku.dk (T. Windfeldt).

0095-8956/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jctb.2007.08.004

Fix a positive integer $k < n$, and let $C_k = \{c_1, \dots, c_k\}$ be a k-element set. Each element of C_k is called a *color*. A (vertex) *k-coloring* of G is a map $\nu : V \to C_k$. We say that a k-coloring ν is *proper* if adjacent vertices receive different colors; otherwise ν is called *improper*. The graph G is said to be *k-colorable* if there exists a proper k-coloring of G.

Let $\Bbbk$ be an algebraically closed field of characteristic not dividing k, so that it contains k distinct kth roots of unity. Also, set $R = \Bbbk[x_1, \dots, x_n]$ to be the polynomial ring over $\Bbbk$ in indeterminates $x_1, \dots, x_n$. Let $\mathcal{H}$ be the set of graphs with vertices $\{1, \dots, n\}$ consisting of a clique of size $k + 1$ and isolated other vertices. We will be interested in the following ideals of R:

$$J_{n,k} = \langle f_H\colon\ H \in \mathcal{H}\rangle,$$
$$I_{n,k} = \langle x_i^k - 1\colon\ i \in V\rangle,$$
$$I_{G,k} = I_{n,k} + \langle x_i^{k-1} + x_i^{k-2}x_j + \dots + x_i x_j^{k-2} + x_j^{k-1}\colon\ \{i, j\} \in E\rangle.$$

One should think of (the zeroes of) $I_{n,k}$ and $I_{G,k}$ as representing k-colorings and proper k-colorings of the graph G, respectively (see Section 3). The idea of using roots of unity and ideal theory to study graph coloring problems seems to originate in Bayer's thesis [4], although it has appeared in many other places, including the work of de Loera [9] and Lovász [10]. These ideals are important because they allow for an algebraic formulation of k-colorability. The following theorem collects the results in the series of works [3,4,9–11].

Theorem 1.1. *The following statements are equivalent*:

(1) *The graph G is not k-colorable.*
(2) $\dim_{\Bbbk} R/I_{G,k} = 0$.
(3) *The constant polynomial* 1 *belongs to the ideal $I_{G,k}$.*
(4) *The graph polynomial f_G belongs to the ideal $I_{n,k}$.*
(5) *The graph polynomial f_G belongs to the ideal $J_{n,k}$.*

The equivalence between (1) and (3) is due to Bayer [4, p. 109–112] (see also Chapter 2.7 of [1]). Alon and Tarsi [3] proved that (1) and (4) are equivalent, but also de Loera [9] and Mnuk [11] have proved this using Gröbner basis methods. The equivalence between (1) and (5) was proved by Kleitman and Lovász [10]. We give a self-contained and simplified proof of Theorem 1.1 in Section 2, in part to collect the many facts we need here.

The next result says that the generators for the ideal $J_{n,k}$ in the above theorem are very special. A proof can be found in [9]. (In Section 2, we will review the relevant definitions regarding term orders and Gröbner bases.)

Theorem 1.2 *(J. de Loera). The set of polynomials, $\{f_H\colon\ H \in \mathcal{H}\}$, is a universal Gröbner basis of $J_{n,k}$.*

Remark 1.3. The set $\mathcal{G} = \{x_1^k - 1, \dots, x_n^k - 1\}$ is a universal Gröbner basis of $I_{n,k}$, but this follows easily since the leading terms of $\mathcal{G}$ are relatively prime, regardless of term order [1, Theorem 1.7.4 and Lemma 3.3.1].

We say that a graph is *uniquely k-colorable* if there is a unique proper k-coloring up to permutation of the colors in C_k. In this case, partitions of the vertices into subsets having the same color are the same for each of the $k!$ proper colorings of G. A natural refinement of Theorem 1.1

would be an algebraic characterization of when a k-colorable graph is uniquely k-colorable. We provide such a characterization. It will be a corollary to our main theorem (Theorem 1.7) that decomposes the ideal $I_{G,k}$ into an intersection of simpler "coloring ideals." To state the theorem, however, we need to introduce some notation.

Let ν be a proper k-coloring of a graph G. Also, let $l \leqslant k$ be the number of distinct colors in $\nu(V)$. The *color class* $cl(i)$ of a vertex $i \in V$ is the set of vertices with the same color as i, and the *maximum* of a color class is the largest vertex contained in it. We set $m_1 < m_2 < \cdots < m_l = n$ to be the maximums of the l color classes.

For a subset $U \subseteq V$ of the vertices, let h_U^d be the sum of all monomials of degree d in the indeterminates $\{x_i\colon i \in U\}$. We also set $h_U^0 = 1$.

Definition 1.4 *(ν-bases).* Let ν be a proper k-coloring of a graph G. For each vertex $i \in V$, define a polynomial g_i as follows:

$$g_i = \begin{cases} x_i^k - 1 & \text{if } i = m_l, \\ h_{\{m_j,\dots,m_l\}}^{k-l+j} & \text{if } i = m_j \text{ for some } j \neq l, \\ x_i - x_{\max cl(i)} & \text{otherwise.} \end{cases} \tag{1.1}$$

The collection $\{g_1, \dots, g_n\}$ is called a *ν-basis* for the graph G with respect to the proper coloring ν.

As we shall soon see, this set is a (minimal) Gröbner basis; its initial ideal is generated by the relatively prime monomials

$$\{x_{m_1}^{k-l+1}, x_{m_2}^{k-l+2}, \dots, x_{m_l}^{k}\} \quad \text{and} \quad \{x_i\colon i \neq m_j \text{ for any } j\}.$$

A concrete instance of this construction may be found in Example 1.8 below.

Remark 1.5. It is easy to see that the map $\nu \mapsto \{g_1, \dots, g_n\}$ depends only on how ν partitions V into color classes $cl(i)$. In particular, if G is uniquely k-colorable, then there is a unique such set of polynomials $\{g_1, \dots, g_n\}$ that corresponds to G.

This discussion prepares us to make the following definition.

Definition 1.6 *(Coloring ideals).* Let ν be a proper k-coloring of a graph G. The *k-coloring ideal* (or simply *coloring ideal* if k is clear from the context) associated to ν is the ideal

$$A_\nu = \langle g_1, \dots, g_n \rangle,$$

where the g_i are given by (1.1).

In a precise way to be made clear later (see Lemma 4.4), the coloring ideal associated to ν algebraically encodes the proper k-coloring of G by ν (up to relabeling of the colors). We may now state our main theorem.

Theorem 1.7. *Let G be a simple graph with n vertices. Then*

$$I_{G,k} = \bigcap_{\nu} A_\nu,$$

where ν runs over all proper k-colorings of G.

Example 1.8. Let $G = (\{1,2,3\}, \{\{1,2\},\{2,3\}\})$ be the path graph on three vertices, and let $k = 3$. There are essentially two proper 3-colorings of G: the one where vertices 1 and 3 receive the same color, and the one where all the vertices receive different colors. If we denote by ν_1 the former, and by ν_2 the latter, then according to Definition 1.6, we have:

$$A_{\nu_1} = \langle x_3^3 - 1, x_2^2 + x_2x_3 + x_3^2, x_1 - x_3 \rangle,$$
$$A_{\nu_2} = \langle x_3^3 - 1, x_2^2 + x_2x_3 + x_3^2, x_1 + x_2 + x_3 \rangle.$$

The intersection $A_{\nu_1} \cap A_{\nu_2}$ is equal to the graph ideal,

$$I_{G,3} = \langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_2^2 + x_2x_3 + x_3^2 \rangle,$$

as predicted by Theorem 1.7.

Two interesting special cases of this theorem are the following. When G has no proper k-colorings, Theorem 1.7 says that $I_{G,k} = \langle 1 \rangle$ in accordance with Theorem 1.1. And for a graph that is uniquely k-colorable, all of the ideals A_ν are the same. This observation allows us to use Theorem 1.7 to give the following algebraic characterization of uniquely colorable graphs.

Theorem 1.9. *Suppose ν is a k-coloring of G that uses all k colors, and let $g_1, \ldots, g_n$ be given by* (1.1). *Then the following statements are equivalent*:

(1) *The graph G is uniquely k-colorable.*
(2) *The polynomials $g_1, \ldots, g_n$ generate the ideal $I_{G,k}$.*
(3) *The polynomials $g_1, \ldots, g_n$ belong to the ideal $I_{G,k}$.*
(4) *The graph polynomial f_G belongs to the ideal $I_{n,k} : \langle g_1, \ldots, g_n \rangle$.*
(5) $\dim_{\Bbbk} R/I_{G,k} = k!$.

There is also a partial analogue to Theorem 1.2 that refines Theorem 1.9. This result gives us an algorithm for determining unique k-colorability that is independent of the knowledge of a proper coloring. To state it, we need only make a slight modification of the polynomials in (1.1). Suppose that ν is a proper coloring with $l = k$ (for instance, this holds when G is uniquely k-colorable). Then, for $i \in V$ we define:

$$\tilde{g}_i = \begin{cases} x_i^k - 1 & \text{if } i = m_l, \\ h^j_{\{m_j,\ldots,m_l\}} & \text{if } i = m_j \text{ for some } j \neq l, \\ h^1_{\{i,m_2,\ldots,m_l\}} & \text{if } i \in cl(m_1), \\ x_i - x_{\max cl(i)} & \text{otherwise.} \end{cases} \tag{1.2}$$

We call the set $\{\tilde{g}_1, \ldots, \tilde{g}_n\}$ a *reduced ν-basis.*

Remark 1.10. When $l = k$, the ideals generated by the polynomials in (1.1) and in (1.2) are the same. This follows because for $i \in cl(m_1) \setminus \{m_1\}$, we have $\tilde{g}_i - \tilde{g}_{m_1} = x_i - x_{m_1} = g_i$.

Theorem 1.11. *A graph G with n vertices is uniquely k-colorable if and only if the reduced Gröbner basis for $I_{G,k}$ with respect to any term order with $x_n \prec \cdots \prec x_1$ has the form $\{\tilde{g}_1, \ldots, \tilde{g}_n\}$ for polynomials as in* (1.2).

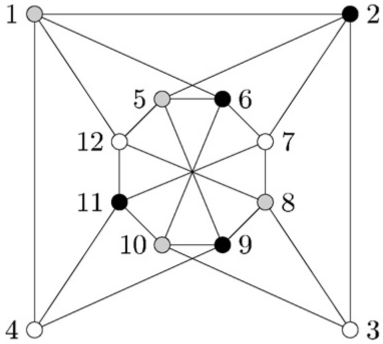


Fig. 1. A uniquely 3-colorable graph [5].

Remark 1.12. It is not difficult to test whether a Gröbner basis is of the form given by (1.2). Moreover, the unique coloring can be easily recovered from the reduced Gröbner basis.

In Section 6, we shall discuss the tractability of our algorithms. We hope that they might be used to perform experiments for raising and settling problems in the theory of (unique) colorability.

Example 1.13. We present an example of a uniquely 3-colorable graph on $n = 12$ vertices and give the polynomials $\tilde{g}_1, \dots, \tilde{g}_n$ from Theorem 1.11.

Let G be the graph given in Fig. 1. The indicated 3-coloring partitions V into $k = l = 3$ color classes with $(m_1, m_2, m_3) = (10, 11, 12)$. The following set of 12 polynomials is the reduced Gröbner basis for the ideal $I_{G,k}$ with respect to any term ordering with $x_{12} \prec \cdots \prec x_1$. The leading terms of each $\tilde{g}_i$ are underlined.

$$\begin{aligned}\{&\underline{x_{12}^3} - 1, \underline{x_7} - x_{12}, \underline{x_4} - x_{12}, \underline{x_3} - x_{12},\\ &\underline{x_{11}^2} + x_{11}x_{12} + x_{12}^2, \underline{x_9} - x_{11}, \underline{x_6} - x_{11}, \underline{x_2} - x_{11},\\ &\underline{x_{10}} + x_{11} + x_{12}, \underline{x_8} + x_{11} + x_{12}, \underline{x_5} + x_{11} + x_{12}, \underline{x_1} + x_{11} + x_{12}\}.\end{aligned}$$

Notice that the leading terms of the polynomials in each line above correspond to the different color classes of this coloring of G.

The organization of this paper is as follows. In Section 2, we discuss some of the algebraic tools that will go into the proofs of our main results. Section 3 is devoted to a proof of Theorem 1.1, and in Sections 4 and 5, we present proofs for Theorems 1.7, 1.9, and 1.11. Theorems 1.1 and 1.9 give algorithms for testing k-colorability and unique k-colorability of graphs, and we discuss the implementation of them in Section 6, along with a verification of a counterexample [2] to a conjecture [5,8,12] by Xu concerning uniquely 3-colorable graphs without triangles.

2. Algebraic preliminaries

We briefly review the basic concepts of commutative algebra that will be useful for us here. We refer to [7] or [6] for more details. Let I be an ideal of $R = \Bbbk[x_1, \dots, x_n]$. The *variety* $V(I)$ of I is the set of points in $\Bbbk^n$ that are zeroes of all the polynomials in I. Conversely, the *vanishing* *ideal* $I(V)$ of a set $V \subseteq \mathbb{k}^n$ is the ideal of those polynomials vanishing on all of V. These two definitions are related by way of $V(I(V)) = V$ and $I(V(I)) = \sqrt{I}$, in which

$$\sqrt{I} = \{f\colon\ f^n \in I \text{ for some } n\}$$

is the *radical* of I. The ideal I is said to be of *Krull dimension zero* (or simply *zero-dimensional*) if $V(I)$ is finite. A *term order* $\prec$ for the monomials of R is a well-ordering which is multiplicative ($u \prec v \Rightarrow wu \prec wv$ for monomials u, v, w) and for which the constant monomial 1 is smallest. The *initial term* (or *leading monomial*) $in_\prec(f)$ of a polynomial $f \in R$ is the largest monomial in f with respect to $\prec$. The *standard monomials* $\mathcal{B}_\prec(I)$ of I are those monomials which are not the leading monomials of any polynomial in I.

Many arguments in commutative algebra and algebraic geometry are simplified when restricted to radical, zero-dimensional ideals (respectively multiplicity-free, finite varieties), and those found in this paper are not exceptions. The following fact is useful in this regard.

Lemma 2.1. *Let I be a zero-dimensional ideal and fix a term order $\prec$. Then* $\dim_{\mathbb{k}} R/I = |\mathcal{B}_\prec(I)| \geqslant |V(I)|$. *Furthermore, the following are equivalent*:

(1) *I is a radical ideal* (*i.e.,* $I = \sqrt{I}$).
(2) *I contains a univariate square-free polynomial in each indeterminate.*
(3) $|\mathcal{B}_\prec(I)| = |V(I)|$.

Proof. See [6, p. 229, Proposition 4] and [7, pp. 39–41, Proposition 2.7 and Theorem 2.10]. □

A finite subset $\mathcal{G}$ of an ideal I is a *Gröbner basis* (with respect to $\prec$) if the *initial ideal*,

$$in_\prec(I) = \langle in_\prec(f)\colon\ f \in I\rangle,$$

is generated by the initial terms of elements of $\mathcal{G}$. It is called *minimal* if no leading term of $f \in G$ divides any other leading term of polynomials in G. Furthermore, a *universal Gröbner basis* is a set of polynomials which is a Gröbner basis with respect to all term orders. Many of the properties of I and $V(I)$ can be calculated by finding a Gröbner basis for I, and such generating sets are fundamental for computation (including the algorithms presented in the last section).

Finally, a useful operation on two ideals I and J is the construction of the *colon ideal* $I : J = \{h \in R\colon\ hJ \subseteq I\}$. If V and W are two varieties, then the colon ideal

$$I(V) : I(W) = I(V \backslash W) \tag{2.1}$$

corresponds to a set difference [6, p. 193, Corollary 8].

3. Vertex colorability

In what follows, the set of colors C_k will be the set of kth roots of unity, and we shall freely speak of points in $\mathbb{k}^n$ with all coordinates in C_k as colorings of G. In this case, a point $(v_1, \ldots, v_n) \in \mathbb{k}^n$ corresponds to a coloring of vertex i with color v_i for $i = 1, \ldots, n$. The varieties corresponding to the ideals $I_{n,k}$, $I_{G,k}$, and $I_{n,k} + \langle f_G\rangle$ partition the k-colorings of G as follows.

Lemma 3.1. *The varieties $V(I_{n,k})$, $V(I_{G,k})$, and $V(I_{n,k} + \langle f_G\rangle)$ are in bijection with all, the proper, and the improper k-colorings of G, respectively.*

Proof. The points in $V(I_{n,k})$ are all n-tuples of kth roots of unity and therefore naturally correspond to all k-colorings of G. Let $\mathbf{v} = (v_1, \ldots, v_n) \in V(I_{G,k})$; we must show that it corresponds to a proper coloring of G. Let $\{i, j\} \in E$ and set

$$q_{ij} = \frac{x_i^k - x_j^k}{x_i - x_j} \in I_{G,k}.$$

If $v_i = v_j$, then $q_{ij}(\mathbf{v}) = kv_i^{k-1} \neq 0$. Thus, the coloring $\mathbf{v}$ is proper. Conversely, suppose that $\mathbf{v} = (v_1, \ldots, v_n)$ is a proper coloring of G. Then, since

$$q_{ij}(\mathbf{v})(v_i - v_j) = \left(v_i^k - v_j^k\right) = 1 - 1 = 0,$$

it follows that for $\{i, j\} \in E$, we have $q_{ij}(\mathbf{v}) = 0$. This shows that $\mathbf{v} \in V(I_{G,k})$. If $\mathbf{v}$ is an improper coloring, then it is easy to see that $f_G(\mathbf{v}) = 0$. Moreover, any $\mathbf{v} \in V(I_{n,k})$ for which $f_G(\mathbf{v}) = 0$ has two coordinates, corresponding to an edge in G, that are equal. □

The next result follows directly from Lemma 2.1. It will prove useful in simplifying many of the proofs in this paper.

Lemma 3.2. *The ideals $I_{n,k}$, $I_{G,k}$, and $I_{n,k} + \langle f_G \rangle$ are radical.*

We next describe a relationship between $I_{n,k}$, $I_{G,k}$, and $I_{n,k} + \langle f_G \rangle$.

Lemma 3.3. $I_{n,k} : I_{G,k} = I_{n,k} + \langle f_G \rangle$.

Proof. Let V and W be the set of all colorings and proper colorings, respectively, of the graph G. Now apply Lemmas 3.1 and 3.2 to Eq. (2.1). □

The vector space dimensions of the residue rings corresponding to these ideals are readily computed from the above discussion. Recall that the *chromatic polynomial* χ_G is the univariate polynomial for which $\chi_G(k)$ is the number of proper k-colorings of G.

Lemma 3.4. *Let χ_G be the chromatic polynomial of G. Then*

$$\begin{aligned} &\chi_G(k) = \dim_{\mathbb{k}} R/I_{G,k}, \\ &k^n - \chi_G(k) = \dim_{\mathbb{k}} R/\left(I_{n,k} + \langle f_G \rangle\right). \end{aligned}$$

Proof. Both equalities follow from Lemmas 2.1 and 3.1. □

Let $K_{n,k}$ be the ideal of all polynomials $f \in R$ such that $f(v_1, \ldots, v_n) = 0$ for any $(v_1, \ldots, v_n) \in \mathbb{k}^n$ with at most k of the v_i distinct. Clearly, $J_{n,k} \subseteq K_{n,k}$. We will need the following result of Kleitman and Lovász [10].

Theorem 3.5 *(Kleitman–Lovász). The ideals $K_{n,k}$ and $J_{n,k}$ are the same.*

We now prove Theorem 1.1. We feel that it is the most efficient proof of this result.

Proof of Theorem 1.1. (1) ⇒ (2) ⇒ (3): Suppose that G is not k-colorable. Then it follows from Lemma 3.4 that $\dim_{\mathbb{k}} R/I_{G,k} = 0$ and so $1 \in I_{G,k}$.

(3) ⇒ (4): Suppose that $I_{G,k} = \langle 1 \rangle$ so that $I_{n,k} : I_{G,k} = I_{n,k}$. Then Lemma 3.3 implies that $I_{n,k} + \langle f_G \rangle = I_{n,k}$ and hence $f_G \in I_{n,k}$.

(4) ⇒ (1): Assume that f_G belongs to the ideal $I_{n,k}$. Then $I_{n,k} + \langle f_G \rangle = I_{n,k}$, and it follows from Lemma 3.4 that $k^n - \chi_G(k) = k^n$. Therefore, $\chi_G(k) = 0$ as desired.

(5) ⇒ (1): Suppose that $f_G \in J_{n,k}$. Then from Theorem 3.5, there can be no proper coloring $\mathbf{v}$ (there are at most k distinct coordinates).

(1) ⇒ (5): If G is not k-colorable, then for every substitution $\mathbf{v} \in \Bbbk^n$ with at most k distinct coordinates, we must have $f_G(\mathbf{v}) = 0$. It follows that $f_G \in J_{n,k}$ from Theorem 3.5. □

4. Coloring ideals

In this section, we study the k-coloring ideals A_ν mentioned in the introduction and prove Theorem 1.7. Let G be a graph with proper coloring ν, and let $l \leqslant k$ be the number of distinct colors in $\nu(V)$. For each vertex $i \in V$, we assign polynomials g_i and $\tilde{g}_i$ as in Eqs. (1.1) and (1.2). One should think (loosely) of the first case of (1.1) as corresponding to a choice of a color for the last vertex; the second, to subsets of vertices in different color classes; and the third, to the fact that elements in the same color class should have the same color. These polynomials encode the coloring ν algebraically in a computationally useful way (see Lemmas 4.1 and 4.4 below). We begin by showing that the polynomials g_i are a special generating set for the coloring ideal A_ν.

Recall that a *reduced Gröbner basis* $\mathcal{G}$ is a Gröbner basis such that (1) the coefficient of $in_\prec(g)$ for each $g \in \mathcal{G}$ is 1 and (2) the leading monomial of any $g \in \mathcal{G}$ does not divide any monomial occurring in another polynomial in $\mathcal{G}$. Given a term order, reduced Gröbner bases exist and are unique.

Lemma 4.1. *Let $\prec$ be any term order with $x_n \prec \cdots \prec x_1$. Then the set of polynomials $\{g_1, \ldots, g_n\}$ is a minimal Gröbner basis with respect to $\prec$ for the ideal $A_\nu = \langle g_1, \ldots, g_n \rangle$ it generates. Moreover, for this ordering, the set $\{\tilde{g}_1, \ldots, \tilde{g}_n\}$ is a reduced Gröbner basis for $\langle \tilde{g}_1, \ldots, \tilde{g}_n \rangle$.*

Proof. Since the initial term of each g_i (respectively $\tilde{g}_i$) is a power of x_i, each pair of leading terms is relatively prime. It follows that these polynomials form a Gröbner basis for the ideal they generate. By inspection, it is easy to see that the set of polynomials given by (1.1) (respectively (1.2)) is minimal (respectively reduced). □

The following innocuous-looking fact is a very important ingredient in the proof of Lemma 4.4.

Lemma 4.2. *Let U be a subset of $\{1, \ldots, n\}$, and suppose that $\{i, j\} \subseteq U$. Then*

$$(x_i - x_j)h_U^d = h_{U \setminus \{j\}}^{d+1} - h_{U \setminus \{i\}}^{d+1}, \tag{4.1}$$

for all nonnegative integers d.

Proof. The first step is to note that the polynomial

$$x_i h_U^d + h_{U \setminus \{i\}}^{d+1}$$

is symmetric in the indeterminants $\{x_\ell \colon \ell \in U\}$. This follows from the polynomial identity

$$h_U^{d+1} - h_{U \setminus \{i\}}^{d+1} = x_i h_U^d,$$

and the fact that h_U^{d+1} is symmetric in the indeterminants $\{x_\ell\colon \ell \in U\}$. Let σ be the permutation (ij), and notice that

$$x_i h_U^d + h_{U\setminus\{i\}}^{d+1} = \sigma\big(x_i h_U^d + h_{U\setminus\{i\}}^{d+1}\big) = x_j h_U^d + h_{U\setminus\{j\}}^{d+1}.$$

This completes the proof. □

We shall also need the following fact that gives explicit representations of some of the generators of $I_{n,k}$ in terms of those of A_ν.

Lemma 4.3. *For each $i = 1, \ldots, l$, we have*

$$x_{m_i}^k - 1 = x_n^k - 1 + \sum_{t=i}^{l-1} \Bigg[\prod_{j=t+1}^{l} (x_{m_i} - x_{m_j})\Bigg] h_{\{m_t,\ldots,m_l\}}^{k-l+t}. \tag{4.2}$$

Proof. To verify (4.2) for a fixed i, we will use Lemma 4.2 and induction to prove that for each positive integer $s \leqslant l - i$, the sum on the right hand-side above is equal to

$$\prod_{j=s+i}^{l} (x_{m_i} - x_{m_j}) h_{\{m_i,m_{s+i},\ldots,m_l\}}^{k-l+s+i-1} + \sum_{t=s+i}^{l-1} \Bigg[\prod_{j=t+1}^{l} (x_{m_i} - x_{m_j})\Bigg] h_{\{m_t,\ldots,m_l\}}^{k-l+t}. \tag{4.3}$$

For $s = 1$, this is clear as (4.3) is exactly the sum on the right-hand side of (4.2). In general, using Lemma 4.2, the first term on the left-hand side of (4.3) is

$$\prod_{j=s+1+i}^{l} (x_{m_i} - x_{m_j}) \big(h_{\{m_i,m_{s+1+i},\ldots,m_l\}}^{k-l+s+i} - h_{\{m_{s+i},\ldots,m_l\}}^{k-l+s+i}\big),$$

which is easily seen to cancel the first summand in the sum found in (4.3).

Now, Eq. (4.3) with $s = l - i$ gives us that the right-hand side of (4.2) is

$$x_n^k - 1 + (x_{m_i} - x_{m_l}) h_{\{m_i,m_l\}}^{k-1} = x_n^k - 1 + x_{m_i}^k - x_n^k = x_{m_i}^k - 1,$$

proving the claim (recall that $m_l = n$). □

That the polynomials $g_1, \ldots, g_n$ represent an algebraic encoding of the coloring ν is explained by the following technical lemma.

Lemma 4.4. *Let $g_1, \ldots, g_n$ be given as in* (1.1). *Then the following three properties hold for the ideal $A_\nu = \langle g_1, \ldots, g_n\rangle$:*

(1) *$I_{G,k} \subseteq A_\nu$,*
(2) *A_ν is radical,*
(3) *$|V(A_\nu)| = \prod_{j=1}^{l}(k - l + j)$.*

Proof. First assume that $I_{G,k} \subseteq A_\nu$. Then A_ν is radical from Lemma 2.1, and the number of standard monomials of A_ν (with respect to any ordering $\prec$ as in Lemma 4.1) is equal to $|V(A_\nu)|$. Since $\{g_1, \ldots, g_n\}$ is a Gröbner basis for A_ν and the initial ideal is generated by the monomials

$$\big\{x_{m_1}^{k-l+1}, x_{m_2}^{k-l+2}, \ldots, x_{m_l}^{k}\big\} \quad \text{and} \quad \{x_i\colon i \neq m_j \text{ for any } j\},$$

it follows that $|\mathcal{B}_\prec(A_\nu)| = \prod_{j=1}^{l}(k - l + j)$. This proves (3).

We now prove statement (1). From Lemma 4.3, it follows that $x_i^k - 1 \in A$ when $i \in \{m_1, \dots, m_l\}$. It remains to show that $x_i^k - 1 \in A_\nu$ for all vertices not in $\{m_1, \dots, m_l\}$. Let $f_i = x_i - x_{\max cl(i)}$ and notice that

$$x_{\max cl(i)}^k - 1 = (x_i - f_i)^k - 1 = x_i^k - 1 + f_i h \in A_\nu$$

for some polynomial h. It follows that $x_i^k - 1 \in A_\nu$.

Finally, we must verify that the other generators of $I_{G,k}$ are in A_ν. To accomplish this, we will prove the following stronger statement:

$$U \subseteq \{m_1, \dots, m_l\} \quad \text{with } |U| \geqslant 2 \quad \Rightarrow \quad h_U^{k+1-|U|} \in A_\nu. \tag{4.4}$$

We downward induct on $s = |U|$. In the case $s = l$, we have $U = \{m_1, \dots, m_l\}$. But then as is easily checked $g_{m_1} = h_U^{k+1-|U|} \in A_\nu$. For the general case, we will show that if one polynomial $h_U^{k+1-|U|}$ is in A_ν, with $|U| = s < l$, then $h_U^{k+1-|U|} \in A_\nu$ for any subset $U \subseteq \{m_1, \dots, m_l\}$ of cardinality s. In this regard, suppose that $h_U^{k+1-|U|} \in A_\nu$ for a subset U with $|U| = s < l$. Let $u \in U$ and $v \in \{m_1, \dots, m_l\} \backslash U$, and examine the following equality (using Lemma 4.2):

$$(x_u - x_v) h_{\{v\} \cup U}^{k-s} = h_U^{k-s+1} - h_{\{v\} \cup U \backslash \{u\}}^{k-s+1}.$$

By induction, the left-hand side of this equation is in A_ν and therefore the assumption on U implies that

$$h_{\{v\} \cup U \backslash \{u\}}^{k-s+1} \in A_\nu.$$

This shows that we may replace any element of U with any element of $\{m_1, \dots, m_l\}$. Since there is a subset U of size s with $h_U^{k+1-|U|} \in A_\nu$ (see (1.1)), it follows from this that we have $h_U^{k+1-|U|} \in A_\nu$ for any subset U of size s. This completes the induction.

A similar trick as before using polynomials $x_i - x_{\max cl(i)} \in A_\nu$ proves that we may replace in (4.4) the requirement that $U \subseteq \{m_1, \dots, m_l\}$ with one that says that U consists of vertices in different color classes. If $\{i, j\} \in E$, then i and j are in different color classes, and therefore the generator $h_{\{i,j\}}^{k-1} \in I_{G,k}$ is in A_ν. This finishes the proof of the lemma. □

Remark 4.5. Property (1) in the lemma says that $V(A_\nu)$ contains only proper colorings of G while properties (2) and (3) say that, up to relabeling the colors, the zeroes of the polynomials $g_1, \dots, g_n$ correspond to the single proper coloring given by ν. The lemma also implies that the polynomials $\{g_1, \dots, g_n\}$ form a complete intersection.

The decomposition theorem for $I_{G,k}$ mentioned in the introduction now follows easily from the results of this section.

Proof of Theorem 1.7. By Lemmas 3.1 and 4.4, we have

$$V(I_{G,k}) = \bigcup_\nu V(A_\nu),$$

where ν runs over all proper k-colorings of G. Since the ideals $I_{G,k}$ and A_ν are radical by Lemmas 3.2 and 4.4, it follows that:

$$I_{G,k} = I\big(V(I_{G,k})\big) = I \bigcup_\nu V(A_\nu) = \bigcap_\nu I\big(V(A_\nu)\big) = \bigcap_\nu A_\nu.$$

This completes the proof. □

5. Unique vertex colorability

We are now in a position to prove our characterizations of uniquely k-colorable graphs.

Proof of Theorem 1.9. (1) $\Rightarrow$ (2) $\Rightarrow$ (3): Suppose the graph G is uniquely k-colorable and construct the set of g_i from (1.1) using the proper k-coloring ν. By Theorem 1.7, it follows that $I_{G,k} = A_\nu$, and thus the g_i generate $I_{G,k}$.

(3) $\Rightarrow$ (4): Suppose that $A_\nu = \langle g_1, \ldots, g_n\rangle \subseteq I_{G,k}$. From Lemma 3.3, we have

$$I_{n,k} + \langle f_G\rangle = I_{n,k} : I_{G,k} \subseteq I_{n,k} : A_\nu.$$

This proves that $f_G \in I_{n,k} : \langle g_1, \ldots, g_n\rangle$.

(4) $\Rightarrow$ (5) $\Rightarrow$ (1): Assume that $f_G \in I_{n,k} : \langle g_1, \ldots, g_n\rangle$. Then,

$$I_{n,k} : I_{G,k} = I_{n,k} + \langle f_G\rangle \subseteq I_{n,k} : \langle g_1, \ldots, g_n\rangle.$$

Applying Lemmas 2.1 and 4.4, we have

$$k^n - k! = \left|V(I_{n,k})\backslash V(A_\nu)\right| = \left|V(I_{n,k} : A_\nu)\right| \leqslant \left|V(I_{n,k} : I_{G,k})\right| \leqslant k^n - k!, \tag{5.1}$$

since the number of improper colorings is at most $k^n - k!$. It follows that equality holds throughout (5.1) so that the number of proper colorings is $k!$. Therefore, we have $\dim_{\Bbbk} R/I_{G,k} = k!$ from Lemma 3.4 and G is uniquely k-colorable. □

Proof of Theorem 1.11. Suppose that the reduced Gröbner basis of $I_{G,k}$ with respect to a term order with $x_n \prec \cdots \prec x_1$ has the form $\{\tilde{g}_1, \ldots, \tilde{g}_n\}$ as in (1.2). Also, let $\{g_1, \ldots, g_n\}$ be the ν-basis (1.1) corresponding to the k-coloring ν read off from $\{\tilde{g}_1, \ldots, \tilde{g}_n\}$. By Remark 1.10, we have $\langle g_1, \ldots, g_n\rangle = \langle \tilde{g}_1, \ldots, \tilde{g}_n\rangle$. It follows that G is uniquely k-colorable from (2) $\Rightarrow$ (1) of Theorem 1.9. For the other implication, by Lemma 4.1, it is enough to show that $A_\nu = \langle g_1, \ldots, g_n\rangle = I_{G,k}$, which is (1) $\Rightarrow$ (2) in Theorem 1.9. □

6. Algorithms and Xu's conjecture

In this section we describe the algorithms implied by Theorems 1.1 and 1.9, and illustrate their usefulness by disproving a conjecture of Xu.[1] We also present some data to illustrate their runtimes under different circumstances.

From Theorem 1.1, we have the following four methods for determining k-colorability. They take as input a graph G with vertices $V = \{1, \ldots, n\}$ and edges E, and a positive integer k, and output TRUE if G is k-colorable and otherwise FALSE.

```
function IsColorable($G$, $k$) [Theorem 1.1 (2)]
    Compute a Gröbner basis $\mathcal{G}$ of $I_{G,k}$.
    Compute the vector space dimension of $R/I_{G,k}$ over $\Bbbk$.
    if $\dim_{\Bbbk} R/I_{G,k} = 0$ then return FALSE else return TRUE.
end function
```

```
function IsColorable($G$, $k$) [Theorem 1.1 (3)]
    Compute a Gröbner basis $\mathcal{G}$ of $I_{G,k}$.
```

[1] Code that performs this calculation along with an implementation in SINGULAR 3.0 (http://www.singular.uni-kl.de) of the algorithms in this section can be found at http://www.math.tamu.edu/~chillar/.

```
3:     Compute the normal form $\mathrm{nf}_{\mathcal{G}}(1)$ of the constant polynomial 1 with respect to $\mathcal{G}$.
4:     if $\mathrm{nf}_{\mathcal{G}}(1) = 0$ then return False else return True.
5: end function
```

```
1: function IsColorable($G$, $k$) [Theorem 1.1 (4)]
2:     Set $\mathcal{G} := \{x_i^k - 1\colon i \in V\}$.
3:     Compute the normal form $\mathrm{nf}_{\mathcal{G}}(f_G)$ of the graph polynomial $f_G$ with respect to $\mathcal{G}$.
4:     if $\mathrm{nf}_{\mathcal{G}}(f_G) = 0$ then return False else return True.
5: end function
```

```
1: function IsColorable($G$, $k$) [Theorem 1.1 (5)]
2:     Let $\mathcal{H}$ be the set of graphs with vertices $\{1, \dots, n\}$ consisting of a clique of size $k + 1$
       and isolated vertices.
3:     Set $\mathcal{G} := \{f_H\colon H \in \mathcal{H}\}$.
4:     Compute the normal form $\mathrm{nf}_{\mathcal{G}}(f_G)$ of the graph polynomial $f_G$ with respect to $\mathcal{G}$.
5:     if $\mathrm{nf}_{\mathcal{G}}(f_G) = 0$ then return False else return True.
6: end function
```

From Theorem 1.9, we have the following three methods for determining unique k-colorability. They take as input a graph G with vertices $V = \{1, \dots, n\}$ and edges E, and output True if G is uniquely k-colorable and otherwise False. Furthermore, the first two methods take as input a proper k-coloring ν of G that uses all k colors, while the last method requires a positive integer k.

```
1: function IsColorable($G$, $\nu$) [Theorem 1.9 (3)]
2:     Compute a Gröbner basis $\mathcal{G}$ of $I_{G,k}$.
3:     for $i \in V$ do
4:         Compute the normal form $\mathrm{nf}_{\mathcal{G}}(g_i)$ of the polynomial $g_i$ with respect to $\mathcal{G}$.
5:         if $\mathrm{nf}_{\mathcal{G}}(g_i) \neq 0$ then return False.
6:     end for
7:     return True.
8: end function
```

```
1: function IsColorable($G$, $\nu$) [Theorem 1.9 (4)]
2:     Compute a Gröbner basis $\mathcal{G}$ of $I_{n,k} : \langle g_1, \dots, g_n \rangle$.
3:     Compute the normal form $\mathrm{nf}_{\mathcal{G}}(f_G)$ of the graph polynomial $f_G$ with respect to $\mathcal{G}$.
4:     if $\mathrm{nf}_{\mathcal{G}}(f_G) = 0$ then return True else return False.
5: end function
```

```
1: function IsColorable($G$, $k$) [Theorem 1.9 (5)]
2:     Compute a Gröbner basis $\mathcal{G}$ of $I_{G,k}$.
3:     Compute the vector space dimension of $R/I_{G,k}$ over $\Bbbk$.
4:     if $\dim_{\Bbbk} R/I_{G,k} = k!$ then return True else return False.
5: end function
```

Remark 6.1. It is possible to speed up the above algorithms dramatically by doing some of the computations iteratively. First of all, step 2 of methods (2) and (3) of Theorem 1.1, and methods (3) and (5) of Theorem 1.9 should be replaced by the following code

```
1: Set $I := I_{n,k}$.
2: for $\{i, j\} \in E$ do
3:     Compute a Gröbner basis $\mathcal{G}$ of $I + \langle x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1}\rangle$.
4:     Set $I := \langle \mathcal{G} \rangle$.
5: end for
```

Secondly, the number of terms in the graph polynomial f_G when fully expanded may be very large. The computation of the normal form $\mathrm{nf}_{\mathcal{G}}(f_G)$ of the graph polynomial f_G in methods (4) and (5) of Theorem 1.1, and method (4) of Theorem 1.9 should therefore be replaced by the following code

```
1: Set $f := 1$.
2: for $\{i, j\} \in E$ with $i < j$ do
3:     Compute the normal form $\mathrm{nf}_{\mathcal{G}}((x_i - x_j)f)$ of $(x_i - x_j)f$ with respect to $\mathcal{G}$,
       and set $f := \mathrm{nf}_{\mathcal{G}}((x_i - x_j)f)$.
4: end for
```

In [12], Xu showed that if G is a uniquely k-colorable graph with $|V| = n$ and $|E| = m$, then $m \geqslant (k-1)n - \binom{k}{2}$, and this bound is best possible. He went on to conjecture that if G is uniquely k-colorable with $|V| = n$ and $|E| = (k-1)n - \binom{k}{2}$, then G contains a k-clique. In [2], this conjecture was shown to be false for $k = 3$ and $|V| = 24$ using the graph in Fig. 2; however, the proof is somewhat complicated. We verified that this graph is indeed a counterexample to Xu's conjecture using several of the above mentioned methods. The fastest verification requires less than two seconds of processor time on a laptop PC with a 1.5 GHz Intel Pentium M processor and 1.5 GB of memory. The code can be downloaded from the link at the beginning of this section. The speed of these calculations should make the testing of conjectures for uniquely colorable graphs a more tractable enterprise.

Below are the runtimes for the graphs in Figs. 1 and 2. The term orders used are given in the notation of the computational algebra program Singular: lp is the lexicographical ordering, Dp is the degree lexicographical ordering, and dp is the degree reverse lexicographical ordering. That

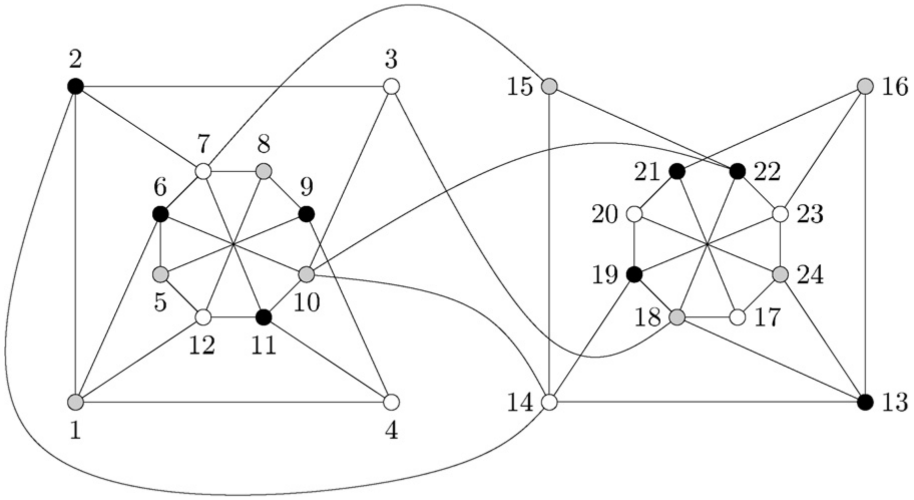


Fig. 2. A counterexample to Xu's conjecture [2].

the computation did not finish within 10 minutes is denoted by "> 600," while "–" means that the computation ran out of memory.

Characteristic	0			2		
Term order	lp	Dp	dp	lp	Dp	dp
Theorem 1.1 (2)	3.28	2.29	1.24	2.02	1.56	0.81
Theorem 1.1 (3)	3.30	2.42	1.25	2.15	1.60	0.94
Theorem 1.1 (4)	1.86	> 600	> 600	1.08	448.28	324.89
Theorem 1.1 (5)	> 600	> 600	> 600	> 600	> 600	> 600
Theorem 1.9 (3)	3.53	2.54	1.43	2.23	1.72	1.03
Theorem 1.9 (4)	> 600	> 600	> 600	> 600	> 600	> 600
Theorem 1.9 (5)	3.30	2.28	1.24	2.03	1.54	0.82

Runtimes in seconds for the graph in Fig. 1.

Characteristic	0			2		
Term order	lp	Dp	dp	lp	Dp	dp
Theorem 1.1 (2)	596.89	33.32	2.91	144.05	12.45	1.64
Theorem 1.1 (3)	598.25	33.47	2.87	144.60	12.44	1.81
Theorem 1.1 (4)	–	> 600	> 600	–	> 600	> 600
Theorem 1.1 (5)	> 600	> 600	> 600	> 600	> 600	> 600
Theorem 1.9 (3)	597.44	34.89	4.29	145.81	13.55	3.02
Theorem 1.9 (4)	–	–	–	–	–	–
Theorem 1.9 (5)	595.97	33.46	2.94	145.02	12.34	1.64

Runtimes in seconds for the graph in Fig. 2.

Another way one can prove that a graph is uniquely k-colorable is by computing the chromatic polynomial and testing if it equals $k!$ when evaluated at k. This is possible for the graph in Fig. 1. Maple reports that it has chromatic polynomial

$$\begin{aligned} &x(x-2)(x-1)\bigl(x^9-20x^8+191x^7-1145x^6+4742x^5 \\ &\quad -14028x^4+29523x^3-42427x^2+37591x-15563\bigr). \end{aligned}$$

When evaluated at $x = 3$ we get the expected result $6 = 3!$. Computing the above chromatic polynomial took 94.83 seconds. Maple, on the other hand, was not able to compute the chromatic polynomial of the graph in Fig. 2 within 10 hours.

Acknowledgments

We would like to thank the anonymous referees for valuable comments that greatly improved this work. We also thank Keith Briggs for pointing out an error in our drawing of the graph appearing in Fig. 2.

References

[1] W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Amer. Math. Soc., 1994.

[2] S. Akbari, V.S. Mirrokni, B.S. Sadjad, K_r-Free uniquely vertex colorable graphs with minimum possible edges, J. Combin. Theory Ser. B 82 (2001) 316–318.

[3] N. Alon, M. Tarsi, Colorings and orientations of graphs, Combinatorica 12 (1992) 125–134.

[4] D. Bayer, The division algorithm and the Hilbert scheme, PhD thesis, Harvard University, 1982.

[5] C.-Y. Chao, Z. Chen, On uniquely 3-colorable graphs, Discrete Math. 112 (1993) 21–27.

[6] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Springer-Verlag, New York, 1997.

[7] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, Springer-Verlag, New York, 1998.

[8] A. Daneshgar, R. Naserasr, On small uniquely vertex-colourable graphs and Xu's conjecture, Discrete Math. 223 (2000) 93–108.

[9] J.A. de Loera, Gröbner bases and graph colorings, Beiträge Algebra Geom. 36 (1995) 89–96.

[10] L. Lovász, Stable sets and polynomials, Discrete Math. 124 (1994) 137–153.

[11] M. Mnuk, On an algebraic description of colorability of planar graphs, in: Koji Nakagawa (Ed.), Logic, Mathematics and Computer Science: Interactions, Proceedings of the Symposium in Honor of Bruno Buchberger's 60th Birthday, RISC, Linz, Austria, October 20–22, 2002, pp. 177–186.

[12] S. Xu, The size of uniquely colorable graphs, J. Combin. Theory Ser. B 50 (1990) 319–320.

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 12, December 2008, Pages 4135–4137
S 0002-9939(08)09427-6
Article electronically published on June 11, 2008

MINIMAL GENERATORS FOR SYMMETRIC IDEALS

CHRISTOPHER J. HILLAR AND TROELS WINDFELDT

(Communicated by Bernd Ulrich)

Abstract. Let $R = K[X]$ be the polynomial ring in infinitely many indeterminates X over a field K, and let $\mathfrak{S}_X$ be the symmetric group of X. The group $\mathfrak{S}_X$ acts naturally on R, and this in turn gives R the structure of a module over the group ring $R[\mathfrak{S}_X]$. A recent theorem of Aschenbrenner and Hillar states that the module R is Noetherian. We address whether submodules of R can have any number of minimal generators, answering this question positively.

Let $R = K[X]$ be the polynomial ring in infinitely many indeterminates X over a field K. Write $\mathfrak{S}_X$ (resp. $\mathfrak{S}_N$) for the symmetric group of X (resp. $\{1, \ldots, N\}$) and $R[\mathfrak{S}_X]$ for its (left) group ring, which acts naturally on R. A *symmetric ideal* $I \subseteq R$ is an $R[\mathfrak{S}_X]$-submodule of R.

Aschenbrenner and Hillar recently proved [1] that all symmetric ideals are finitely generated over $R[\mathfrak{S}_X]$. They were motivated by finiteness questions in chemistry [3] and algebraic statistics [2]. In proving the Noetherianity of R, it was shown that a symmetric ideal I has a special, finite set of generators called a *minimal Gröbner basis*. However, the more basic question of whether I is always cyclic (already asked by Josef Schicho [4]) was left unanswered in [1]. Our result addresses a generalization of this important issue.

Theorem 1. *For every positive integer n, there are symmetric ideals of R generated by n polynomials which cannot have fewer than n $R[\mathfrak{S}_X]$-generators.*

In what follows, we work with the set $X = \{x_1, x_2, x_3, \ldots\}$, although as remarked in [1], this is not really a restriction. In this case, $\mathfrak{S}_X$ is naturally identified with $\mathfrak{S}_\infty$, the permutations of the positive integers, and $\sigma x_i = x_{\sigma i}$ for $\sigma \in \mathfrak{S}_\infty$.

Let M be a finite multiset of positive integers and let $i_1, \ldots, i_k$ be the list of its distinct elements, arranged so that $m(i_1) \geq \cdots \geq m(i_k)$, where $m(i_j)$ is the multiplicity of i_j in M. The *type* of M is the vector $\lambda(M) = (m(i_1), m(i_2), \ldots, m(i_k))$. For instance, the multiset $M = \{1, 1, 1, 2, 3, 3\}$ has type $\lambda(M) = (3, 2, 1)$. Multisets are in bijection with monomials of R. Given M, we can construct the monomial:

$$\mathbf{x}_M^{\lambda(M)} = \prod_{j=1}^{k} x_{i_j}^{m(i_j)}.$$

Conversely, given a monomial, the associated multiset is the set of indices appearing in it, along with multiplicities. The action of $\mathfrak{S}_\infty$ on monomials coincides with the

Received by the editors September 6, 2006, and, in revised form, October 25, 2007.
2000 *Mathematics Subject Classification.* Primary 13E05, 13E15, 20B30, 06A07.
Key words and phrases. Invariant ideal, symmetric group, Gröbner basis, minimal generators.
The work of the first author was supported under an NSF Postdoctoral Fellowship.

natural action of $\mathfrak{S}_\infty$ on multisets M, and this action preserves the type of a multiset (resp. monomial). We also note the following elementary fact.

Lemma 2. *Let $\sigma \in \mathfrak{S}_\infty$ and $f \in R$. Then there exists a positive integer N and $\tau \in \mathfrak{S}_N$ such that $\tau f = \sigma f$.*

Theorem 1 is a direct corollary of the following result.

Theorem 3. *Let $G = \{g_1, \dots, g_n\}$ be a set of monomials of degree d with distinct types and fix a matrix $C = (c_{ij}) \in K^{n \times n}$ of rank r. Then the submodule $I = \langle f_1, \dots, f_n \rangle_{R[\mathfrak{S}_\infty]} \subseteq R$ generated by the n polynomials, $f_j = \sum_{i=1}^n c_{ij} g_i$ $(j = 1, \dots, n)$, cannot have fewer than r $R[\mathfrak{S}_\infty]$-generators.*

Proof. Suppose that $p_1, \dots, p_k$ are generators for I; we prove that $k \geq r$. Since each $p_l \in I$, it follows that each is a linear combination, over $R[\mathfrak{S}_\infty]$, of monomials in G. Therefore, each monomial occurring in p_l has degree at least d, and, moreover, any degree d monomial in p_l has the same type as one of the monomials in G.

Write each of the monomials in G in the form $g_i = \mathbf{x}_{M_i}^{\lambda_i}$ for multisets $M_1, \dots, M_n$ with corresponding distinct types $\lambda_1, \dots, \lambda_n$, and express each generator p_l as

$$p_l = \sum_{i=1}^n \sum_{\lambda(M) = \lambda_i} u_{ilM} \mathbf{x}_M^{\lambda_i} \; + \; q_l, \tag{1}$$

in which $u_{ilM} \in K$ with only finitely many of them nonzero, each monomial in q_l has degree larger than d, and the inner sum is over multisets M with type λ_i.

Since each polynomial in $\{f_1, \dots, f_n\}$ is a finite linear combination of the p_l, and since only finitely many integers are indices of monomials appearing in $p_1, \dots, p_k$, we may pick N large enough so that all of these linear combinations can be expressed with coefficients in the subring $R[\mathfrak{S}_N]$ (cf. Lemma 2). Therefore, we have

$$f_j = \sum_{l=1}^k \sum_{\sigma \in \mathfrak{S}_N} s_{lj\sigma} \sigma p_l \tag{2}$$

for some polynomials $s_{lj\sigma} \in R$. Substituting (1) into (2) gives us that

$$f_j = \sum_{l=1}^k \sum_{\sigma \in \mathfrak{S}_N} \sum_{i=1}^n \sum_{\lambda(M) = \lambda_i} v_{lj\sigma} u_{ilM} \mathbf{x}_{\sigma M}^{\lambda_i} \; + h_j,$$

in which each monomial appearing in $h_j \in R$ has degree greater than d and $v_{lj\sigma}$ is the constant term of $s_{lj\sigma}$. Since each f_j has degree d, we have that $h_j = 0$. Thus,

$$\sum_{i=1}^n c_{ij} \mathbf{x}_{M_i}^{\lambda_i} = \sum_{l=1}^k \sum_{\sigma \in \mathfrak{S}_N} \sum_{i=1}^n \sum_{\lambda(M) = \lambda_i} v_{lj\sigma} u_{ilM} \mathbf{x}_{\sigma M}^{\lambda_i}.$$

Next, for a fixed i, take the sum on each side in this last equation of the coefficients of monomials with the type λ_i. This produces the n^2 equations

$$c_{ij} = \sum_{l=1}^k \sum_{\sigma \in \mathfrak{S}_N} \sum_{\lambda(M) = \lambda_i} v_{lj\sigma} u_{ilM} = \sum_{l=1}^k \left(\sum_{\lambda(M) = \lambda_i} u_{ilM} \right) \left(\sum_{\sigma \in \mathfrak{S}_N} v_{lj\sigma} \right) = \sum_{l=1}^k U_{il} V_{lj},$$

in which $U_{il} = \sum_{\lambda(M) = \lambda_i} u_{ilM}$ and $V_{lj} = \sum_{\sigma \in \mathfrak{S}_N} v_{lj\sigma}$. Set U to be the $n \times k$ matrix (U_{il}) and similarly let V denote the $k \times n$ matrix (V_{lj}). These n^2 equations are represented by the equation $C = UV$, leading to the following chain of inequalities:

$$r = \operatorname{rank}(C) = \operatorname{rank}(UV) \leq \min\{\operatorname{rank}(U), \operatorname{rank}(V)\} \leq \min\{n, k\} \leq k.$$

Therefore, we have $k \geq r$, and this completes the proof. □

References

[1] M. Aschenbrenner and C. Hillar, *Finite generation of symmetric ideals*, Trans. Amer. Math. Soc. **359** (2007), 5171–5192. MR2327026

[2] M. Drton, B. Sturmfels and S. Sullivant, *Algebraic factor analysis: tetrads, pentads and beyond*, Probability Theory and Related Fields **138** (2007) 463–493. MR2299716

[3] E. Ruch, A. Schönhofer and I. Ugi, *Die Vandermondesche Determinante als Näherungsansatz für eine Chiralitätsbeobachtung, ihre Verwendung in der Stereochemie und zur Berechnung der optischen Aktivität*, Theor. Chim. Acta **7** (1967), 420–432.

[4] J. Schicho, private communication, 2006.

Department of Mathematics, Texas A&M University, College Station, Texas 77843
E-mail address: chillar@math.tamu.edu

Department of Mathematical Sciences, University of Copenhagen, DK-1165 Copenhagen, Denmark
E-mail address: windfeldt@math.ku.dk