

ABSTRACT

Title of Thesis: GRÖBNER BASES WITH APPLICATIONS IN GRAPH THEORY

Degree candidate: Angela M. Hennessy

Degree and year: Master of Arts, 2006

Thesis directed by: Professor Lawrence C. Washington
Department of Mathematics

Gröbner basis theory has been applied to the problem of graph coloring with interesting results. A graph on n vertices is represented by a polynomial in n variables with degree equal to the number of edges in the graph. In the polynomial ring in n variables, the question of k -colorability is equivalent to determining if the polynomial which represents the graph is contained in a specific ideal. By finding a Gröbner basis for this ideal, the problem becomes greatly simplified. We review two different approaches used to solve this problem, and demonstrate the techniques with examples. We also give a new algebraic characterization of the Gröbner basis of a particular ideal when there is a unique k -coloring of a graph.

GRÖBNER BASES WITH APPLICATIONS IN GRAPH THEORY

by

Angela M. Hennessy

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Master of Arts
2006

Advisory Committee:

Professor Lawrence C. Washington, Chairman/Advisor
Professor James A. Schafer
Professor Thomas J. Haines

TABLE OF CONTENTS

1	Introduction	1
2	Gröbner Bases	3
3	Graph Coloring	10
3.1	Examples	16
3.2	Uniquely Colorable Graphs	18
4	Another Approach to Graph Coloring	21
4.1	Bipartite Graphs	23
4.2	Graph Coloring with Roots of Unity	25
4.3	Enumeration of Graph Colorings	27

Chapter 1

Introduction

The theory of Gröbner bases is applied to the problem of graph coloring in [2]. A graph with n vertices is represented by a polynomial in n variables. This polynomial lies in a particular ideal if and only if the graph is k -colorable. Thus, the problem of k -coloring a graph is equivalent to an ideal membership problem. A Gröbner basis is given for this ideal. This method has the advantages that the ideal is identical for any graph on n vertices, and the polynomials in the Gröbner basis are homogeneous. It is also shown in [8] that this Gröbner basis is universal, meaning it is a Gröbner basis under any monomial ordering. The Gröbner basis contains $\binom{n}{k}$ polynomials, and for larger graphs, computations become unwieldy.

In [2], another ideal is described, which has a Gröbner Basis consisting of $n+e$ generators, where e is the number of edges in the graph. The underlying field may be the complex numbers, where the colors are defined to be the k -th roots of unity, or the underlying field may be a finite field. In this approach, however, a different Gröbner basis must be computed for each graph.

In chapter two, we review the theory of Gröbner bases; more information can be found in [3] and [6]. In the third chapter, we review this first method of describing the graph coloring problem via Gröbner bases, and give examples

to demonstrate the theory. We also describe the situation of uniquely colorable graphs, and give an algebraic interpretation of the results. In the fourth chapter, we describe the alternate method, and demonstrate the results when the graph is bipartite.

Chapter 2

Gröbner Bases

Let \mathbb{F} be any field, and let R be the polynomial ring $\mathbb{F}[x_1, \dots, x_n]$. A ring with unity is called *Noetherian* if every ideal contained in it is finitely generated. Hilbert's basis theorem states that if a ring Q is Noetherian, then so is its ring of polynomials $Q[x]$. By induction on n , we can see that the polynomial ring $R = \mathbb{F}[x_1, \dots, x_n]$ is Noetherian. That is, every ideal in R is finitely generated.

In order to define the leading term of a polynomial in more than one variable, we need to specify a monomial ordering. A *monomial ordering* is a well-ordering of monomials from the ring R . This means that the following two conditions are satisfied for all monomials $m_1, m_2, m_3 \in R$.

$$1 \leq m_1 \text{ and } m_1 m_3 \leq m_2 m_3 \text{ whenever } m_1 \leq m_2.$$

The lexicographic, or lex ordering, is defined as follows. Let m_1 and m_2 be any monomials in R . Let the n -tuples $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$ represent the exponents of m_1 and m_2 , respectively. That is, let a_i be the exponent of the variable x_i in m_1 , and let b_i be the exponent of the variable x_i in m_2 . Let c be the n -tuple $c = (a_1 - b_1, \dots, a_n - b_n)$. If position i is the first non-zero value in c , then $m_1 > m_2$ if $c_i > 0$ and $m_1 < m_2$ if $c_i < 0$. For example, under

lex ordering with $x_1 > x_2 > x_3$ we have:

$$x_1^2 > x_1 > x_2^2 > x_2x_3 > x_3.$$

The graded lexicographic, or grlex ordering, uses total degrees. Let m_1, m_2, a and b be defined as before. Then the *total degree* of the monomial m_1 is defined to be $\sum_{i=1}^n a_i$. Under the grlex ordering, monomials are sorted by total degree first, that is, $m_1 > m_2$ if $\sum_{i=1}^n a_i > \sum_{i=1}^n b_i$. Any monomials that have the same total degree are then sorted by the lex ordering. For example, under grlex ordering with $x_1 > x_2 > x_3$ we have:

$$x_1x_2 > x_2^2 > x_2x_3 > x_1.$$

The graded reverse lexicographic, or grevlex ordering, again sorts monomials by total degree. Any monomials with the same total degree are sorted in the reverse of the lex ordering. For example, under grevlex ordering we have:

$$x_2x_3 > x_2^2 > x_1^2 > x_3 > x_1.$$

Given a monomial ordering, we can then define the leading term of a polynomial $f \in R$. We will write $\text{LT}(f)$ for the leading term of f . Additionally, we will write $\text{LM}(f)$ for the leading monomial of f , and $\text{LC}(f)$ for the leading coefficient of the leading term. Therefore, $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$. Let I be an ideal of R . The *leading ideal* of I , written $\langle \text{LM}(I) \rangle$, is defined to be the ideal generated by the leading monomials of all polynomials in I . That is,

$$\langle \text{LM}(I) \rangle = \langle \text{LM}(f) \mid f \in I \rangle.$$

Note that the leading ideal is also generated by the leading terms of all f in I . If the generating set of an ideal consists entirely of monomials, then I is called a *monomial ideal*.

A *Gröbner basis* for an ideal I with respect to a particular monomial ordering is a set $G = \{g_1, \dots, g_m\}$ of polynomials in I whose leading monomials under that ordering generate the leading ideal of I . That is,

$$\langle \text{LM}(I) \rangle = \langle \text{LM}(g_1), \dots, \text{LM}(g_m) \rangle.$$

Under any monomial ordering, it can be shown that every non-zero ideal $I \subset R$ has a Gröbner basis.

Once a monomial ordering is specified, we can divide a polynomial f by an ordered set $G = \{g_1, \dots, g_m\}$. This process is called the *general polynomial division algorithm*, and it proceeds as follows.

1. Set the remainder r and the quotients q_1, \dots, q_m to zero.
2. For $i = 1, 2, \dots, m$ do:
 - 2.1. If $\text{LT}(f)$ is divisible by $\text{LT}(g_i)$ then:
 - 2.1.1. Add $(\text{LT}(f)/\text{LT}(g_i))$ to the quotient q_i .
 - 2.1.2. Replace f by $f - (\text{LT}(f)/\text{LT}(g_i))g_i$.
 - 2.1.3. Set $i = 1$ and return to step 2.
3. If $\text{LT}(f)$ is not divisible by any of $\{\text{LT}(g_1), \dots, \text{LT}(g_m)\}$ then:
 - 3.1 Add $\text{LT}(f)$ to the remainder r .
 - 3.2 Replace f by $f - \text{LT}(f)$.
4. Return to step 2 until f is zero.

Proposition 1. *The general polynomial division algorithm ends in a finite number of steps.*

Proof. Fix a monomial ordering. Using the algorithm above to divide a polynomial $f \in R$ by an ordered set $G = \{g_1, \dots, g_m\}$, initially set the remainder r and

the quotients q_i, \dots, q_m to zero. If the leading term of f is not divisible by any of $\{\text{LT}(g_i), \dots, \text{LT}(g_m)\}$, then $\text{LT}(f)$ is added to the remainder and f is replaced by $f - \text{LT}(f)$. Note that the leading term of $f - \text{LT}(f)$ is strictly less than $\text{LT}(f)$.

Otherwise, at some step in the algorithm $\text{LT}(f)$ is divisible by $\text{LT}(g_i)$, for some i . Then the leading monomial of the polynomial $f - \frac{\text{LT}(f)}{\text{LT}(g_i)}g_i$ is strictly less than the leading monomial of f . Under any monomial ordering, there is a finite number of monomials strictly less than a given monomial. That is, there is no infinite strictly decreasing sequence of monomials in R under any ordering. Since the leading monomial of f is strictly decreasing at each iteration of the algorithm, it must end in a finite number of steps. \square

The next proposition shows that if G is a Gröbner basis for the ideal I , then G is a generating set for that ideal.

Proposition 2. *If $G = \{g_1, \dots, g_m\}$ is a Gröbner basis for the ideal I , then G is also a generating set for the ideal I .*

Proof. For any $f \in I$, using the general polynomial division algorithm, we can write f as

$$f = a_1g_1 + \dots + a_mg_m + r.$$

From step three of the division algorithm, we can see that a term is added to the remainder only when it is not divisible by any leading monomial from G . Therefore, no term in r is divisible by any leading monomial from G . However, since

$$r = f - a_1g_1 - \dots - a_mg_m \in I$$

the leading term of r must be zero. Therefore, f can be written as a linear combination of the elements in G , and G must generate I . \square

The advantage of using Gröbner bases is that, as the next theorem shows, the polynomial division algorithm returns a unique solution.

Theorem 1. *If $G = \{g_1, \dots, g_m\}$ is a Gröbner basis of an ideal I in $R = \mathbb{F}[x_1, \dots, x_n]$ with respect to a particular monomial ordering, then we can write any $f \in R$ as $f = f_1 + r$, where $f_1 \in I$ and no term in r is divisible by any $LM(g_i)$ for $1 \leq i \leq m$. Further, the values f_1 and r are unique.*

Proof. Using the general polynomial division algorithm, we can write f as $f = f_1 + r$, where $f_1 \in I$ and no term in r is divisible by any of $\{LM(g_i) | 1 \leq i \leq m\}$.

Say we can also write f as $f = f'_1 + r'$ where $f'_1 \in I$ and no term in r' is divisible by any of $\{LM(g_i) | 1 \leq i \leq m\}$. Then $r - r' = f'_1 - f_1 \in I$. Since $LM(f'_1 - f_1) \in \langle LM(I) \rangle$ we know $LM(f'_1 - f_1) = LM(r - r') \in \langle LM(I) \rangle$. Therefore the leading monomial of $r - r'$ is divisible by $LM(g_i)$ for some $g_i \in G$. The only possibility is $r - r' = 0$, and therefore $r = r'$ and $f_1 = f'_1$. \square

Some Gröbner bases have further properties that are useful in computations. A *reduced Gröbner basis* of an ideal is a set G of monic polynomials such that for all $g \in G$, no term of g is divisible by any of $\{LM(G - \{g\})\}$. A *universal Gröbner basis* is a Gröbner basis with respect to any monomial ordering. The following theorem gives a set of conditions for a universal Gröbner basis.

Theorem 2. [8] *Let $G = \{g_1, \dots, g_m\}$ be a set of polynomials from R where each g_i is a product of linear factors in the variables x_1, \dots, x_n . Further, assume that*

for any permutation σ on the set $\{1, 2, \dots, n\}$, each polynomial $g_i \in G$ satisfies $g_i(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \in G$. If the set G is a Gröbner basis for the ideal it generates under a particular monomial ordering, then it is a universal Gröbner basis for this ideal.

Proof. We can write each g_i as a product of linear polynomials

$$g_i = \prod_{j=1}^{m_i} (a_{j,1}x_1 + \dots + a_{j,n}x_n + a_{j,n+1}).$$

The leading monomial of g_i is equal to the product of the leading monomials of its linear factors. Under the monomial ordering $x_{i_1} > x_{i_2} > \dots > x_{i_n}$, the leading monomial of the linear polynomial

$$c_1x_{i_1} + c_2x_{i_2} + \dots + c_nx_{i_n} + c_{n+1}$$

is the first variable in the ordering with a non-zero coefficient. Therefore, the leading monomial of each g_i only depends on which constants are non-zero and the ordering of the variables $\{x_1, \dots, x_n\}$.

Without loss of generality, we can assume G is a Gröbner basis under the ordering $x_1 > x_2 > \dots > x_n$. Let $>$ be another ordering which satisfies $x_{i_1} > x_{i_2} > \dots > x_{i_n}$. Let σ be the permutation that sends i_1 to 1, i_2 to 2, and in general sends i_k to k . If we permute the variables in g_i based on σ , the linear factor

$$c_1x_{i_1} + c_2x_{i_2} + \dots + c_nx_{i_n} + c_{n+1}$$

under the ordering $x_{i_1} > \dots > x_{i_n}$ becomes the polynomial

$$c_1x_1 + c_2x_2 + \dots + c_nx_n + c_{n+1}.$$

Since we assumed that G is a Gröbner basis under the ordering $x_1 > \dots > x_n$, the set of all polynomials under this permutation is a Gröbner basis. However, since

each polynomial $g_i \in G$ satisfies $g_i(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \in G$, the set of permuted polynomials is still the set G , so it must also be a Gröbner basis under the ordering $x_{i_1} > x_{i_2} > \dots > x_{i_n}$. Therefore G is a Gröbner basis under any monomial ordering, so it is a universal Gröbner basis. \square

Proposition 3. *For a given monomial ordering, a reduced Gröbner basis for an ideal is unique.*

Proof. Say that G and G' are both reduced Gröbner bases for the ideal I . First, we show that the set of leading monomials of polynomials in G is equal to the set of leading monomials of polynomials in G' . Let m be the monomial that is minimal among the set of monomials in one set but not the other. Without loss of generality, we can assume that m is the leading monomial of some polynomial $g \in G$. Then since the ideals generated by both these sets of leading terms are the same, there is some polynomial $g' \in G'$ where $\text{LM}(g')$ divides $\text{LM}(g)$. There cannot be a polynomial in G with leading monomial $\text{LM}(g')$, since this would not be a reduced Gröbner basis. The monomial $\text{LM}(g')$ is in one set but not the other, but this contradicts the minimality of m . Therefore, the sets of leading monomials of both G and G' are equal. This implies that that the sets have the same cardinality.

For any $g \in G$, we know $\text{LM}(g) = \text{LM}(g')$ for some $g' \in G'$. Let h be the polynomial $h = g - g'$, which is still in I . Since $\text{LM}(g) = \text{LM}(g')$ and both are monic polynomials, these leading terms cancel in h . We also know that none of the remaining terms in h are divisible by any $\text{LM}(G)$ or $\text{LM}(G')$, since this holds for g and g' individually. Therefore, $h = 0$ and $g = g'$ and the reduced Gröbner bases G and G' are equal. \square

Chapter 3

Graph Coloring

Let \mathcal{G} be a graph with n vertices. We will write the vertices of \mathcal{G} as $V = \{v_1, v_2, \dots, v_n\}$, and the set of edges of \mathcal{G} as E . A graph is called *k-colorable* if it is possible to assign one of k values to each vertex such that no two vertices which are adjoined by an edge have the same value. We can think of a k -coloring as a map from the set $\{v_1, v_2, \dots, v_n\}$ to a set of k distinct elements. Any such map f must have the property that for every edge $(v_i, v_j) \in E$, $f(v_i) \neq f(v_j)$.

Let $V_{n,k}$ be the set of n -tuples in \mathbb{F}^n with the property that there are at most k distinct coordinates in the n -tuple. If we think of the k distinct coordinates in an n -tuple as colors, then $V_{n,k}$ is the set of all possible k -colorings of a graph with n vertices. Define the ideal $J_{n,k}$ as follows:

$$J_{n,k} = \left\langle \prod_{1 \leq r < s \leq k+1} (x_{i_r} - x_{i_s}) \mid 1 \leq i_1 < \dots < i_{k+1} \leq n \right\rangle.$$

This generating set is of size $\binom{n}{k+1}$, and each of the polynomials in it is homogeneous of total degree $\frac{k(k+1)}{2}$.

We also define the ideal corresponding to any set $S \subseteq \mathbb{F}^n$ as

$$I(S) = \{f \in R \mid f(a) = 0 \text{ for all } a \in S\}.$$

It is not hard to see that this set of polynomials is indeed an ideal. Similarly, the

variety of an ideal I , written $V(I)$, is defined to be the set of common zeros of all polynomials in the ideal:

$$V(I) = \{(a_1, \dots, a_n) \in \mathbb{F}^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in I\}.$$

The next theorem shows $I(V_{n,k}) = J_{n,k}$, and that the generating set of $J_{n,k}$ is a universal Gröbner basis for this ideal.

Theorem 3. [8],[2] *If the field \mathbb{F} is infinite, the set $G_{n,k}$ is a universal Gröbner basis for the ideal $I(V_{n,k})$, where*

$$G_{n,k} = \left\{ \prod_{1 \leq r < s \leq k+1} (x_{i_r} - x_{i_s}) \mid 1 \leq i_1 < \dots < i_{k+1} \leq n \right\}.$$

Since $J_{n,k}$ is defined as the ideal generated by the set $G_{n,k}$, we have $I(V_{n,k}) = J_{n,k}$.

Proof. First, we show that $J_{n,k} \subseteq I(V_{n,k})$. Since $J_{n,k}$ is generated by the set $G_{n,k}$, it is enough to show $g \in I(V_{n,k})$ for each $g \in G_{n,k}$. For any $g \in G_{n,k}$, g is the graph polynomial of a complete graph on $k+1$ vertices. Since g is the product of all factors of the form $x_{i_r} - x_{i_s}$ on $k+1$ variables, g vanishes on any point which contains a repeated coordinate among these $k+1$ values. Since $V_{n,k}$ is defined to be the set of n -tuples with at most k distinct coordinates, any set of $k+1$ coordinates contains a repeat. Therefore, $g \in I(V_{n,k})$ and $J_{n,k} \subseteq I(V_{n,k})$.

Now, we show that the set $G_{n,k}$, which generates $J_{n,k}$, is a universal Gröbner basis of $I(V_{n,k})$. Since every polynomial in $G_{n,k}$ satisfies the conditions of Theorem 2, it is enough to prove that it is a Gröbner basis for the ideal $I(V_{n,k})$ under the lexicographic ordering with $x_1 > x_2 > \dots > x_n$.

The proof proceeds by double induction on n and k . First, let $k = 1$ and fix a value for n . Then $G_{n,1}$ is the set $\{x_i - x_j \mid 1 \leq i < j \leq n\}$ and the ideal generated

by $\text{LT}(G_{n,k})$ is $\langle x_1, \dots, x_{n-1} \rangle$. We see that $I(V_{n,1})$ contains all polynomials that vanish on all n -tuples where all entries are equal. If $\text{LM}(f)$ contains x_i , where $i < n$, then $\text{LM}(f)$ is contained in the ideal generated by $\text{LT}(G_{n,1})$. If this is not the case, then $\text{LM}(f) = x_n^t$. However, under the lex ordering, this implies that f is a polynomial in x_n alone. Therefore, since f vanishes on any n -tuple (a, a, \dots, a) , where $a \in \mathbb{F}$, and since \mathbb{F} is infinite, we must have $f = 0$. Therefore, $\text{LM}(f)$ is in the ideal generated by $\text{LT}(G_{n,k})$. This completes the case for $k = 1$.

Now we prove the hypothesis for the smallest possible value of n , which is $n = k + 1$. When $n = k + 1$, the set $G_{n,k}$ consists of the single polynomial $g = \prod_{1 \leq i < j \leq k+1} (x_i - x_j)$, and $V_{n,k}$ is the set of all $k + 1$ -tuples with at most k distinct coordinates. Therefore, each $k + 1$ -tuple contains at least one repeat among its coordinates. Since a polynomial $f \in I(V_{n,k})$ must vanish on every one of these $k + 1$ -tuples, it must be divisible by $x_i - x_j$, for every $x_i > x_j$. Consider, for example, $x_2 - x_1$. We can write f as $f = (x_2 - x_1)P + Q$, where P and Q are polynomials and Q does not contain x_1 . Since f vanishes on all tuples that satisfy $x_1 = x_2$, we have $Q = 0$ on all tuples (x_2, \dots, x_n) . Since \mathbb{F} is infinite, Q is identically zero, so $x_2 - x_1$ divides f . Therefore, any $f \in I(V_{n,k})$ must be a multiple of g , and $\text{LM}(f)$ is a multiple of $\text{LM}(g)$. This completes the case for $n = k + 1$.

By induction, we assume the hypothesis is true for $n - 1$ and $k - 1$. Let f be any polynomial in $I(V_{n,k})$. We wish to show that $\text{LM}(f)$ is divisible by $\text{LM}(g)$, for some $g \in G_{n,k}$. Given any set $S \subseteq \{1, \dots, n - 1\}$, we define f_S to be the polynomial obtained by substituting the variable x_n for x_i , for each $i \in S$. We define another polynomial

$$p(f) = \sum_{S \subseteq \{1, \dots, n-1\}} (-1)^{|S|} f_S.$$

We claim that if we substitute x_n for any other variable x_i in the polynomial $p(f)$, the result is the zero polynomial. To see this, we split the summation in $p(f)$ into two summations.

$$p(f) = \sum_{S_1 \subseteq \{1, \dots, i-1, i, i+1, \dots, n-1\}} (-1)^{|S_1|} f_{S_1} + \sum_{S_2 \subseteq \{1, \dots, i-1, i+1, \dots, n-1\}} (-1)^{|S_2|} f_{S_2}$$

The first summation contains all subsets which contain i , and the second summation contains all subsets which do not contain i . The polynomial resulting from the first summation does not contain the variable x_i , since i is in every subset S_1 . Therefore, when we substitute x_n for x_i in $p(f)$, the only changes are in the second summation. For each subset S_2 in the second summation, the set $\{i\} \cup S_2$ is equal to a subset S_1 from the first summation. Since the set S_1 is of size one larger than S_2 , the values $(-1)^{|S_1|}$ and $(-1)^{|S_2|}$ have opposite signs. Therefore, when we substitute x_n for x_i in each of the summands in the second summation, the result will be the negative of one of the summands in the first summation. Therefore, $p(f)$ must be divisible by $x_i - x_n$ for each $i \neq n$ and is of the form $p(f) = (x_1 - x_n) \cdots (x_{n-1} - x_n)h$ where $h \in R$.

We know that f vanishes on every n -tuple with at most k distinct coordinates. If the set S is empty, then $f_S = f$. If S is non-empty, then f_S is a polynomial in at most $n - 1$ variables, and still vanishes on all tuples with at most k distinct coordinates. Therefore, $p(f)$ also vanishes on all tuples with at most k distinct coordinates. If at most $k - 1$ of the values $\{x_1, \dots, x_{n-1}\}$ are distinct, then h is a polynomial in x_n that vanishes for all values of x_n . Since \mathbb{F} is infinite, the coefficients of this polynomial vanish. Therefore, if we expand h as a polynomial in x_n , the coefficients will belong in $G_{n-1, k-1}$. By induction, we can assume the coefficients belong to $I(V_{n-1, k-1})$. It follows that $p(f) \in I(V_{n, k})$. Finally we have $f = p(f) - \sum_{S \neq \emptyset} (-1)^{|S|} f_S \in I(V_{n, k})$, which completes the induction.

Therefore, we have shown that the set $G_{n,k}$ is a universal Gröbner basis for the ideal $I(V_{n,k})$. From Proposition 2, this set also generates the ideal $I(V_{n,k})$. Since by definition, $G_{n,k}$ generates the ideal $J_{n,k}$, we conclude that $J_{n,k} = I(V_{n,k})$. \square

For each graph \mathcal{G} with n vertices, we associate a *graph polynomial* as follows:

$$f_{\mathcal{G}}(x_1, x_2, \dots, x_n) = \prod_{i < j, (x_i, x_j) \in E} (x_i - x_j).$$

Each possible k -coloring of the graph corresponds to an n -tuple in \mathbb{F}^n which has at most k distinct coordinates. The value in position i of the n -tuple corresponds to the color assigned to vertex v_i .

Notice that each polynomial in the generating set for $J_{n,k}$ is the graph polynomial of a complete graph on $k+1$ vertices. The following propositions describe the relationship between a graph polynomial and the ideal $J_{n,k}$.

Proposition 4. *The graph polynomial $f_{\mathcal{G}}$ has a zero at an n -tuple in $V_{n,k}$ if and only if the n -tuple does not correspond to a valid k -coloring of the graph \mathcal{G} .*

Proof. We defined $V_{n,k}$ to be the set of all n -tuples in \mathbb{F}^n with at most k distinct coordinates. This is the set of all possible k -colorings of the graph. Let (a_1, a_2, \dots, a_n) be an n -tuple in $V_{n,k}$. By associating the value a_i to the vertex v_i , this n -tuple corresponds to a valid graph coloring if and only if $a_i \neq a_j$ for each edge $(x_i, x_j) \in E$. This means the n -tuple is a valid graph coloring if and only if $x_i - x_j \neq 0$ for each edge $(x_i, x_j) \in E$ when it is evaluated at the point (a_1, a_2, \dots, a_n) . This is equivalent to the statement that a zero of the graph polynomial corresponds to a non-valid k -coloring of the graph. \square

Proposition 5. *A graph \mathcal{G} with n vertices is not k -colorable if and only if its graph polynomial $f_{\mathcal{G}}$ belongs to the ideal $J_{n,k}$.*

Proof. From the previous proposition, we know that the graph polynomial has a zero precisely at points in $V_{n,k}$ that correspond to non-valid k -colorings of the graph. From Theorem 3, $J_{n,k} = I(V_{n,k})$. This means the ideal $J_{n,k}$ consists of polynomials that vanish on $V_{n,k}$. Therefore, the graph \mathcal{G} is not k -colorable if and only if the graph polynomial $f_{\mathcal{G}}$ belongs to the ideal $J_{n,k}$. \square

In summary, to determine if a given graph \mathcal{G} with n vertices is k -colorable, we compute its graph polynomial $f_{\mathcal{G}} = \prod_{i < j, (x_i, x_j) \in E} (x_i - x_j)$. We also compute the set of graph polynomials of complete graphs on $k + 1$ of the n vertices, call this set G . This set G generates and is a Gröbner basis for the ideal $J_{n,k}$, which is the ideal corresponding to the set of possible k -colorings of the graph. Using the general polynomial division algorithm, we divide the graph polynomial $f_{\mathcal{G}}$ by the set G , and the graph \mathcal{G} is not k -colorable if and only if the remainder is zero.

We showed that the remainder upon division by a Gröbner basis G is unique and none of the terms is divisible by the leading term of any $g \in G$. Therefore, the remainders are in a one-to-one correspondence with cosets in the quotient R/I . If a point in $V_{n,k}$ is a zero of the graph polynomial, then it corresponds to an invalid coloring of the graph. Therefore, the points in $V_{n,k}$ that correspond to valid graph colorings are exactly the points in $V_{n,k}$ that are not zeros of $f_{\mathcal{G}}$.

An operation on two ideals I and J is called the *colon ideal*, written $I : J$, and defined as follows:

$$I : J = \{f \in R \mid fJ \subseteq I\}.$$

If V and W are two varieties, then the colon ideal of their respective ideals corresponds to their set difference. That is,

$$I(V) : I(W) = \{f \in R \mid fI(W) \subseteq I(V)\} = I(V - W).$$

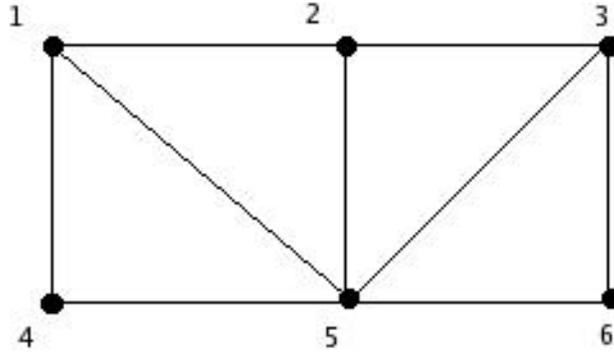


Figure 3.1: Example 1.

Therefore, we can write the valid k -colorings of the graph \mathcal{G} as the variety corresponding to the ideal $J_{n,k} : \langle f_{\mathcal{G}} \rangle$. If there are no multiple edges in the graph \mathcal{G} , then $f_{\mathcal{G}}$ can be written as a product of distinct irreducible factors, and $\langle f_{\mathcal{G}} \rangle$ is the ideal corresponding to the variety consisting of zeros of $f_{\mathcal{G}}$. That is, $\langle f_{\mathcal{G}} \rangle$ is a radical ideal.

3.1 Examples

Example 1. Let \mathcal{G}_1 be the graph on six vertices and nine edges shown in Figure 3.1. Let $\mathbb{F} = \mathbb{Q}$ be the rationals, and $R = \mathbb{Q}[x_1, \dots, x_6]$ under lexicographic ordering. The graph polynomial $f_{\mathcal{G}_1}$ is a homogeneous polynomial of total degree nine and leading term $x_1^3 x_2^2 x_3^2 x_4 x_5$. To determine if \mathcal{G}_1 is 3-colorable, we compute

the Gröbner basis for the ideal $J_{6,3}$ as follows.

$$G_{6,3} = \left\{ \prod_{1 \leq r < s \leq 4} (x_{i_r} - x_{i_s}) \mid 1 \leq i_1 < \dots < i_4 \leq 6 \right\}$$

There are $\binom{6}{4} = 15$ polynomials in this basis.

Using the computer program Magma, we can compute the ideal $J_{n,k}$ and verify that $f_{\mathcal{G}}$ is not contained in $J_{n,k}$. Therefore, the graph is 3-colorable, which can be verified by inspection. Using Magma, we can also find a reduced Gröbner basis for the colon ideal $J_{n,k} : \langle f_{\mathcal{G}} \rangle$. This reduced Gröbner basis is:

$$\{x_1 - x_3, x_2 - x_6, x_4 - x_6\}.$$

Since the variety corresponding to this basis is the set of valid colorings, we can see that there is only one valid 3-coloring of this graph, and it is described by these equations.

Example 2. Let \mathcal{G}_2 be the graph with six vertices and ten edges shown in Figure 2. Again we calculate the graph polynomial $f_{\mathcal{G}_2}$ and the Gröbner basis $G_{6,3}$ under lexicographic ordering. We calculate the remainder of $f_{\mathcal{G}_2}$ modulo $G_{6,3}$ to be zero, so $f_{\mathcal{G}_2} \in J_{6,3}$ and the graph is not 3-colorable. This can be verified by inspection. The graph is 4-colorable, however, which is verified by the computation $f_{\mathcal{G}_2} \notin J_{6,4}$. We find a reduced Gröbner basis for the colon ideal $J_{n,k} : \langle f_{\mathcal{G}_2} \rangle$

$$\langle (x_2 - x_6)(x_1 - x_3 + x_4 - x_6), (x_3 - x_4)(x_1 - x_3), (x_4 - x_6)(x_3 - x_4)(x_2 - x_6) \rangle.$$

One possible coloring of the graph is $(1, 2, 1, 3, 4, 2)$.

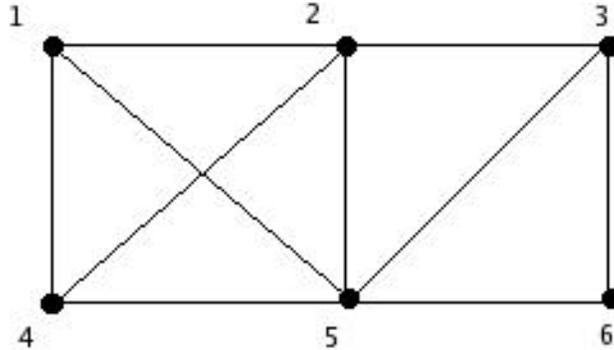


Figure 3.2: Example 2.

3.2 Uniquely Colorable Graphs

These examples suggest a correspondence between the reduced Gröbner basis of the colon ideal $J_{n,k} : \langle f_{\mathcal{G}_2} \rangle$ and the valid k -colorings of the graph. The following theorem, which is our main result, states when there is a unique coloring of the graph. Colorings are considered distinct if they induce different partitions of the set of vertices based on the color assigned.

Theorem 4. *Let \mathcal{G} be a graph on n vertices with graph polynomial $f_{\mathcal{G}}$. There exists a unique k -coloring of the graph which uses all k colors if and only if a reduced Gröbner basis (under any monomial ordering) of the colon ideal $(J_{n,k} : \langle f_{\mathcal{G}} \rangle)$ consists of $n - k$ polynomials of the form $(x_i - x_j)$.*

Proof. First, we assume that a reduced Gröbner basis of the colon ideal $(J_{n,k} :$

$\langle f_{\mathcal{G}} \rangle$) contains $n - k$ polynomials of the form $(x_i - x_j)$. We will prove that there exists a unique k -coloring of the graph \mathcal{G} .

Recall that the points that represent valid k -colorings of a graph are exactly the points in the variety of the colon ideal $(J_{n,k} : \langle f_{\mathcal{G}} \rangle)$. If $x_i - x_j$, where $x_i > x_j$ is a polynomial in the reduced Gröbner basis, then there cannot be any other polynomials in it with leading term x_i .

We can think of each of the polynomials as a row of an $n - k$ by n matrix, where the values in each row are the coefficients of the n variables. Permuting these rows yields the row echelon form, since the basis is reduced. A solution to these equations corresponds to a valid k -coloring. Since there are k free variables, these values determine the other values in the coloring. Since these k values must all be different, there is only one valid coloring which uses all k colors.

Now we assume that there is a unique valid coloring for the graph \mathcal{G} that uses all k colors, and we wish to show that the colon ideal $(J_{n,k} : \langle f_{\mathcal{G}} \rangle)$ has a reduced Gröbner basis consisting of $n - k$ polynomials of the form $x_i - x_j$ under a particular monomial ordering. We will call vertices that are assigned the same color to be in the same *color class*. Since there is a unique k -coloring of the graph \mathcal{G} , there are k color classes, call them C_1, C_2, \dots, C_k . We know that none of these sets are empty.

Let the vertices x_i and x_j be in different color classes. Then any coloring which assigns the same color to x_i and x_j is an invalid coloring. That is, if $x_i = x_j$, then we have a bad coloring. Since all invalid colorings are zeros of the graph polynomial $f_{\mathcal{G}}$, we see that the polynomial $(x_i - x_j)$ must divide $f_{\mathcal{G}}$.

Since $n > k$, one of the color classes contains more than one vertex. Say C_k contains the values x_i and x_j , and $x_i > x_j$ under our monomial ordering. Then

since there is only one valid coloring, any n -tuple which represents this coloring must satisfy $x_i = x_j$. This means the polynomial $x_i - x_j$ does not divide the graph polynomial. We wish to show that this polynomial is in the colon ideal. That is, we wish to show that $(x_i - x_j)f_{\mathcal{G}} \in J_{n,k}$. We know that the color classes C_1, \dots, C_{k-1} are non-empty, so let $x_{i_1} \in C_1, \dots, x_{i_{k-1}} \in C_{k-1}$. Since they are in different color classes, the polynomials $(x_{i_1} - x_j), \dots, (x_{i_{k-1}} - x_j)$ divide $f_{\mathcal{G}}$. By the same argument, the polynomials $(x_{i_1} - x_i), \dots, (x_{i_{k-1}} - x_i)$ and $(x_{i_r} - x_{i_s})$ for $1 \leq r < s \leq k - 1$ also divide $f_{\mathcal{G}}$. The product of all these linear factors (including $(x_i - x_j)$) is a complete graph polynomial on $k + 1$ vertices, which is in the ideal $J_{n,k}$. Therefore, the polynomial $x_i - x_j$ is in the colon ideal.

We have shown that for any values x_i and x_j in the same color class, the polynomial $(x_i - x_j)$ is in the colon ideal. Since there are k color classes, there are $n - k$ such pairs of values in the same class, and therefore $n - k$ such polynomials in the colon ideal. This completes the second direction of the proof. \square

Chapter 4

Another Approach to Graph Coloring

Another method of determining graph colorability is described in [1] and [6]. Any set S of k distinct elements from the field \mathbb{F} can be the possible k colors assigned to the vertices. Call $U_{n,k}$ the set of n -tuples that represent possible colorings, which is of size k^n . Colorings are considered distinct if they form different partitions on the set of vertices. Therefore, there are $k!$ n -tuples that represent the same coloring if all k colors are used.

Given the set S of possible colors, we define a polynomial $g(x)$:

$$g(x) = \prod_{\alpha \in S} (x - \alpha).$$

Let G be the set of polynomials obtained by substituting each variable x_i for x , $G = \{g(x_i) | 1 \leq i \leq n\}$, and let $I_{n,k}$ be the ideal generated by these polynomials. The following proposition relates the possible colorings of the graph \mathcal{G} to the ideal $I_{n,k}$.

Proposition 6. [8] *Let $g(x)$ be of the form $g(x) = \prod_{\alpha \in S} (x - \alpha)$ as above. Then the set $G = \{g(x_i) | 1 \leq i \leq n\}$ is a universal Gröbner basis for the ideal it generates. A graph \mathcal{G} with n vertices is not k -colorable if and only if its graph polynomial $f_{\mathcal{G}}$ belongs to the ideal $I_{n,k}$ generated by the set G .*

Proof. Since the polynomials in the set G are each in a different variable, the leading terms of these polynomials must be relatively prime with respect to any monomial ordering. We will make use of a result known as Buchberger's First Criterion, which states that if the leading terms in a set of polynomials are pairwise relatively prime under a particular monomial ordering, then the set is a Gröbner basis for the ideal it generates. Since every polynomial in the set G also satisfies the conditions of Theorem 2, G is a universal Gröbner basis.

The possible k -colorings of the graph \mathcal{G} are n -tuples (a_1, a_2, \dots, a_n) , where $g(a_i) = 0$ for $1 \leq i \leq n$. The graph \mathcal{G} is not k -colorable if and only if each possible k -coloring is a zero of the graph polynomial $f_{\mathcal{G}}$. Therefore, the graph is not k -colorable if and only if the graph polynomial is in the radical of $I_{n,k}$. Since $I_{n,k}$ is shown to be a radical ideal in Proposition 16, the graph is not k -colorable if and only if the graph polynomial is in $I_{n,k}$. \square

Therefore, another method of determining if a graph is k -colorable is to see if the graph polynomial lies in the ideal $I_{n,k}$. While this tells us if the graph is k -colorable or not, it does not give an actual coloring. Recall that $U_{n,k}$ is the set of n -tuples that represent possible k -colorings of the graph, and each coordinate of the n -tuple must be a root of the polynomial g . We define the polynomial h as follows.

$$h(x_i, x_j) = \frac{g(x_i) - g(x_j)}{x_i - x_j} = g'(x_j) + \frac{x_i - x_j}{2} g''(x_j) + \dots$$

Let the n -tuple $a = (a_1, a_2, \dots, a_n)$ be a solution of the following set of equations.

$$g(x_i) = 0, \text{ for } 1 \leq i \leq n$$

$$h(x_i, x_j) = 0 \text{ for } (x_i, x_j) \in E$$

The condition $g(x_i) = 0$ for $1 \leq i \leq n$ requires each vertex be assigned a valid color a_i from the set S . The condition $h(x_i, x_j) = 0$ for each edge (x_i, x_j) requires $a_i \neq a_j$, and since g has no multiple roots, $g'(a) \neq 0$ for all $a \in S$, which implies that $h(a, a) \neq 0$ for all $a \in S$. So finding a valid k -coloring of the graph \mathcal{G} is equivalent to solving this set of equations.

4.1 Bipartite Graphs

In this section we assume \mathbb{F} has characteristic $p \neq 0$. For example, if \mathbb{F} has exactly p elements, where p is prime and $p = k$, then we compute the polynomials $g(x_i)$ and $h(x_i, x_j)$ as follows.

$$g(x_i) = x_i^p - x_i$$

$$h(x_i, x_j) = (x_i - x_j)^{p-1} - 1$$

This last equality follows from the fact that the binomial coefficients $\binom{p}{i}$ are divisible by p , when $1 \leq i \leq p - 1$.

For example, to determine if a graph is 2-colorable, or bipartite, we let \mathbb{F} be the field of order 2, and compute the polynomials as follows.

$$g(x_i) = x_i^2 - x_i$$

$$h(x_i, x_j) = x_i + x_j + 1$$

To determine if the graph is bipartite, we look for a solution to the equations $h(x_i, x_j) = 0$. This is a solution to the equations $x_i + x_j = 1$ for each edge (x_i, x_j) .

Example 3. Let \mathcal{G}_3 be the bipartite graph in shown in Figure 3.

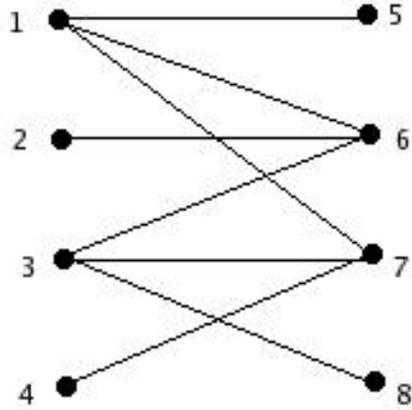


Figure 4.1: Example 3.

We compute the equations $h(x_i, x_j)$ as follows.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

A solution to these equations is

$$x_1 = x_2 = x_3 = x_4 = 1, x_5 = x_6 = x_7 = x_8 = 0.$$

Therefore, determining if a graph is bipartite is equivalent to solving a system

of linear equations, where the number of equations is equal to the number of edges in the graph. A solution to this system of equations reveals the partition of vertices into the two color classes, and if the system has no solution, then the graph is not bipartite.

4.2 Graph Coloring with Roots of Unity

We let $\mathbb{F} = \mathbb{C}$ be the complex numbers, and let the set S of possible colors be the k -th roots of unity. Then the polynomials g and h are as follows.

$$g(x_i) = x_i^k - 1$$

$$h(x_i, x_j) = x_i^{k-1} + x_i^{k-2}x_j + \dots + x_ix_j^{k-2} + x_j^{k-1}$$

This last equality follows since

$$x_i^k - 1 - (x_j^k - 1) = (x_i - x_j)(x_i^{k-1} + x_i^{k-2}x_j + \dots + x_ix_j^{k-2} + x_j^{k-1})$$

Again we let $I_{n,k}$ be the ideal generated by the polynomials $\{g(x_i) | 1 \leq i \leq n\}$.

We also define the ideal $I_{\mathcal{G},k}$ via

$$I_{\mathcal{G},k} = I_{n,k} + \langle x_i^{k-1} + x_i^{k-2}x_j + \dots + x_ix_j^{k-2} + x_j^{k-1} | (x_i, x_j) \in E \rangle.$$

Recall that the variety of an ideal I is the set of zeros common to all polynomials in I . The following proposition describes the varieties of the ideals $I_{n,k}$, $I_{\mathcal{G},k}$ and $I_{n,k} + \langle f_{\mathcal{G}} \rangle$.

Proposition 7. [7] *The points in the varieties $V(I_{n,k})$, $V(I_{\mathcal{G},k})$ and $V(I_{n,k} + \langle f_{\mathcal{G}} \rangle)$ are in bijection with all possible k -colorings, all the valid k -colorings, and all the invalid k -colorings of the graph \mathcal{G} on n vertices.*

Proof. The common roots of the polynomials $x_i^k - 1$ consist of all n -tuples whose coordinates are k -th roots of unity. These correspond to all possible k -colorings, where the possible colors are the k -th roots of unity. The common roots of all polynomials in $I_{\mathcal{G},k}$ must be common roots of all polynomials in $I_{n,k}$ and of the polynomial $x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1}$ for each edge (x_i, x_j) . But these are just the roots of the polynomials $g(x_i)$ and $h(x_i, x_j)$ from the previous section, so these correspond to the valid k -colorings of the graph. We already determined that n -tuples that are roots of the graph polynomial $f_{\mathcal{G}}$ are invalid k -colorings, so these are in the last variety. \square

The weak Nullstellensatz states that in an algebraically closed field, if the variety of an ideal $V(I)$ is the empty set, then I is not a proper ideal. Therefore, we can state the k -colorability of \mathcal{G} in terms of the ideal $I_{\mathcal{G},k}$.

Proposition 8. *The graph \mathcal{G} is not k -colorable if and only if the polynomial 1 is in the ideal $I_{\mathcal{G},k}$.*

Proof. It was shown in the previous proposition that the variety $V(I_{\mathcal{G},k})$ contains all valid k -colorings of the graph \mathcal{G} . Therefore \mathcal{G} is not k -colorable if and only if the variety $V(I_{\mathcal{G},k})$ is empty, which happens if and only if $I_{\mathcal{G},k}$ is not a proper ideal (and therefore contains the unit 1). \square

For example, to determine if a graph \mathcal{G} with n vertices is 3-colorable (as described in [1]) we compute the graph polynomial $f_{\mathcal{G}}$ and the following ideals:

$$I_{n,k} = \langle x_i^3 - 1 \mid 1 \leq i \leq n \rangle,$$

$$I_{\mathcal{G},k} = I_{n,k} + \langle x_i^2 + x_i x_j + x_j^2 \mid (x_i, x_j) \in E \rangle.$$

The graph is 3-colorable if and only if f_G is not in the ideal $I_{n,k}$ or, equivalently, if 1 is not in the ideal $I_{G,k}$. To find a 3-coloring, we need to find a point in the variety $V(I_{G,k})$.

4.3 Enumeration of Graph Colorings

Since the remainder upon division by a Gröbner basis is a linear combination of monomials not in $\langle \text{LM}(I) \rangle$, a basis for R/I is the set of monomials not in the leading ideal of I . An ideal I is called *zero-dimensional* if this basis is finite. The following theorem describes varieties that correspond to zero-dimensional ideals when the underlying field is \mathbb{C} .

Theorem 5. *Let I be an ideal of \mathbb{C}^n . Its corresponding affine variety $V = V(I)$ is finite if and only if $\mathbb{C}[x_1, \dots, x_n]/I$ is a finite-dimensional vector space over \mathbb{C} .*

Proof. First, suppose the variety $V(I)$ corresponding to the ideal I is finite. If $I = R$, then we are done. Otherwise I is a proper ideal, and by the weak Nullstellensatz, $V(I)$ is not the empty set. Let $\{a_{i_1}, a_{i_2}, \dots, a_{i_{m_i}}\}$ (for $i = 1, 2, \dots, n$) be the set of distinct values from \mathbb{C} that appear in the i th coordinate of any n -tuple in V . Also for each i in $1, 2, \dots, n$, define a polynomial f_i in variable x_i as follows.

$$f_i(x_i) = \prod_{j=1}^{m_i} (x_i - a_{i_j})$$

Each polynomial f_i vanishes on every point in $V(I)$, so each f_i must belong to $I(V(I))$. By the Nullstellensatz, $I(V(I)) = \sqrt{I}$, so there exists some positive integer r_i such that $f_i^{r_i} \in I$. Under any monomial ordering, the leading term

of $f_i^{r_i}$ is $x_i^{m_i r_i}$. Since $f_i^{r_i} \in I$, we know that $\text{LT}(f_i^{r_i}) = x_i^{m_i r_i}$ is in the leading ideal of I . Therefore, for each variable x_i , there is some integer $a_i \geq 1$ such that $x_i^{a_i}$ is in the leading ideal of I . A generic monomial in $\mathbb{C}[x_1, \dots, x_n]$ is of the form $x_1^{b_1} \cdots x_n^{b_n}$. We can see that there is only a finite number of monomials in $\mathbb{C}[x_1, \dots, x_n]$ that are not divisible by some monomial in the leading ideal of I . Since the monomials not in the leading ideal of I span the vector space $\mathbb{C}[x_1, \dots, x_n]/I$, we can see that this vector space is of finite dimension.

Now suppose that $\mathbb{C}[x_1, \dots, x_n]/I$ is a finite-dimensional vector space over \mathbb{C} . We wish to show that the variety $V(I)$ is finite. We will show that for $i = 1, \dots, n$, there is only a finite number of distinct complex values that may appear in the i th coordinate for any n -tuple in $V(I)$. For a fixed value of i , the cosets $x_i^0, x_i^1, x_i^2, \dots$ in $\mathbb{C}[x_1, \dots, x_n]/I$ must eventually be linearly dependent, since $\mathbb{C}[x_1, \dots, x_n]/I$ is a finite-dimensional vector space. This means there exist complex values c_j (not all zero) such that $\sum_{j=0}^s c_j x_i^j = 0$ in $\mathbb{C}[x_1, \dots, x_n]/I$. Therefore, this polynomial is in I . Since the polynomial can only have a finite number of roots, there is only a finite number of distinct values that appear in the i th coordinate of points in $V(I)$. Therefore, $V(I)$ is finite. \square

Using this theorem, we can describe the size of a variety corresponding to a zero-dimensional ideal, and use this to determine if the ideal is radical.

Theorem 6. *Let I be a zero-dimensional ideal in $\mathbb{C}[x_1, \dots, x_n]$. Then the dimension of the \mathbb{C} -vector space $\mathbb{C}[x_1, \dots, x_n]/I$ is greater than or equal to the size of the variety $V(I)$. Further, these values are equal if and only if I is a radical ideal.*

Proof. Let I be a zero-dimensional ideal. This means that the dimension of

$\mathbb{C}[x_1, \dots, x_n]/I$ is finite. From the previous theorem, $V(I)$ is a finite set in \mathbb{C}^n , say $V(I) = \{p_1, \dots, p_m\}$. Define a map $\phi : \mathbb{C}[x_1, \dots, x_n]/I \rightarrow \mathbb{C}^m$ by $\phi(f) = (f(p_1), \dots, f(p_m))$. This map evaluates a polynomial at each of the points in $V(I)$. It is clear that ϕ is well defined, and is linear since $\phi((f+g)(x)) = \phi(f(x)+g(x)) = \phi(f) + \phi(g)$. In fact, ϕ is a ring homomorphism, since $\phi(fg) = \phi(f)\phi(g)$. Now we show that ϕ is onto. For $i = 1, \dots, m$, choose g_i as follows:

$$g_i(p_j) = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j. \end{cases}$$

Specifically, the polynomial g_i is defined to be:

$$g_i(x) = \frac{1}{m-1} \sum_{j \neq i} \prod_{p_j^{(k)} \neq p_i^{(k)}} \frac{(x - p_j^{(k)})}{(p_i^{(k)} - p_j^{(k)})}.$$

Let $(a_1, \dots, a_m) \in \mathbb{C}^m$ and $f = a_1g_1 + a_2g_2 + \dots + a_mg_m$. Then we have:

$$\phi(f) = \phi(a_1g_1) + \dots + \phi(a_mg_m) = (a_1, \dots, a_m).$$

Therefore ϕ is onto the m -dimensional space \mathbb{C}^m . This proves that the dimension of $\mathbb{C}[x_1, \dots, x_n]/I$ is no smaller than m .

Now we show that the dimensions are equal if and only if I is a radical ideal. We will do this by proving the map ϕ is an isomorphism if and only if I is radical. First say I is a radical ideal, and let f be in the kernel of ϕ . This means that f vanishes on every point in $V(I)$, and is therefore in $I(V(I))$. By the Nullstellensatz, $I(V(I)) = \sqrt{I}$. Since I is radical, $\sqrt{I} = I$, and f is therefore in I . This means that f is in the zero coset of $\mathbb{C}[x_1, \dots, x_n]/I$, so the map ϕ has the trivial kernel and ϕ is therefore one-to-one. This shows that ϕ is an isomorphism of vector spaces, so they must be of the same dimension. Now say that the dimension of $\mathbb{C}[x_1, \dots, x_n]/I$ is equal to m , the size of $V(I)$. Then ϕ

must be an isomorphism, since it is an onto map of vector spaces, so ϕ must be one-to-one. Now we show that I is radical. The inclusion $I \subset \sqrt{I}$ follows by definition. Let $f \in \sqrt{I} = I(V(I))$ (by the Nullstellensatz). Then each $p_i \in V(I)$ is a zero of f , and $\phi(p_i)$ is the zero point in \mathbb{C}^m . Since ϕ is one-to-one, f must be in the zero coset of $\mathbb{C}[x_1, \dots, x_n]/I$, so $f \in I$. Therefore, $\sqrt{I} \subset I$ and I is a radical ideal. \square

We showed the bijection between the varieties of the ideals $I_{n,k}$, $I_{\mathcal{G},k}$ and $I_{n,k} + \langle f_{\mathcal{G}} \rangle$ and the set of all, the set of valid, and the set of invalid k -colorings of the graph \mathcal{G} . As a consequence of the last theorem, we can see that the ideal $I_{n,k}$ is radical. Further, we can verify the following based on the set differences of valid and invalid colorings.

$$I_{n,k} : I_{\mathcal{G},k} = I_{n,k} + \langle f_{\mathcal{G}} \rangle .$$

Using the previous theorem, we can see that there are $\dim_{\mathbb{F}}(R/I_{\mathcal{G},k})$ valid graph colorings, where two colorings are considered distinct if they induce different partitions on the set of vertices based on the color assigned.

BIBLIOGRAPHY

- [1] W. Adams, Minicourse in Gröbner Bases at University of Maryland, March 2005.
- [2] N. Alon and M. Tarsi, “Colorings and Orientations of Graphs,” *Combinatorica* 12 (1992), 125-134.
- [3] D. Cox, J. Little and D. O’Shea, *Ideals, Varieties and Algorithms*, Springer Undergraduate texts in Mathematics, Springer-Verlag, New York, 1992.
- [4] D. Cox, J. Little and D. O’Shea, *Using Algebraic Geometry*, Springer-Verlag, New York, 1998.
- [5] M. Domokos, “Gröbner Bases of Certain Determinantal Ideals,” *Contributions to Algebra and Geometry* Vol. 40 (1999), No. 2, p. 479-493.
- [6] D. Dummit and R. Foote, *Abstract Algebra*, Third Edition, John Wiley & Sons, Inc., 2004.
- [7] C. Hillar and T. Windfeldt, “An Algebraic Characterization of Uniquely Vertex Colorable Graphs,” June 22, 2006, available at: <http://arxiv.org/abs/math/0606565>.
- [8] J. A. de Loera, “Gröbner Bases and Graph Colorings,” *Contributions to Algebra and Geometry*, Vol. 36 (1995), No. 1, p. 89-96.

- [9] L. Lovász, “Stable Sets and Polynomials,” *Discrete Mathematics* 124 (1994), p. 137-153.