GROEBNER BASIS APPROACH IN GRAPH-THEORETICAL PROBLEMS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
MASTER OF SCIENCE
IN
MATHEMATICS

By
Onur Muharrem Örün
June 2016

GROEBNER BASIS APPROACH IN GRAPH-THEORETICAL PROBLEMS

By Onur Muharrem Örün

June 2016

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Müfit Sezer(Advisor)

Özgün Ünlü

Mesut Şahin

Approved for the Graduate School of Engineering and Science:

Levent Onural
Director of the Graduate School

ABSTRACT

GROEBNER BASIS APPROACH IN GRAPH-THEORETICAL PROBLEMS

Onur Muharrem Örün
M.S. in Mathematics
Advisor: Müfit Sezer
June 2016

In the study of graphs, it is often desirable to know about the colorability properties of a given graph or whether it is planar or if it contains a Hamiltonian cycle. We consider such problems and describe corresponding encodings to equate these problems to problems of solving systems of polynomial equations. This in turn reduces the problem to computing lead term ideals from a certain generating set using Groebner basis theory.

Keywords: Groebner basis, Hilbert's Nullstellensatz, Graph colorability, Hamiltonian cycle, Planar graph, Edge-chromatic number.

ÖZET

ÇİZGE KURAMSAL PROBLEMLERDE GROEBNER BAZ YAKLAŞIMI

Onur Muharrem Örün
Matematik, Yüksek Lisans
Tez Danışmanı: Müfit Sezer
Haziran 2016

Çizgeler kuramında, verili bir çizgenin renklendirilebilme özellikleri, düzlemsel olup olmadığı, Hamiltonyan bir döngü içerip içermediği gibi özellikler o çizgenin başat özellikleri arasındadır. Bu tür problemlerin çeşitli kodlamalarla bir polinom sisteminin çözümünü elde etme problemlerine dönüştürülebileceğinden söz edeceğiz. Bu polinom sistemlerine Groebner bazları tekniklerini uygulayıp problemimizin kodlamaların verdiği üretici bir kümeden başat terim ideali hesaplanmasına indirgenebileceğini ortaya koyacağız.

Anahtar sözcükler: Groebner baz, Hilbert Nullstellensatz, Çizge renklendirme, Hamiltonyan döngü, Düzlemsel çizge, Kenar kromatik sayısı.

Acknowledgement

I would like to express my deepest gratitude to my advisor Assoc. Prof. Dr. Müfit Sezer. Without his indispensable support and guidance this thesis would not have been possible.

I would also like to thank to Asst. Prof. Dr. Özgün Ünlü and Assoc. Prof. Dr. Mesut Şahin for their time in reviewing our work and agreeing to serve as committee members at my thesis defense.

I am eternally grateful to my mom Ayten, dad Önder, brother Anıl, and uncle Tuncay for their unconditional love, support, and encouragement.

Last but not least, thanks to all my friends, in particular, Hatice, Cemile, Berrin, Kemal, Mehmet, Mustafa, Gökçen, Cihan, and Akif for making the time I spent in Ankara forever memorable.

Contents

Chapter 1

Introduction

In this study, we consider some basic questions that arise naturally in graph theory. For instance, for a given graph G, it is of interest to decide if G is Hamiltonian or to find the smallest integer k such that G is k-colorable. We describe how such problems can be transformed into problems of solving polynomial equations using the relevant encodings. Then this problem reduces to computing the lead term ideal of the ideal generated by the polynomials that arise in the encodings.

In Chapter two we review preliminary results from commutative algebra. We revisit Hilbert's basis theorem that states every ideal in a polynomial ring with finitely many variables over a field is finitely generated. Then we introduce monomial orders and go over their basic properties. We also define and verify the existence of Groebner basis. Then we demonstrate the uniqueness of the reduced Groebner basis.

In Chapter three we reproduce a proof of Hilbert's Nullstellensatz. This theorem lies in the center of our approach to the graph theoretic questions. We also include Noether's normalization lemma and talk about some results about "Nullstellensatz Certificate". This certificate provides degrees of the coefficients of the generators in the identity that gives one in the ideal. Furthermore, we prove some results on generation of an ideal up to radical, and the size of the

variety of a zero-dimensional ideal. These results are more on the technical side and are required for the number of solutions of the encodings that we introduce in the following chapter.

In Chapter four we introduce the graph theoretical questions of our interest. The first one is the graph colorability problem: For a given graph G, we want to determine the smallest number k such that the vertices of G can be colored in such a way that no two adjacent vertices have the same color. Secondly, we want to check if G is Hamiltonian, i.e., if there is a cycle in G that visits every vertex exactly once. Also we want to check if the graph G is planar, that is if G can be drawn on a plane with no edges intersecting with each other. Otherwise we determine if G has a planar subgraph with a fixed number of edges. In the last encoding, we want to determine the edge-chromatic number of the graph G which is the smallest number of colors needed to color all the edges of G with no edges incident on the same vertex have the same color. For each of these problems we reproduce the corresponding encoding that is we describe a generating set for an ideal such that the problem has an affirmative answer if and only if the ideal being proper in the polynomial ring.

Groebner bases methods are very useful to determine whether a system of polynomial equations has a solution. In the final chapter, we apply these methods to study some explicit cases. For some classes of examples we compute the reduced Groebner basis for some problems introduced in the previous chapter. The properness of the ideal of the encoding can be just checked from the generating set of the lead term ideal. The software system CoCoA is used to work out these examples. For the cases where the colorability and Hamiltonian cycle problems have positive answers, we also compute the number of colorings and the number of Hamiltonian cycles.

Chapter 2

Groebner Bases

Groebner bases theory was first presented by Bruno Buchberger in his PhD dissertation *"An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal"* [1] in 1965. Buchberger named them after his advisor Wolfgang Gröbner. He also introduced an algorithm (Buchberger's Algorithm) in [1] to compute Groebner bases.

As defined in [2] and [3], a Groebner basis is a set consisting of multivariate polynomials satisfying certain properties. Groebner bases are very useful for finding solutions to many problems in mathematics and other branches of science. We can write some of the problems in which Groebner bases are used as follows: The ideal membership problem: Given a polynomial f from a polynomial ring R with finitely many variables over a field, and an ideal $I \subset R$, does f lie in the ideal I? This problem also related to the problem which asks if $\mathbf{V}(I)$ lies on $\mathbf{V}(f)$. The problem of solving a polynomial equations system: Find all the common solutions to the system of polynomial equations $f_1 = f_2 = \ldots = f_m = 0$ $\big($Note that this problem is the same as the problem asking the points in $\mathbf{V}(f_1, \ldots, f_m)\big)$.

In this chapter, we briefly give the definition and some properties of a Groebner basis along with some theorems and definitions related to Groebner basis theory.

2.1 Hilbert's Basis Theorem

Definition 2.1.1. *Let R be a commutative ring with identity. If every ideal of R is finitely generated, then R is said to be a Noetherian ring.*

Theorem 2.1.2 (**Hilbert's Basis Theorem**)**.** *Let R be a Noetherian ring. Then the polynomial ring $R[x]$ is also a Noetherian ring.*

Proof. Let I be an arbitrary ideal in the polynomial ring $R[x]$. Define L as the set containing all leading coefficients of the polynomials of I. We first prove that the following claim holds.

***Claim*:** L is an ideal of R.

***Proof of Claim*:** L contains 0 since the zero polynomial is contained in I. Let $f = ax^d + f_{rest}$ and $g = bx^e + g_{rest}$ be two polynomials (of degree d and e, respectively) in the ideal I. Clearly, $a \in R$ is the leading coefficient of f and $b \in R$ is the leading coefficient of g. Now define $h = rx^e f - x^d g$ for any $r \in R$. Since $h = (ra - b)x^{e+d} + h_{rest}$ when $ra - b \neq 0$, the leading coefficient of h is $ra - b$. Then since $h \in I$, $(ra - b) \in L$. Therefore, L is an ideal of R, and the claim is proven.

Since L is an ideal of R, and R is Noetherian, L is finitely generated. So let $L = \langle a_1, \ldots, a_n \rangle$ where $a_i \in R$ for $i = 1, 2, \ldots, n$. Suppose also that f_i is a polynomial in I of degree e_i defined as $f_i = a_i x^{e_i} + f_{i_{rest}}$ for each $i = 1, 2, \ldots, n$. Then clearly the leading coefficient of f_i is a_i. Let also $N = \max\{e_1, \ldots, e_n\}$.

Now assume for each d in $\{0, 1, \ldots, N\}$ that L_d is the set containing all leading coefficients of the polynomials (of degree d) in I along with the zero polynomial. Then it is easy to show that L_d is an ideal of R (Similar to the case of L as shown in the above claim). Then, since L_d is an ideal of R which is Noetherian, L_d is finitely generated. Let $L_d = \langle b_{d,1}, \ldots, b_{d,n_d} \rangle$ where $b_{d,i} \in R$ for $i = 1, 2, \ldots, n_d$. Then suppose that $f_{d,i}$ is a polynomial of degree d in the ideal I defined as $f_{d,i} = b_{d,i}x^d + f_{d,i_{rest}}$ for $1 \leq i \leq n_d$. So the leading coefficient of $f_{d,i}$ is $b_{d,i}$.

Our aim is to show that

$$I = \left\langle \{f_1, \ldots, f_n\} \cup \{f_{d,i} : 0 \leq d \leq N, 1 \leq i \leq n_d\} \right\rangle$$

Let J denote the ideal in the right side of the above equation, i.e, $J = \left\langle \{f_1, \ldots, f_n\} \cup \{f_{d,i} : 0 \leq d \leq N, 1 \leq i \leq n_d\} \right\rangle$. Assume on the contrary that $J \neq I$. Note that all of the generators of J are from I. Thus, we conclude that J is included in I. Then there exists a polynomial $f \neq 0$ in I of minimum degree such that $f \notin J$. Let the degree of f be d and the leading coefficient of f be a.

First assume that $d \geq N$. Since a is the leading coefficient of f, we know that $a \in L = \langle a_1, \ldots, a_n \rangle$. Thus, we can write $a = r_1 a_1 + \ldots + r_n a_n$ with $r_i \in R$. Now define $g = r_1 x^{d-e_1} f_1 + \ldots + r_n x^{d-e_n} f_n$. Clearly, $g \in J$ which implies that $g \in I$. We can rewrite g as $g = (r_1 x^{d-e_1} a_1 x^{e_1} + f_{1_{rest}}) + \ldots + (r_n x^{d-e_n} a_n x^{e_n} + f_{n_{rest}}) = (a_1 r_1 + \ldots + a_n r_n) x^d + g_{rest} = a x^d + g_{rest}$. Thus g is also of degree d with the leading coefficient a. Hence, $f - g$ is in I and it is a polynomial of a degree smaller than the degree of f. Since $f \in I$ has minimal degree, we obtain $f - g = 0$, therefore $f = g \in J$ which contradicts with $f \notin J$.

Now assume that $d < N$. Then, for some d, we have $a \in L_d$. Since $L_d = \langle b_{d,1}, \ldots, b_{d,n} \rangle$, we can write $a = r_1 b_{d,1} + \ldots + r_{n_d} b_{d,n_d}$ where $r_i \in R$. Define $g = r_1 f_{d,1} + \ldots + r_{n_d} f_{d,n_d}$. Again, $g \in J$ which implies $g \in I$. We can rewrite g as $g = (b_{d,1} r_1 + \ldots + b_{d,n_d} r_n) x^d + g_{rest} = a x^d + g_{rest}$. Thus, g has degree d and the leading coefficient of g is a. We know that f is also of degree d, and its leading coefficient is a. Hence there is a contradiction as in the previous case.

Therefore, $I = J$ which implies that I is finitely generated. Thus, $R[x]$ is a Noetherian ring. □

Corollary 2.1.3. *Let R be a Noetherian ring. Then every ideal in $R[x_1, \ldots, x_n]$ is finitely generated.*

Proof. We use induction on n to prove this corollary. Let $n = 1$. Then $R[x_1]$ is Noetherian by the Hilbert's Basis Theorem. Assume the theorem holds for

$(n-1>1)$. Then since $R[x_1,\ldots,x_{n-1}]$ is Noetherian, $R[x_1,\ldots,x_{n-1}][x_n]$ is also Noetherian, again by the Hilbert's Basis Theorem. □

2.2 Monomial Orders

A term $x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ is referred as a monomial where a_i is a non-negative integer for all i. Note that the monomial $x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ is denoted by $\mathbf{x^a}$ where $\mathbf{a} = (a_1, a_2, \ldots, a_n)$. For instance, in the case of $n = 3$, $x_1^2x_2^3x_3^5$ is denoted by $\mathbf{x^{(1,3,5)}}$.

Definition 2.2.1 (**Monomial Order**). *Let $\mathbb{K}$ be a field. A monomial order is a total order $<$ on the set of monomials of $\mathbb{K}[x_1,\ldots,x_n]$ which satisfies the following properties:*

(i) $1 < m$ *for all* $1 \neq m$ *in the set of monomials of* $\mathbb{K}[x_1,\ldots,x_n]$.

(ii) If m_1, m_2 *are two monomials of* $\mathbb{K}[x_1,\ldots,x_n]$ *and* $m_1 < m_2$, *then* $m_1m < m_2m$ *for all* m *in the set of monomials of* $\mathbb{K}[x_1,\ldots,x_n]$.

Note that a monomial ordering is a well-ordering. One can see this from the next proposition.

Proposition 2.2.2. *A monomial order on $\mathbb{K}[x_1,\ldots,x_n]$ is Artinian which means that there is a smallest element in every non-empty subset of the set of monomials of $\mathbb{K}[x_1,\ldots,x_n]$.*

Proof. Let I be the ideal generated by the set of monomials of $\mathbb{K}[x_1,\ldots,x_n]$ (Note that the set of monomials does not have to be finite). Then by Proposition 2.1.3, I is finitely generated. Hence we can write $I = \langle m_1,\ldots,m_n\rangle$ where m_i are from the set of monomials of $\mathbb{K}[x_1,\ldots,x_n]$, and $1 \leq i \leq n$. Now define $N = \{m_1,\ldots,m_n\}$. Then let m be the smallest element of N. From the first property of the monomial order definition, we have that $1 < s$ for all monomials s of $\mathbb{K}[x_1,\ldots,x_n]$. Then from the second property of the same definition, we can write $m_i < sm_i$. We also know that each monomial in the ideal I is of the form

sm_i for $1 \leq i \leq n$. Since m is the smallest element in N, we know that $m < m_i$, and hence $m < m_i < sm_i$. Therefore, m is the smallest element in the set of monomials of $\mathbb{K}[x_1, \ldots, x_n]$. $\square$

Now we introduce some examples of the monomial orderings.

Example (Lexicographic Ordering): Let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ be two vectors in $\mathbb{Z}^n_{\geq 0}$. Let $\mathbf{x^a}$ and $\mathbf{x^b}$ be monomials from $\mathbb{K}[x_1, \ldots, x_n]$. We say that $\mathbf{x^a} > \mathbf{x^b}$ with respect to the lexicographic, or lex, ordering induced by $x_1 > x_2 > \ldots > x_n$ if the first non-zero component of $\mathbf{a} - \mathbf{b} = (a_1 - b_1, \ldots, a_n - b_n)$ from the left is positive.

For instance, $x_1^2 x_2^2 x_3^2 > x_1^2 x_2 x_3^5$ with respect to the lex ordering $x_1 > x_2 > x_3$.

Example (Graded Lexicographic Ordering): Let $\mathbf{x^a}$ and $\mathbf{x^b}$ be monomials as in the above example. The total degree of the monomial $\mathbf{x^a}$ defined as $\sum_i^n a_i$. We say that $\mathbf{x^a} > \mathbf{x^b}$ with respect to the graded lexicographic, or grlex, ordering induced by $x_1 > x_2 > \ldots > x_n$ if $\sum_i^n a_i > \sum_i^n b_i$. If $\sum_i^n a_i = \sum_i^n b_i$, then we order the monomials $\mathbf{x^a}$ and $\mathbf{x^b}$ by lex ordering.

For instance, $x_1 x_2^5 x_3 > x_1^2 x_2 x_3^3$ with respect to the grlex ordering $x_1 > x_2 > x_3$.

Example (Graded Reverse Lexicographic Ordering): Let $\mathbf{x^a}$ and $\mathbf{x^b}$ be monomials same as above. The graded reverse lexicographic, or grevlex, ordering again uses total degrees first. We say that $\mathbf{x^a} > \mathbf{x^b}$ with respect to the grevlex ordering induced by $x_1 > x_2 > \ldots > x_n$ if $\sum_i^n a_i > \sum_i^n b_i$. If $\sum_i^n a_i = \sum_i^n b_i$, then we investigate the vector $\mathbf{a} - \mathbf{b} = (a_1 - b_1, \ldots, a_n - b_n)$. If the first non-zero component from the right is negative, then we say that $\mathbf{x^a} > \mathbf{x^b}$ with respect to the grevlex ordering induced by $x_1 > x_2 > \ldots > x_n$.

For instance, $x_1^3 x_2^3 x_3 > x_1^2 x_2^3 x_3^2$ with respect to the grlex ordering $x_1 > x_2 > x_3$.

2.3 Groebner Basis and The Division Algorithm

We first present some preliminary definitions.

Definition 2.3.1. *Let $<$ be a fixed monomial ordering on the set of monomials of the given polynomial ring. The leading term of a non-zero polynomial f is the biggest monomial with respect to $<$ among all the monomials in f. It is denoted by $LT(f)$.*

For instance, the leading term of the polynomial $x_1^2x_2x_3 + x_1x_2^3x_3^2$ with respect to the lex ordering $x_1 > x_2 > x_3$ is $x_1^2x_2x_3$.

Definition 2.3.2. *Let $<$ be a fixed monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$ and I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$. The ideal generated by the leading terms of all the polynomials in I is referred as the ideal of leading terms. The set of leading terms of all the elements in I is denoted by $LT(I)$, i.e., $LT(I) = \{LT(f) : f \in I\}$. The ideal of leading terms is denoted by $\langle LT(I)\rangle$.*

Definition 2.3.3 (**Groebner Basis**)**.** *Let I be a non-zero ideal in $\mathbb{K}[x_1, \ldots, x_n]$ and $<$ be a fixed monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. A finite set of elements $\{g_1, \ldots, g_m\}$ of I is said to be a Groebner basis of I with respect to $<$ if the ideal of leading terms, $\langle LT(I)\rangle$, is generated by the leading terms of $\{g_i\}_{i=1}^m$, i.e.,*

$$\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_m)\rangle.$$

The next theorem shows that a non-zero ideal always has a Groebner basis.

Theorem 2.3.4 (**Existence of Groebner Basis**)**.** *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be a non-zero ideal. Then I has a Groebner basis.*

Proof. First fix a monomial order $<$ on the set of monomials of $\mathbb{K}[x_1, \ldots, x_n]$. Then consider the ideal $\langle LT(I)\rangle$ (the ideal generated by the leading terms of all polynomials of I). By Corollary 2.1.3, we obtain that the ideal $\langle LT(I)\rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ is finitely generated. Thus, we can write $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_m)\rangle$ for $\{g_i\}_{i=1}^m$ in I. By the Definition 2.3.3, $\{g_1, \ldots, g_m\}$ is a Groebner basis for the ideal I with respect to the fixed monomial order $<$. □

We now introduce the general polynomial division algorithm.

Definition 2.3.5 (**Division Algorithm**). *We begin with fixing a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Let $g_1, \ldots, g_m$ be non-zero polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. A polynomial f in $\mathbb{K}[x_1, \ldots, x_n]$ can be divided by the polynomials $\{g_1, \ldots, g_m\}$. Let $q_1, \ldots, q_m$ be the quotients and r be the remainder which are all initially zero.*

If $LT(f)$ is divisible by $LT(g_i)$ for some i, then add $\frac{LT(f)}{LT(g_i)}$ to q_i. Next, replace f by $f - \frac{LT(f)}{LT(g_i)} g_i$, and repeat the procedure.

If $LT(f)$ is not divisible by any of $LT(g_i)$ for $1 \leq i \leq m$, then add $LT(f)$ to r. Next, replace f by $f - LT(f)$, and repeat the procedure.

Note that when the dividend is zero, the process ends and we have $f = q_1 g_1 + \ldots + q_m g_m + r$.

Proposition 2.3.6. *The general polynomial division algorithm over $\mathbb{K}[x_1, \ldots, x_n]$ terminates in a finite number of iterations.*

Proof. First fix a monomial order $<$ on the set of monomials of $\mathbb{K}[x_1, \ldots, x_n]$. Note that a monomial order is Artinian which means that there is a smallest element in every non-empty subset of the set of monomials of $\mathbb{K}[x_1, \ldots, x_n]$. Then the set of monomials of $\mathbb{K}[x_1, \ldots, x_n]$ satisfies the descending chain condition which says that any chain of monomials in $\mathbb{K}[x_1, \ldots, x_n]$ is finite. We know that the leading term of the dividend polynomial (biggest monomial w.r.t. the fixed order $<$) is descending at each step of the division algorithm. Therefore, we conclude that the general polynomial division algorithm terminates in a finite number of iterations. □

Theorem 2.3.7. *Let I be a non-zero ideal in $\mathbb{K}[x_1, \ldots, x_n]$ and $\{g_1, \ldots, g_m\}$ be a Groebner basis with respect to a fixed monomial ordering $<$ on $\mathbb{K}[x_1, \ldots, x_n]$. Then I is generated by the elements of the Groebner basis, i.e.,*

$$I = \langle g_1, \ldots, g_m \rangle.$$

Proof. Clearly, $\langle g_1, \ldots, g_m \rangle \subset I$ since all g_i for $1 \leq i \leq m$ are in I. Now let f be a non-zero polynomial in I. Then $LT(f) \in LT(I)$. Since $\{g_1, \ldots, g_m\}$ is a Groebner basis for I, we have that $\big\langle LT(I) \big\rangle = \big\langle LT(g_1), \ldots, LT(g_m) \big\rangle$. Thus, there is a g_{i_1} for some $i = 1, 2, \ldots, m$ such that $LT(f) = a_1 LT(g_{i_1})$ where a_1 is a monomial in $\mathbb{K}[x_1, \ldots, x_n]$. Now define $h_1 = f - a_1 g_{i_1}$. Clearly, $h_1 \in I$. Note also that the degree of the leading term of h_1 is lower than f, i.e., $LT(h_1) < LT(f)$. If $h_1 = 0$, we have $f = a_1 g_{i_1}$, and $f \in \langle g_1, \ldots, g_m \rangle$. If $h_1 \neq 0$, then reiterate the entire procedure. Define $h_2 = h_1 - a_2 g_{i_2}$. Then $h_2 \in I$. We see that $LT(h_2) < LT(h_1)$. If $h_2 = 0$, then $h_1 = a_2 g_{i_2}$, and $h_1 \in \langle g_1, \ldots, g_m \rangle$. If $h_2 \neq 0$, reiterate the entire procedure. The previous lemma ensures that this procedure must end in a finite number of steps. Say this process terminates at s meaning that $h_s = 0$. Then we obtain

$$f = \sum_{k=1}^{s} a_k g_{i_k}$$

Then we have $f \in \langle g_1, \ldots, g_m \rangle$, so $I \subset \langle g_1, \ldots, g_m \rangle$. Therefore, we get $I = \langle g_1, \ldots, g_m \rangle$ as desired. □

Now we introduce the minimal and reduced Groebner basis.

Definition 2.3.8. *Let I be a non-zero ideal in $\mathbb{K}[x_1, \ldots, x_n]$, and a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$ be fixed. A Groebner basis $\{g_1, \ldots, g_m\}$ of I is said to be a minimal Groebner basis if each $LT(g_i)$ is monic and $LT(g_i)$ is not divisible by $LT(g_j)$ for $i \neq j$.*

Definition 2.3.9 (**Reduced Groebner Basis**). *Let I be a non-zero ideal in $\mathbb{K}[x_1, \ldots, x_n]$, and a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$ be fixed. A Groebner basis $\{g_1, \ldots, g_m\}$ of I is said to be a reduced Groebner basis if each $LT(g_i)$ is monic and any term in g_i is not divisible by $LT(g_j)$ for $i \neq j$.*

As we see, a reduced Groebner basis is a minimal Groebner basis. The speciality of reduced Groebner bases is that they are unique.

Proposition 2.3.10. *Let I be any non-zero ideal of $\mathbb{K}[x_1, \ldots, x_n]$. There is a unique reduced Groebner basis for I for a given monomial ordering.*

Proof. Before proving the uniqueness of reduced Groebner basis, we will give the following two claims:

***Claim*:** Let a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$ be fixed. $\{g_1, \ldots, g_k\}$ is a minimal Groebner basis for $I \subset \mathbb{K}[x_1, \ldots, x_n]$ with respect to the fixed monomial ordering if and only if $\{LT(g_1), \ldots, LT(g_k)\}$ is a minimal generating set for $LT(I)$.

***Proof of Claim*:** First assume that $\{g_1, \ldots, g_k\}$ is a minimal Groebner basis for $I \subset \mathbb{K}[x_1, \ldots, x_n]$ with respect to the fixed monomial ordering. Then by the definition of Groebner basis (Definition 2.3.3), we obtain that $\{LT(g_1), \ldots, LT(g_k)\}$ generates $LT(I)$. Since $\{g_1, \ldots, g_k\}$ is a minimal Groebner basis, we also have, by Definition 2.3.8, that $LT(g_i$ is monic for each $1 \leq i \leq k$, and $LT(g_j)$ is not divisible by $LT(g_i)$ for $i \neq j$. Then we can conclude that no proper subset of $\{LT(g_1), \ldots, LT(g_k)\}$ generates $LT(I)$. Thus, this makes $\{LT(g_1), \ldots, LT(g_k)\}$ a minimal generating set for $LT(I)$. Conversely, assume that $\{LT(g_1), \ldots, LT(g_k)\}$ is a minimal generating set for $LT(I)$ which means that no proper subset of $\{LT(g_1), \ldots, LT(g_k)\}$ generates $LT(I)$. Hence, $LT(g_i)$ is not divisible by $LT(g_j)$ for $i \neq j$. Additionally, since $\{LT(g_1), \ldots, LT(g_k)\}$ generates $LT(I)$, $\{g_1, \ldots, g_k\}$ is a Groebner basis for I (by Definition 2.3.3). Now it is left to show that $LT(g_i$ is monic for each $1 \leq i \leq k$ to prove that $\{g_1, \ldots, g_k\}$ is a minimal Groebner basis. Note that since $\mathbb{K}$ is field, we can scale each polynomial in $I \subset \mathbb{K}[x_1, \ldots, x_n]$ by the multiplicative inverse of the coefficient of its leading term to make that polynomial monic. So without loss of generality, we can assume that $LT(g_i)$ is monic for $1 \leq i \leq k$. Therefore, $\{g_1, \ldots, g_k\}$ is a minimal Groebner basis.

***Claim*:** Let a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$ be fixed. Two minimal Groebner bases for the ideal I have the same leading terms and number of elements.

***Proof of Claim*:** Let $\{g_1, \ldots, g_k\}$ and $\{h_1, \ldots, h_s\}$ be two minimal Groebner bases for the ideal I. By the first claim, $\{LT(g_1), \ldots, LT(g_k)\}$ and $\{LT(h_1), \ldots, LT(h_s)\}$ are two minimal generating sets for $LT(I)$. Note that

if $\{m_1, \ldots, m_l\}$ is a minimal generating set of monomials which generates the monomial ideal J, then m_j for $1 \leq j \leq l$ are unique; see [4] (Page 332, Exercise 14). Therefore, $LT(g_i)$ for $1 \leq i \leq k$ and $LT(h_j)$ for $1 \leq j \leq s$ are unique, and $k = s$. Then, without loss of generality, we may assume $LT(g_i) = LT(h_i)$ for $1 \leq i \leq k$. Therefore, two minimal Groebner bases, $\{g_1, \ldots, g_k\}$ and $\{h_1, \ldots, h_k\}$, for the ideal I have the same leading terms and number of elements.

Now we are ready to prove the uniqueness of the reduced Groebner basis.

Let $G = \{g_1, \ldots, g_k\}$ and $G' = \{g'_1, \ldots, g'_m\}$ be two different reduced Groebner basis for the ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Since reduced Groebner bases are also minimal Groebner bases, by the previous claim we obtain that the number of elements in G and G' are the same, i.e., $k = m$, and G and G' have the same leading terms. Then, without loss of generality, we can assume $LT(g_i) = LT(g'_i) = p_i$ for $1 \leq i \leq k$. Now define the polynomial h_i for fixed i as $h_i = g_i - g'_i$. Let h_i be a non-zero polynomial. We know that h_i is in I (since g_i and g'_i are in I), hence $LT(g_j) = LT(g'_j) = p_j$, for some j, should divide $LT(h_i)$. Since G and G' are reduced Groebner bases, no term in g_i, or g'_i is divisible by p_j for $i \neq j$ which implies $LT(h_i)$ is not divisible by p_j. Moreover, note that the leading terms of g_i and g'_i cancel each other out in h_i, hence the degree of h_i is smaller than the degree of p_i. Thus, $LT(h_i)$ also is not divisible by p_i. Therefore, h_i must be equal to zero, which implies $g_i = g'_i$ for $1 \leq i \leq k$. Hence the two reduced Groebner bases G and G' for the ideal I are equal. $\square$

Chapter 3

Hilbert's Nullstellensatz

The *Nullstellensatz* which is translated as *"theorem of zeros"* into English was presented and proven by David Hilbert in his paper *"Uber die vollen Invariantensysteme"* [5] in 1893.

In this chapter, we will present the weak and strong forms of the Hilbert's Nullstellensatz along with Noether's Normalization Lemma which we use in the proof of the Hilbert's Nullstellensatz. We will also introduce Nullstellensatz certificate which emerges when the system of polynomial equations $f_1 = \ldots = f_s = 0$ in the given polynomial ring has no solution.

3.1 Weak and Strong Forms of Hilbert's Nullstellensatz

We will first present some definitions which are used in the rest of the chapter.

Definition 3.1.1. *Let Q be a subring of a commutative ring R with identity. An element $r \in R$ is said to be integral over Q if it is a root of a monic polynomial in $Q[x]$. The ring R is said to be integral over Q if every $r \in R$ is integral over Q.*

Definition 3.1.2. *Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is a field. Then*

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}$$

is said to be the affine variety defined by the polynomials $f_1, \ldots, f_s$.

Definition 3.1.3. *Let $\mathbf{V} \in \mathbb{K}^n$ be an affine variety. Then*

$$\mathbf{I}(\mathbf{V}) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in \mathbf{V}\}$$

It is easy to see that $\mathbf{I}(\mathbf{V}) \in \mathbb{K}[x_1, \ldots, x_n]$ is an ideal and called the ideal of $\mathbf{V}$.

Now we will state the Noether's Normalization Lemma.

Lemma 3.1.4 (Noether's Normalization Lemma [4, Page 699]). *Let $\mathbb{K}$ be a field and suppose that $\mathbb{K}[r_1, \ldots, r_m]$ is a finitely generated $\mathbb{K}$-algebra. Then for some q with $0 \leq q \leq m$, there are algebraically independent elements $\lambda_1, \ldots, \lambda_q$ in $\mathbb{K}[r_1, \ldots, r_m]$ such that $\mathbb{K}[r_1, \ldots, r_m]$ is integral over $\mathbb{K}[\lambda_1, \ldots, \lambda_q]$.*

Proof. We will prove the lemma by induction on m. First note that if $r_1, \ldots, r_m$ are algebraically independent over $\mathbb{K}$, then we can take $\lambda_i = r_i$ for $1 \leq i \leq m$, and the result is clear. If $r_1, \ldots, r_m$ are not algebraically independent over $\mathbb{K}$, then there exists a polynomial $f(x_1, \ldots, x_m)$ in $\mathbb{K}[x_1, \ldots, x_m]$ such that $f(r_1, \ldots, r_m) = 0$. Note that f is a polynomial which is a sum of monomials $ax_1^{e_1}x_2^{e_2}\ldots x_m^{e_m}$, and let the degree of f be d. We can assume that f is non-constant in x_m with coefficients from $\mathbb{K}[x_1, \ldots, x_{m-1}]$. We will make a transformation that converts f to a monic polynomial in x_m with coefficients from a subring of $\mathbb{K}[r_1, \ldots, r_m]$ which is generated by $m-1$ elements over $\mathbb{K}$.

Now define $\alpha_i = (1+d)^i$ and $x_i^* = x_i - x_m^{\alpha_i}$ for $1 \leq i \leq m-1$. Let also

$$g(x_1^*, \ldots, x_{m-1}^*, x_m) = f(x_1^* + x_m^{\alpha_1}, \ldots, x_{m-1}^* + x_m^{\alpha_{m-1}}, x_m).$$

Clearly, g is in $\mathbb{K}[x_1^*, \ldots, x_{m-1}^*, x_m]$. We know that f is a sum of monomials of the form $ax_1^{e_1}x_2^{e_2}\ldots x_m^{e_m}$ which is equal to $a(x_1^* + x_m^{\alpha_1})^{e_1}\ldots(x_{m-1}^* + x_m^{\alpha_{m-1}})^{e_{m-1}}x_m^{e_m}$ by the newly defined variables. Hence each monomial in f provides a term of the

form ax_m^e to g where a is constant. Note also that since $\alpha_i = (1+d)^i$ (d is the degree of f and $e_1 + \ldots + e_m$ is at most d.), distinct monomials in f provides different values of e for ax_m^e in g. Let k be the highest power of x_m in g. Then we have

$$g = cx_m^k + \sum_i^{k-1} h_i(x_1^*, \ldots, x_{m-1}^*)x_m^i$$

for non-zero $c \in \mathbb{K}$. If we divide g by c, then clearly $\frac{g}{c}$ is a monic polynomial in x_m. Since $g(x_1^*, \ldots, x_{m-1}^*, x_m) = f(x_1, \ldots, x_m)$, $\frac{f}{c}$ is also a monic polynomial in x_m. We also know that

$$\frac{1}{c}g(r_1 - r_m^{\alpha_1}, \ldots, r_{m-1} - r_m^{\alpha_{m-1}}, r_m) = \frac{1}{c}f(r_1, \ldots, r_{m-1}, r_m) = 0.$$

Let $s_i = r_i - r_m^{\alpha_i}$. Then it follows that r_m is integral over $\mathbb{K}[s_1, \ldots, s_{m-1}]$. Let $A = \mathbb{K}[s_1, \ldots, s_{m-1}]$. Note that r_i is a root of the monic polynomial $x - s_i - r_m^{\alpha_i}$. Hence every r_i is integral over $A[r_m]$ for $1 \leq i \leq m-1$ which follows that $\mathbb{K}[r_1, \ldots, r_m]$ is integral over $A[r_m]$. Since the integrality is transitive, we also have that $\mathbb{K}[r_1, \ldots, r_m]$ is integral over A. We know that A is a $\mathbb{K}-$algebra which is generated by $m-1$ elements, so by induction, the proof is done. □

The following is a simple version of the previous lemma which is specific to the case in which the field $\mathbb{K}$ is infinite.

Lemma 3.1.5 ([**6, Page 169**]). *Let f be a non-constant polynomial in $\mathbb{K}[x_1, \ldots, x_n]$ where $n \geq 2$ and $\mathbb{K}$ is an infinite field. Then we can find $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ such that the coefficient of the term x_n^d (the total degree of the polynomial f is d) is non-zero in*

$$f(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1}x_n, x_n).$$

Proof. Clearly, we may assume that f is homogeneous. Let $x_{i_1}x_{i_2}\ldots x_{i_d}$ stand for any monomial in f (of degree d since f is homogeneous) where $i_1, \ldots, i_d$ do not have to be distinct. Now evaluate f at $\{x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1}x_n, x_n\}$. If we look at the coefficient of x_n^d in $f(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1}x_n, x_n)$, we see that it equals to $\lambda_{i_1}\ldots\lambda_{i_d}$ since the monomial $x_{i_1}x_{i_2}\ldots x_{i_d}$ of f becomes $(x_{i_1} + \lambda_{i_1}x_n)(x_{i_2}+\lambda_{i_2}x_n)\ldots(x_{i_d}+\lambda_{i_d}x_n)$ under $f(x_1+\lambda_1 x_n, \ldots, x_{n-1}+\lambda_{n-1}x_n, x_n)$. Then,

we can deduce that the coefficient of x_n^d in $f(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1} x_n, x_n)$ is actually equals to:

$$f(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, 1).$$

Now by induction on n, we are able to find a point at which $f(x_1, \ldots, x_{n-1}, 1) \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ does not vanish since $\mathbb{K}$ is an infinite field. If we take this point as $(\lambda_1, \lambda_2, \ldots, \lambda_{n-1})$, we conclude that $f(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, 1)$ is non-zero which follows that the coefficient of term x_n^d in $f(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1} x_n, x_n)$ is non-zero. □

Theorem 3.1.6 (**Hilbert's Nullstellensatz (Weak Form)**). *Let I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is an algebraically closed field. If $\mathbf{V}(I) = \emptyset$, then $I = \mathbb{K}[x_1, \ldots, x_n]$.*

(Note that the converse also holds. If $I = \mathbb{K}[x_1, \ldots, x_n]$, then $1 \in I$, hence $\mathbf{V}(I) = \emptyset$.)

We can also state Hilbert's Weak Nullstellensatz in the following form:

Theorem 3.1.7 ([**6, Page 170**]). *Let $\mathbb{K}$ be an algebraically closed field. If I is a proper ideal of $\mathbb{K}[x_1, \ldots, x_n]$, then there exists a point $(a_1, \ldots, a_n)$ in $\mathbb{K}^n$ such that $f(a_1, \ldots, a_n) = 0$ for all f in I.*

Proof. First assume that $I = \{0\}$. In this case, zero polynomial is the only polynomial in I and it obviously vanishes at all points. Now assume that the ideal I is non-zero. We will prove the theorem by induction on n.

Let $n = 1$. Then $\mathbb{K}[x_1]$ is a Principal Ideal Domain. Therefore, any proper, non-zero ideal I in $\mathbb{K}[x_1]$ is principal which follows that a non-constant, single polynomial generates I. Since $\mathbb{K}$ is an algebraically closed field, that polynomial has at least one root, say β, in $\mathbb{K}$. Hence we obtain that $f(\beta) = 0$ for all the polynomials f in I.

Now let $n > 1$. Assume that the theorem holds for all proper ideals in $\mathbb{K}[x_1, \ldots, x_{n-1}]$. Our goal is to show that the theorem holds for a proper ideal I in $\mathbb{K}[x_1, \ldots, x_n]$.

The simple version of the Noether's Normalization Lemma (Lemma 3.1.5) tells us that the coefficient of the term x_n^d is non-zero for a non-constant polynomial $f \in I$ when f is evaluated at a suitable polynomial. Hence we can scale f accordingly in order to obtain a monic polynomial (in x_n) $g \in I$. Now consider the ideal $I' = I \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$ which contains all the polynomials in I except the ones with the indeterminate x_n. Note that I' is a proper ideal of $\mathbb{K}[x_1, \ldots, x_{n-1}]$ since I is proper and I' contains polynomials from I. Thus, the induction hypothesis allows us to find a point $(a_1, \ldots, a_{n-1})$ with $f(a_1, \ldots, a_{n-1}) = 0 \; \forall f \in I'$. Now we present a claim:

***Claim*:** $J = \{f(a_1, \ldots, a_n, x_n) : f \in I\}$ is a proper ideal of $\mathbb{K}[x_n]$.

Assume that the claim holds. Therefore, J is generated either by h=0, or by a non-constant single polynomial $h(x_n)$. When $h = 0$, it is obvious that $h(x_n)$ has a root. When h is a non-constant polynomial, $h(x_n)$ has a root, say a_n, in $\mathbb{K}$ since $\mathbb{K}$ is algebraically closed. Thus, in both cases, $f(a_1, \ldots, a_{n-1}, a_n) = 0$ for all f in I which proves that there exists a point $(a_1, \ldots, a_n)$ in $\mathbb{K}^n$ such that $f(a_1, \ldots, a_n) = 0$ for all f in any proper I.

Therefore, it remains to show that the claim holds to complete the proof.

***Proof of Claim*:** Assume on the contrary that $J = \{f(a_1, \ldots, a_n, x_n) : f \in I\}$ is a not proper ideal of $\mathbb{K}[x_n]$. Then there exists a polynomial f in I such that $f(a_1, \ldots, a_n, x_n) = 1$. We can express f as $f = f_0 + f_1 x_n + \ldots + f_d x_n^d$ where $f_1(a_1, \ldots, a_{n-1}) = \ldots = f_d(a_1, \ldots, a_{n-1}) = 0$ and $f_0(a_1, \ldots, a_{n-1}) = 1$ with $f_i \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ for all i. Similarly, we can write the polynomial $g \in I$, which is monic in x_n, as $g = g_0 + g_1 x_n + g_2 x_n^2 + \ldots + g_{e-1} x_n^{e-1} + x_n^e$ where $g_j \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ for all $0 \leq j \leq (e-1)$. Now define R as the resultant of f and g with respect to the indeterminate x_n. The resultant R, which is the determinant of the $(d+e) \times (d+e)$ matrix constructed as follows, is a polynomial

in $\mathbb{K}[x_1, \ldots, x_{n-1}]$.

$$R = \begin{pmatrix} f_0 & f_1 & \ldots & f_d & 0 & 0 & \ldots & 0 \\ 0 & f_0 & \ldots & f_{d-1} & f_d & 0 & \ldots & 0 \\ & & \ddots & & & & & \\ 0 & \ldots & 0 & f_0 & f_1 & \ldots & f_{d-1} & f_d \\ g_0 & g_1 & \ldots & g_{e-1} & 1 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{e-2} & g_{e-1} & 1 & 0 \ldots & 0 \\ & & \ldots & & & & \ldots & \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{e-1} & 1 \end{pmatrix}$$

We can conclude that $R \in I$. To observe this, add x_n times the second column to the first column, then add x_n^2 times the third column to the first column. Continue doing this until adding x_n^{d+e-1} times the last column $\big((d+e)^{th}$ column$\big)$ to the first column. Since the determinant is expanded along the first column, the resultant R, which is generated by f and g, is in I. Recall that $I' \subset \mathbb{K}[x_1, \ldots, x_{n-1}]$ includes all of the polynomials in I except the ones with the indeterminate x_n. Thus, R is in I' since R is a polynomial in $\mathbb{K}[x_1, \ldots, x_{n-1}]$. Now we evaluate the resultant R at the point $(a_1, \ldots, a_{n-1})$. We can do this by first evaluating the values of all the polynomials at $(a_1, \ldots, a_{n-1})$, and then computing the determinant of the matrix. By doing so, we obtain a lower triangular matrix with all the diagonal entries are equal to 1. Thus, $R(a_1, \ldots, a_{n-1}) = 1$ which implies $R \notin I'$ since the induction hypothesis says $f(a_1, \ldots, a_{n-1}) = 0$ for all $f \in I'$. It is a contradiction, so the claim holds. □

The following theorem states the Hilbert's Nullstellensatz in the strong form.

Theorem 3.1.8 (**Hilbert's Nullstellensatz (Strong Form)**). *Let I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is an algebraically closed field. Then*

$$\mathbf{I}\big(\mathbf{V}(I)\big) = \sqrt{I}.$$

To prove this theorem we first need the following theorem.

Theorem 3.1.9. *If* $f \in \mathbf{I}\big(\mathbf{V}(f_1, \ldots, f_s)\big)$ *where* $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ *and* $\mathbb{K}$ *is an algebraically closed field, then there exists an integer* $m \geq 1$ *such that*

$$f^m \in \langle f_1, \ldots, f_s \rangle.$$

Proof. Our aim is to prove that

$$f^m = \sum_{i=1}^{s} \alpha_i f_i$$

for some polynomials $\alpha_i \in \mathbb{K}[x_1, \ldots, x_n]$. Now consider the following ideal

$$J = \langle f_1, \ldots, f_s, 1 - yf \rangle \text{ in } \mathbb{K}[x_1, \ldots, x_n, y].$$

Our claim is that $\mathbf{V}(J) = \emptyset$.

***Claim*: $\mathbf{V}(J) = \emptyset$.**

***Proof of Claim*:** Let $(a_1, \ldots, a_n, a_{n+1})$ be an arbitrary point in $\mathbb{K}^{n+1}$. We have two cases:

(i) $f_i(a_1, \ldots, a_n) = 0$ *for all* $1 \leq i \leq s$.

(ii) $f_i(a_1, \ldots, a_n) \neq 0$ *for some* $1 \leq i \leq s$.

In case (i), we also have $f(a_1, \ldots, a_n) = 0$ since $f \in \mathbf{I}\big(\mathbf{V}(f_1, \ldots, f_s)\big)$. When the polynomial $1 - yf$ is evaluated at $(a_1, \ldots, a_n, a_{n+1})$, we see that it equals to the value $1 - a_{n+1}f(a_1, \ldots, a_n) = 1$. Hence $(a_1, \ldots, a_n, a_{n+1})$ is not in $\mathbf{V}(J)$. In case (ii), we can think of f_i, for some i, as a polynomial in $n+1$ variables that does not depend on the last variable. Then $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$ since $f_i(a_1, \ldots, a_n) \neq 0$. It follows that $(a_1, \ldots, a_n, a_{n+1})$ is not in $\mathbf{V}(J)$ again. Then we can obtain the result that $\mathbf{V}(J) = \emptyset$ since the point $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{K}^{n+1}$ was chosen arbitrarily. The claim is proven.

By the weak form of Hilbert's Nullstellensatz (Theorem 3.1.6), we obtain that $J = \mathbb{K}[x_1, \ldots, x_n, y]$ since $\mathbf{V}(J) = \emptyset$. So this implies that $1 \in J$ which is:

$$1 = \sum_{i=1}^{s} f_i g_i(x_1, \ldots, x_n, y) + (1 - yf)h(x_1, \ldots, x_n, y)$$

for some g_i and h in $\mathbb{K}[x_1, \ldots, x_n, y]$. Now let $y = 1/f(x_1, \ldots, x_n)$. Then the above equation transforms to the following:

$$1 = \sum_{i=1}^{s} f_i g_i(x_1, \ldots, x_n, 1/f).$$

When we multiply both sides of the above equation by f^m for a large enough integer m, all the denominators can be cancelled and we get

$$f^m = \sum_{i=1}^{s} \alpha_i f_i$$

for some $\alpha_i \in \mathbb{K}[x_1, \ldots, x_n]$ which completes the proof. □

Now we can state the proof of the Strong Nullstellensatz as follows:

Proof. Let $f \in \sqrt{I}$. Then we have $f^m \in I$ for some $m \geq 1$. Thus, f^m vanishes at all points of $\mathbf{V}(I)$. Then clearly f vanishes at all points of $\mathbf{V}(I)$, so $f \in \mathbf{I}\big(\mathbf{V}(I)\big)$. Therefore, $\sqrt{I} \subset \mathbf{I}\big(\mathbf{V}(I)\big)$. Now let us show that $\mathbf{I}\big(\mathbf{V}(I)\big) \subset \sqrt{I}$. Let $f \in \mathbf{I}\big(\mathbf{V}(I)\big)$ which means f vanishes at all points of $\mathbf{V}(I)$. Then by the previous theorem, we can conclude that there exists an integer $m \geq 1$ such that $f^m \in I$. Hence, $f \in \sqrt{I}$. Therefore, we have $\mathbf{I}\big(\mathbf{V}(I)\big) = \sqrt{I}$. □

3.2 Hilbert's Nullstellensatz Certificate

The following theorem can be considered as a corollary of the Weak Hilbert's Nullstellensatz (Theorem 3.1.7).

Theorem 3.2.1. *Let $f_1, f_2, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is an algebraically closed field. The system of polynomial equations $f_1 = f_2 = \ldots = f_s = 0$ has no solution in $\mathbb{K}^n$ if and only if there exists polynomials $\beta_1, \beta_2, \ldots, \beta_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ satisfying*

$$\sum_{i=1}^{s} \beta_i f_i = 1.$$

Proof. Assume that $I = \langle f_1, f_2, \ldots, f_s \rangle$ and that the system of polynomial equations $f_1 = f_2 = \ldots = f_s = 0$ has no solution in $\mathbb{K}^n$. Then, by the Theorem 3.1.2, we can conclude that I is not proper which implies I is the whole ring, hence $1 \in I$. Thus, we can find polynomials $\beta_1, \ldots, \beta_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that $\sum_{i=1}^{s} \beta_i f_i = 1$. Conversely, assume that there exists polynomials $\beta_1, \beta_2, \ldots, \beta_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ satisfying $\sum_{i=1}^{s} \beta_i f_i = 1$. Then $1 \in I$, which implies $\mathbf{V}(I) = \emptyset$. Hence, $f_1 = f_2 = \ldots = f_s = 0$ has no solution. □

Definition 3.2.2 (**Nullstellensatz Certificate**). *The set of polynomials $\{\beta_i\}_i$ in $\sum \beta_i f_i$ is referred as a Nullstellensatz certificate.*

As you can easily see, if a Nullstellensatz certificate exists, then 1 is in the ideal generated by $\{f_i\}_{i=1}^{s}$ which shows that there is no solution to the given polynomial equations system. Therefore, like Groebner basis, it may also be used to determine if a given system has a solution. J. A. De Loera et al. introduced an algorithm (NulLA) in [7], [8] to determine whether a given polynomial equations system has a solution or not. If the system has no solution, then this algorithm gives an associated Nullstellensatz certificate. Hence this algorithm may also be used (like Groebner basis) to test whether a graph-theoretic problem encoded by a polynomial equations system has an affirmative answer or not. Now we have a simple example.

Example: Consider the following polynomial equations system.

$$f_1 = x + 1 = 0$$
$$f_2 = x^2 + y = 0$$
$$f_3 = x + y = 0.$$

As we can easily see, this system of polynomial equations has no solution over $\mathbb{K}[x, y]$ for any algebraically closed field $\mathbb{K}$ whose characteristic is different from 2. Thus, there exists a Nullstellensatz certificate $\{\beta_i\}_i$ satisfying $\sum_{i=1}^{3} \beta_i f_i = 1$. Suppose that the degree of the associated Nullstellensatz certificate is 1. Then

we can write:

$$\underbrace{(\alpha_0 x + \alpha_1 y + \alpha_2)}_{\beta_1}(x+1) + \underbrace{(\alpha_3 x + \alpha_4 y + \alpha_5)}_{\beta_2}(x^2+y) + \underbrace{(\alpha_6 x + \alpha_7 y + \alpha_8)}_{\beta_3}(x+y) = 1.$$

We expand this into monomials and get:

$$(\alpha_0 + \alpha_2 + \alpha_8)x + (\alpha_0 + \alpha_5 + \alpha_6)x^2 + \alpha_3 x^3 + (\alpha_1 + \alpha_5 + \alpha_8)y + (\alpha_4 + \alpha_7)y^2 + (\alpha_1 + \alpha_3 + \alpha_6 + \alpha_7)xy + \alpha_4 x^2 y + \alpha_2 = 1.$$

Then we obtain:

$$(\alpha_0 + \alpha_2 + \alpha_8) = (\alpha_0 + \alpha_5 + \alpha_6) = \ldots = \alpha_4 = 0, \quad \text{and} \quad \alpha_2 = 1.$$

We solve the above system, and then obtain the Nullstellensatz certificate as

$$\{\underbrace{\frac{1}{2}y + 1}_{\beta_1}, \underbrace{\frac{1}{2}}_{\beta_2}, \underbrace{-\frac{1}{2}x - 1}_{\beta_3}\}$$

satisfying

$$(\frac{1}{2}y + 1)(x+1) + \frac{1}{2}(x^2+y) + (-\frac{1}{2}x - 1)(x+y) = 1.$$

There are some well-known upper bounds for the degrees of the Nullstellensatz certificates. We will first present the result introduced by Kollár in [9].

Lemma 3.2.3 (Kollár). *Let $\mathbb{K}$ be an algebraically closed field. Suppose that $f_1, f_2, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ with $d = \max\{deg(f_i)\}$. If $f_1, f_2, \ldots, f_s$ have no common zeros, then*

$$\sum_{i=1}^{s} \beta_i f_i = 1 \text{ where } deg(\beta_i) \leq \max\{3, d\}^n.$$

The next result was originally introduced by Daniel Lazard in [10]. We now consider the summarized result presented in [8].

Lemma 3.2.4 (**Lazard**). *Let $\mathbb{K}$ be an algebraically closed field. Suppose that $f_1, f_2, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ with $d = \max\{deg(f_i)\}$. If $f_1, f_2, \ldots, f_s$ have no common zeros, then we get*

$$\sum_{i=1}^{s} \beta_i f_i = 1 \text{ where } deg(\beta_i) \leq n(d-1).$$

3.3 Some Preliminary Results

Proposition 3.3.1. *Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ and $p = (x_1 - a_1)\ldots(x_1 - a_d)$ where the $a_1, a_2, \ldots, a_d$ are distinct. Then*

$$I + \langle p \rangle = \bigcap_j (I + \langle x_1 - a_j \rangle).$$

Proof. We first show that $I + \langle p \rangle \subset \bigcap_j (I + \langle x_1 - a_j \rangle)$. Let $m + pk \in I + \langle p \rangle$ where $m \in I$ and $k \in \mathbb{C}[x_1, \ldots, x_n]$. Since $p = (x_1 - a_1)\ldots(x_1 - a_d)$, pk is in the ideal generated by $(x_1 - a_j)$ for all $1 \leq j \leq d$, i.e., $pk \in \langle x_1 - a_j \rangle \ \forall_j$. Thus, $m + pk \in I + \langle x_1 - a_j \rangle \ \forall_j$ which implies $m + pk \in \bigcap_j (I + \langle x_1 - a_j \rangle)$. Hence $I + \langle p \rangle \subset \bigcap_j (I + \langle x_1 - a_j \rangle)$ as desired. Now we show that $p_j(I + \langle x_1 - a_j \rangle) \subset I + \langle p \rangle$ where $p_j = \prod_{i \neq j} (x_1 - a_i)$. Let $m + k(x_1 - a_j) \in I + \langle x_1 - a_j \rangle$ where $m \in I$ and $k \in \mathbb{C}[x_1, \ldots, x_n]$. Note that $p_j(m + k(x_1 - a_j)) = p_j m + k p_j (x_1 - a_j) = p_j m + kp \in I + \langle p \rangle$. Hence $p_j(I + \langle x_1 - a_j \rangle) \subset I + \langle p \rangle$ is proven. Recall that $p_j = \prod_{i \neq j} (x_1 - a_i)$. Thus, there does not exist a point a_i such that $p_j(a_i) = 0$ for all j. Thus, the system of polynomial equations $p_1, \ldots, p_n = 0$ has no solution. Then by the Theorem 3.2.1, there exist polynomials $h_1, \ldots, h_n$ such that $\sum_j h_j p_j = 1$. Now we show that $\bigcap_j (I + \langle x_1 - a_j \rangle) \subset I + \langle p \rangle$ to conclude the proof. Let $g \in \bigcap_j (I + \langle x_1 - a_j \rangle)$. Since $\sum_j h_j p_j = 1$, we can write $g = \sum_j h_j p_j g$. We know that $g h_j \in I + \langle x_1 - a_j \rangle$ for all j. Then since $p_j(I + \langle x_1 - a_j \rangle) \subset I + \langle p \rangle$, $g p_j h_j \in I + \langle p \rangle$ for all j. Thus, $g = \sum_j h_j p_j g \in I + \langle p \rangle$ which proves $\bigcap_j (I + \langle x_1 - a_j \rangle) \subset I + \langle p \rangle$. □

Definition 3.3.2. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal where $\mathbb{K}$ is a field. I is said to be zero-dimensional if $\mathbf{V}(I)$ is a finite set.*

Proposition 3.3.3 ([**11, Page 39**]). *Let I be a zero-dimensional ideal in $\mathbb{C}[x_1, \ldots, x_n]$. Let p_i be the unique monic generator of $I \cap \mathbb{C}[x_i]$ for each $i = 1, \ldots, n$, and $p_{i,red}$ be the square-free part of p_i. Then*

$$\sqrt{I} = I + \langle p_{1,red}, \ldots, p_{n,red} \rangle.$$

Proof. Let $J = I + \langle p_{1,red}, \ldots, p_{n,red} \rangle$. Our first step is to show that J is radical which is $J = \sqrt{J}$. After showing that J is radical, we will prove that $J = \sqrt{I}$. Since $\mathbb{C}$ is algebraically closed, $\mathbb{C}$ contains a root for every non-constant polynomial in $\mathbb{C}[x_i]$. We know that $p_{i,red}$ is the square-free part of p_i which is the unique monic generator of $I \cap \mathbb{C}[x_i]$. Therefore, we can write $p_{i,red} = (x_i - a_{i1})(x_i - a_{i2}) \ldots (x_i - a_{id_i})$ for each $p_{i,red}$ where a_{ij} are distinct. Then we obtain the following:

$$J = J + \langle p_{1,red} \rangle = \bigcap_j (J + \langle x_1 - a_{1j} \rangle).$$

Let us first show that the first equality, $J = J + \langle p_{1,red} \rangle$, holds. $J \subseteq J + \langle p_{1,red} \rangle$ is clear. Conversely, consider the element $f + hp_{1,red} \in J + \langle p_{1,red} \rangle$, where $f \in J$ and $h \in \mathbb{C}[x_1, x_2, \ldots, x_n]$. Since $f \in J$ and $hp_{1,red} \in J$ (since $p_{1,red} \in J$), $f + hp_{1,red} \in J$. Thus, $J + \langle p_{1,red} \rangle \subseteq J$, and hence $J = J + \langle p_{1,red} \rangle$.

Now let us show that the second equality $J + \langle p_{1,red} \rangle = \bigcap_j (J + \langle x_1 - a_{1j} \rangle)$ holds. We know that $p_{1,red} = (x_1 - a_{11})(x_1 - a_{12}) \ldots (x_1 - a_{1d_1})$ where a_{1j} are distinct. Hence, by the Proposition 3.3.1, we obtain

$$J + \langle p_{1,red} \rangle = \bigcap_j (J + \langle x_1 - a_{1j} \rangle)$$

as desired. Now apply the same process to $p_{2,red}$ to decompose each $J + \langle x_1 - a_{1j} \rangle$. Then we get

$$J = \bigcap_{j_1, j_2} (J + \langle x_1 - a_{1j}, x_2 - a_{2j_2} \rangle).$$

By applying this process for all $i = 1, 2, \ldots, n$, we obtain the following:

$$J = \bigcap_{j_1, \ldots, j_n} (J + \langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n} \rangle).$$

Now we introduce a claim.

***Claim*:** $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is a maximal ideal of $\mathbb{K}[x_1, \ldots, x_n]$.

***Proof of Claim*:** Let $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Assume that I is included properly in J. Then there exists $g \in J \setminus I$. We want to show that I is maximal, therefore if we show that J is the whole ring, then we are done. We apply the division algorithm to f n times and we get $g = b_1(x_1 - a_1) + b_2(x_2 - a_2) + \ldots + b_n(x_n - a_n) + k$ where $b_1 \in \mathbb{K}[x_1, \ldots, x_n]$, $b_2 \in \mathbb{K}[x_2, \ldots, x_n]$, ..., $b_n \in \mathbb{K}[x_n]$, and $k \in \mathbb{K}$. Since g is not in I, $k \neq 0$. But we have $g \in J$, so k is in J. We know that $k \neq 0$, so $(1/k)k = 1 \in J$. Since J contains the identity, it is the whole ring. Thus, I is a maximal ideal.

By the above claim, we know that $\langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n} \rangle$ is a maximal ideal. Therefore, the ideal $J + \langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n} \rangle$ has to be equal to the ideal $\langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n} \rangle$ or the whole ring $\mathbb{C}[x_1, \ldots, x_n]$. Hence we conclude that J is a finite intersection of maximal ideals. We also know that a maximal ideal is a radical ideal and an intersection of radical ideals is again a radical ideal. Thus, we can get the result that J is radical.

Now it is left to show that $J = \sqrt{I}$ in order to complete the proof. Since $J = I + \langle p_{1,red}, \ldots, p_{n,red} \rangle$, we have $I \subset J$. In order to show that $J \subset \sqrt{I}$, we use the Strong Nullstellensatz. Consider the square-free part of the p_i which is $p_{i,red} \in J$. We know that $p_{i,red} = (x_i - a_{i1})(x_i - a_{i2}) \ldots (x_i - a_{id_i})$ where a_{ij} are distinct. Hence, $p_{i,red} \in J$ vanish at all points of $\mathbf{V}(I)$. It follows that $p_{i,red} \in \mathbf{I}\big(\mathbf{V}(I)\big)$. By the Strong Nullstellensatz, we get $p_{i,red} \in \sqrt{I}$. Therefore, we obtain

$$I \subset J \subset \sqrt{I}.$$

After taking the radicals, we get $\sqrt{I} = \sqrt{J}$. Since J is a radical ideal, we conclude that $\sqrt{I} = J$ as desired. Hence the following equality:

$$\sqrt{I} = I + \langle p_{1,red}, \ldots, p_{n,red} \rangle$$

holds. □

Proposition 3.3.4 ([**3, Page 235**]). *Let I be an ideal in $\mathbb{C}[x_1, \ldots, x_n]$ and $V = \mathbf{V}(I)$ be a finite set. Then*

(i) The cardinality of V is at most $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$ (where the "dim" refers dimension as a vector space over $\mathbb{C}$).

(ii) If I is a radical ideal, then the cardinality of V is equal to $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$, i.e., $|V| = \dim(\mathbb{C}[x_1, \ldots, x_n]/I)$.

Proof. We will begin by showing that the following claim holds:

***Claim*:** Let $p_1, \ldots, p_m$ be distinct points in $\in \mathbb{C}^n$. Then there is a polynomial $f_1 \in \mathbb{C}[x_1, \ldots, x_n]$ satisfying $f_1(p_1) = 1$ and $f_1(p_2) = \ldots = f_1(p_m) = 0$.

***Proof of Claim*:** We know that if $a \neq b \in \mathbb{C}^n$, then at least one component must be different in a and b. Let j denote the component at which a and b differ. Then define $g = \frac{x_j - b_j}{a_j - b_j}$ such that $g(a) = 1$ and $g(b) = 0$. Now by applying the same process to each pair $p_1 \neq p_i$ for $i \geq 2$, we obtain $g = \frac{x_j - p_{i_j}}{p_{1_j} - p_{i_j}}$ satisfying $g_i(p_1) = 1$ and $g_i(p_i) = 0$ for $i \geq 2$. Then define $f_1 = g_2 g_3 ... g_m$ which satisfies $f_1(p_1) = 1$ and $f_1(p_i) = 0$ for $i \geq 2$ as desired. Moreover, note that if we apply the same procedure to each pair $p_2 \neq p_i$ for $i = 1, 3, \ldots, m$, then we observe that $g_i(p_2) = 1$ and $g_i(p_i) = 0$, therefore $f_2(p_2) = 1$ and $f_2(p_i) = 0$ for $i = 1, 3, \ldots, m$. If we generalize this process to all $p_1, \ldots, p_m$, then we get $f_i(p_i) = 1$ and $f_i(p_j) = 0$ for $i \neq j$.

Now we will prove the first part of the proposition. Assume for distinct p_i that $V = \{p_1, p_2, \ldots, p_m\}$. Then we obtain that $f_i(p_i) = 1$ and $f_i(p_j) = 0$ for $i \neq j$. If we show that the elements $[f_1], \ldots, [f_m]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$ are linearly independent, then it will be shown that $m \leq \dim(\mathbb{C}[x_1, \ldots, x_n]/I)$ which means the cardinality of V is at most $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$. So let us show that $[f_1], \ldots, [f_m] \in \mathbb{C}[x_1, \ldots, x_n]/I$ are linearly independent. Assume that $\sum_{i=1}^{m} a_i[f_i] = [0]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$, where the a_i are in $\mathbb{C}$. Since $\sum_{i=1}^{m} a_i[f_i] = [0]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$, $\sum_{i=1}^{m} a_i f_i \in I \subset \mathbb{C}[x_1, \ldots, x_n]$. Let $g = \sum_{i=1}^{m} a_i f_i$. Since $g \in I$, and

$V = \mathbf{V}(I) = \{p_1, p_2, \ldots, p_m\}$, we get that $g(p_j) = 0$ for all $1 \leq j \leq m$. Thus, we obtain

$$0 = g(p_j) = \sum_{i=1}^{m} a_i f_i(p_j) = 0 + a_j f_j(p_j) = a_j \text{ for } 1 \leq j \leq m.$$

We have got that $a_j = 0$ for $1 \leq j \leq m$. Hence $[f_1], \ldots, [f_m] \in \mathbb{C}[x_1, \ldots, x_n]/I$ are linearly independent.

Now we will prove the second part. Assume that I is a radical ideal. Our goal is to prove that $m = \dim(\mathbb{C}[x_1, \ldots, x_n]/I)$. If we show that $[f_1], \ldots, [f_m]$ form a basis of $\mathbb{C}[x_1, \ldots, x_n]/I$, then the equality will follow. Since we have showed that $[f_1], \ldots, [f_m]$ are linearly independent, it is left to show that they span $\mathbb{C}[x_1, \ldots, x_n]/I$. Let $[g]$ be an arbitrary element of $\mathbb{C}[x_1, \ldots, x_n]/I$. Then let $g(p_i) = a_i$, and define $h = g - \sum_{i=1}^{m} a_i f_i$. Then we obtain,

$$h(p_j) = g(p_j) - \sum_{i=1}^{m} a_i f_i(p_j) = a_j - a_j f_j(p_j) = a_j - a_j = 0 \text{ for } 1 \leq j \leq m.$$

Since $h(p_j) = 0$ for all j, $h \in \mathbf{I}(V)$. Moreover, since $\mathbb{C}$ is algebraically closed, we can use the Strong Nullstellensatz and get that $\mathbf{I}(V) = \mathbf{I}\big(\mathbf{V}(I)\big) = \sqrt{I}$. We also know that I is a radical ideal, so we obtain $\mathbf{I}(V) = \sqrt{I} = I$ which implies that $h \in I$. Therefore, $[h] = [0]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$. Since $[h] = [0]$ and $h = g - \sum_{i=1}^{m} a_i f_i$, we get $[g] = \sum_{i=1}^{m} a_i [f_i]$. Hence, $[f_1], \ldots, [f_m]$ span $\mathbb{C}[x_1, \ldots, x_n]/I$ and this completes the proof. $\square$

Chapter 4

Encodings for Some Graph-Theoretical Problems

In this chapter, we discuss some encodings for some combinatorial problems such as graph k-colorability problem, Hamiltonian cycle problem, edge-chromatic number problem and planar graph problem. Before starting to present these encodings, we introduce some notation. For a graph G with n vertices, $V(G)$ denotes the set of vertices $i = 1, \ldots, n$. Similarly, $E(G)$ denotes the set of edges $\{i, j\}$ where $\{i, j\}$ is the edge connecting the vertices i, j. In addition, $Adj(i)$ denotes the set of vertices adjacent to the vertex i. Lastly, a graph is said to be simple if it is undirected, unweighed, and contains no loops or multiple edges.

4.1 Graph Colorability Problem

In graph colorability, the fundamental question is that if we have k colors and a graph G with n vertices, is it possible to color the vertices of G with k colors such that no adjacent vertices will have the same color. In this section, we present some encodings for graph k-colorability problem. For the details of the encodings presented here, you can see [8]. We first state the following lemma. This lemma

helps us to determine the number of distinct k-colorings in a given graph.

Lemma 4.1.1. *Let G be a graph having n vertices. For the graph G, let I be the ideal in $\mathbb{C}[x_1, \ldots, x_n]$ defined as:*

$$I = \left\langle x_1^k - 1, \ldots, x_n^k - 1, \underbrace{\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d}_{\{i,j\} \in E(G)} \right\rangle.$$

Then I is radical and $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$ equals to the number of points in $\mathbf{V}(I)$.

Proof. As wee can see, for each x_i, the square-free polynomial $x_i^k - 1$ is included in I. Then by the Proposition 3.3.3 in the previous chapter, we obtain that

$$\sqrt{I} = I + \langle x_1^k - 1, \ldots, x_n^k - 1 \rangle.$$

Since the ideal $\langle x_1^k - 1, \ldots, x_n^k - 1 \rangle$ is contained in I, we have $I + \langle x_1^k - 1, \ldots, x_n^k - 1 \rangle = I$. Hence, $\sqrt{I} = I$ which proves I is a radical ideal. Then by the Proposition 3.3.4 in the previous chapter, we get $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$ equals to the number of points in $\mathbf{V}(I)$. □

Now we are ready to introduce the encodings of graph k-colorability. We start with a degree-k encoding presented by Bayer in [12].

Theorem 4.1.2 (**Bayer**). *A graph G is k-colorable if and only if the below zero-dimensional polynomial equations system has a solution over $\mathbb{C}$. Additionally, the number of solutions is equal to $k!$ times the number of distinct k-colorings.*

$$x_i^k - 1 = 0, \text{ for every vertex } i \in V(G),$$

$$\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = 0, \text{ for every edge } \{i, j\} \in E(G).$$

Proof. Suppose that G is k-colorable. Then we know that there is a coloring satisfying no two vertices, which are adjacent, have the same color. Now let the k-colors be the k roots of unity. Thus, for the vertices i and j connected with an edge, the variable x_i is different from x_j. It is easy to see that the first equation (associated with the vertices), $x_i^k - 1 = 0$, holds since the k-colors are the k roots of unity. We also know that $\frac{x_i^k - x_j^k}{x_i - x_j} = \sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d$. Then we have $(x_i - x_j) \sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = x_i^k - x_j^k$. Since $x_i^k = 1$ and $x_j^k = 1$, we obtain $x_i^k - x_j^k = 0$. We also have that x_i is not equal to x_j, so we get $\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = 0$ which satisfies the second edge equation. Now suppose that the given system of equations has a solution. From the first vertex equation $x_i^k - 1 = 0$, the variable x_i is equal to one of the k roots of unity. To prove that no two adjacent vertices have the same color, we assume on the contrary that x_i and x_j, for adjacent vertices i and j, are equal to the same root of unity, say α. Then $\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = \sum_{d=0}^{k-1} \alpha^{k-1-d} \alpha^d = k\alpha^{k-1} \neq 0$. But, this contradicts with the edge equation $\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = 0$. Hence, every two adjacent vertices have different colors.

Since we have shown that if there is a k-coloring, the system of equations has a solution. In order to see that $k!$ times the number of distinct k-colorings is equal to the number of solutions, it is sufficient to show that the map between the k-colorings and solutions is bijective. Let us map the k colors to the k roots of unity. If the two colorings map to the same solution, then they are the same, which proves injectivity. The map is also surjective since we have shown that for every solution there is a k-coloring. Hence the map between the k-colorings and solutions is bijective. We also know that k roots of unity can be assigned with $k!$ ways with k colors. Therefore, the number of solutions equals to the $k!$ times the number of distinct k-colorings. □

The next lemma introduces a degree two encoding for the graph k-colorability.

Lemma 4.1.3. *A graph G is k-colorable if and only if the following zero-dimensional polynomial equations system:*

$$\left(\sum_{p=1}^{k} x_{ip}\right) - 1 = 0, \text{ for every vertex } i \in V(G),$$

$$x_{ip}x_{jp} = 0, \text{ for every edge } \{i,j\} \in E(G) \text{ and } p = 1, \ldots, k.$$

$$x_{ip}(x_{ip} - 1) = 0, \text{ for every edge } \{i,j\} \in E(G) \text{ and } p = 1, \ldots, k.$$

has a solution in the polynomial ring $\mathbb{C}[x_{ip}]$ with $1 \leq i \leq n$ and $1 \leq p \leq k$.

Proof. The idea used for proving this lemma is partitioning the graph G into k disjoint sets. Assume that G is k-colorable. Then let x_{is} be equal to 1 if the vertex i colored with the s^{th} color and let other x_{ip} be equal to 0. Hence both of the first equation $\left(\sum_{p=1}^{k} x_{ip}\right) - 1 = 0$, and the last equation $x_{ip}(x_{ip} - 1) = 0$ hold. Also, since G is k-colorable, there exists a coloring such that no two adjacent vertices have the same color which implies that no two adjacent vertices are included in the same partition. This proves the equation $x_{ip}x_{jp} = 0$. Now assume that the given system of polynomial equations has a solution. Clearly, the equation $x_{ip}(x_{ip}-1) = 0$ guarantees that x_{ip} is either 1 or 0. The equation $\left(\sum_{p=1}^{k} x_{ip}\right)-1 = 0$ also guarantees that x_{is} is equal to 1 if the vertex i colored with the s^{th} color and other x_{ip} are equal to 0. Thus, each vertex is included in just one partition. The equation $x_{ip}x_{jp} = 0$ also says that no two adjacent vertices are included in the same partition. Hence we can conclude that G is k-colorable since the mapping between partitions and vertices allows a k-coloring. □

Before giving the last encoding for this chapter, we state a remark.

Remark 4.1.4. *Let p and n be relatively prime. Then the polynomial equation $x^n - 1 = 0$ has n distinct roots over $\overline{\mathbb{F}_p}$.*

The next lemma presents the last encoding of graph k-colorability problem in this section which is over $\overline{\mathbb{F}_p}$. As you notice, the first encoding and this one differs only in polynomial ring they are over. The first one is over $\mathbb{C}$ and this one is over $\overline{\mathbb{F}_p}$.

Lemma 4.1.5. *Let k and p be relatively prime. Then a graph G is k-colorable if and only if the following zero-dimensional polynomial equations system:*

$$x_i^k - 1 = 0, \text{ for every vertex } i \in V(G),$$

$$\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = 0, \text{ for every edge } \{i,j\} \in E(G).$$

has a solution over $\overline{\mathbb{F}_p}$. Additionally, the number of solutions equals to $k!$ times the number of distinct k-colorings.

Proof. Proof is clear by Theorem 4.1.2 and the previous remark. □

4.2 Hamiltonian Cycle Problem

A cycle in a graph is said to be Hamiltonian, if it visits every vertex exactly once. We present three encodings in this section. The first one is for finding a cycle of length L, where L is an integer and the next one is for finding a Hamiltonian cycle in the graph G. The last encoding is again for finding a Hamiltonian cycle in the graph G. The difference between the last and second encodings is that second one is over $\mathbb{C}$ and last one is over $\overline{\mathbb{F}_p}$. For the details of these encodings, you may see [8].

Now we present the first encoding of this section.

Lemma 4.2.1. *There exists a cycle of length L in a simple graph G with n vertices if and only if the following zero-dimensional polynomial equations system:*

$$\left(\sum_{i=1}^{n} y_i \right) - L = 0,$$

$$y_i(y_i - 1) = 0,\ \prod_{s=1}^{n}(x_i - s) = 0,$$

$$y_i \prod_{j \in Adj(i)} (x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(L-1)) = 0.$$

has a solution over $\mathbb{C}$ *for every vertex* $i \in V(G)$.

Proof. Assume that there exists a cycle, denoted by C, with length L in the graph G. Then let y_i take the value 1 if the vertex i is in the cycle C, and 0 if it is not in the cycle C, i.e.,

$$y_i = \begin{cases} 0 & \text{if the vertex } i \text{ is not in } C \\ 1 & \text{if the vertex } i \text{ is in } C \end{cases}$$

Since y_i is either 1 or 0, the equation $y_i(y_i - 1) = 0$ is satisfied. Clearly, the first equation $\left(\sum_{i=1}^{n} y_i\right) - L = 0$ is also satisfied. Now numerate every vertex in the cycle C. Note that we can begin this numerating process from any vertex. Then assign $x_i = j$ if the vertex i of the graph G is the j-th vertex of the cycle C. Hence, the equation $\prod_{s=1}^{n} x_i - s = 0$ is also satisfied since j takes one of the values between 1 and n. Additionally, x_i could be assigned to any value from $1, 2, \ldots, n$ if the vertex i is not contained in the cycle C. Now it is left to verify the last equation. We know that the vertex i of G is the j-th vertex of C. So one of the vertices adjacent to i must be the $(j+1)$-th vertex of C. Let this vertex be the k-th vertex of the graph G. As we know, $x_i = j$, so $x_k = j + 1$. Since the cycle C has length L, j must be less or equal to L. In the former case ($j < L$), the factor $(x_i - y_k x_k + y_k)$ becomes $x_i - x_k + 1$ since k is contained in C which implies $y_k = 1$. $x_i - x_k + 1$ is equal to $j - (j+1) + 1$ which is zero. Thus if $j < L$, the last equation is satisfied. In the latter case ($j = L$), i is the last vertex of C, so the following vertex, k, must be the first vertex of C. Therefore, $x_i = j = L$, and $x_k = 1$. Then the factor $(x_i - y_k x_k - y_k(L-1))$ becomes $L - 1 - (L-1)$ which is zero. Hence, if $j = L$, the last equation is also satisfied. Now consider all of the other vertices i of G which are not in the cycle C. As you remember, we assign $y_i = 0$, if i is not in the cycle, so the last equation is automatically zero in this case.

Conversely, assume that the given system of polynomial equations has a solution. From the equation $y_i(y_i - 1) = 0$, clearly y_i takes the values either 0 or 1. Also from the first equation $\left(\sum_{i=1}^{n} y_i\right) - L = 0$, there are L many variables y_i which are equal to 1. Let these vertices i, which are associated with these variables $(y_i = 1)$ constitute the set C. In other words, C contains the vertices i of the graph G such that $y_i = 1$. Our claim is that C is a cycle of length of L. Since we assumed that C contains the vertices i with $y_i = 1$, we will not deal with the case $y_i = 0$. From the last equation $y_i \prod_{j \in Adj(i)} (x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(L-1)) = 0$, we obtain that either $(x_i - y_j x_j + y_j)$, or $(x_i - y_j x_j - y_j(L-1))$ must be zero. Note that for every j in C, these equations reduce to the forms $x_i - x_j + 1$ and $(x_i - x_j - (L-1))$. Therefore, we have either $x_j = x_i + 1$, or $x_j = x_i - L + 1$. Note that $x_j = x_i + 1$ tells us that the vertex i is adjacent to the vertex j. Now let x_{i_1} be the variable in C which takes the smallest value. In this case, x_{i_1} cannot be adjacent to $x_j = x_{i_1} - L + 1$ since L is the length of C which means L is the largest value that x_{i_k} can take (If x_{i_1} is adjacent to $x_j = x_{i_1} - L + 1$, then it would not be the smallest in the cycle C). Therefore x_{i_1} must be adjacent to $x_j = x_{i_2}$ (the next highest value), i.e., $x_{i_1} + 1 = x_{i_2} = x_j$. This condition satisfies for all $x_{i_1}, x_{i_2}, \ldots, x_{i_{L-1}}$, except for the last element x_{i_L}. Thus, x_{i_L} must be equal to the highest value (which is L) of all values in C. Hence it should be adjacent to the variable $x_j = x_{i_L} - L + 1$. The only variable holding this condition is the smallest value x_{i_1}. Thus, C forms a cycle of length L in C. □

Lemma 4.2.2. *There exists a Hamiltonian cycle in a graph G with n vertices if and only if the following zero-dimensional polynomial equations system:*

$$\prod_{s=1}^{n} (x_i - s) = 0, \text{ for every vertex } i \in V(G),$$

$$\prod_{j \in Adj(i)} (x_i - x_j + 1)(x_i - x_j - (n-1)) = 0, \text{ for every vertex } i \in V(G).$$

has a solution over $\mathbb{C}$. Additionally, the number of solutions divided by $2n$ is equal to the number of distinct Hamiltonian cycles in G.

Proof. Note that if we have all y_i (in the previous lemma) assigned to the value 1, then we obtain the system of equations in this lemma. Note also that since

we are looking for a Hamiltonian cycle in this lemma, all vertices of the graph G must be included in the cycle. Therefore, all y_i from the previous lemma have to be assigned to 1 in this case. Thus, if we take L (length of the cycle in the previous lemma) equal to n, first part of the proof will be the same as in the previous lemma. Now it is left to show that the number of Hamiltonian cycles in G is equal to the number of solutions divided by $2n$. We know that there are n vertices in every Hamiltonian cycle of G. We can pick any of these n vertices as the starting vertex of the cycle. So there are n ways to pick the starting vertex. In each cycle, after picking the starting vertex, we have two possible directions to go and pick the second vertex of the cycle. Hence the number of Hamiltonian cycles in G is equal to the number of solutions divided by $2n$. □

Lemma 4.2.3. *There exists a Hamiltonian cycle in a connected graph G with n vertices if and only if the following zero-dimensional polynomial equations system:*

$$x_i^n - 1 = 0, \text{ for every vertex } i \in V(G),$$

$$\prod_{j \in Adj(i)} (wx_i - x_j) = 0, \text{ for every vertex } i \in V(G).$$

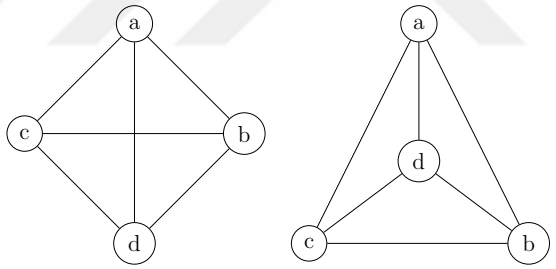
has a solution over $\overline{\mathbb{F}_p}$, where n and p are relatively prime, and w is an n^{th} primitive root of unity.

Proof. Assume that the graph G has a Hamiltonian cycle, say, $i_1, i_2, \ldots, i_n$. Next, set variables associated with the vertices as powers of w, i.e., $x_{i_1} = w, x_{i_2} = w^2, \ldots, x_{i_n} = w^n = 1$. As you notice, for all $i \in V(G)$, the first equation $x_i^n - 1 = 0$ holds. For two adjacent vertices i_k and i_{k+1} in the Hamiltonian cycle, we know that if $x_{i_k} = w^s$, then $x_{i_{k+1}} = w^{s+1}$. Therefore, the expression $wx_{i_k} - x_{i_{k-1}}$ becomes $ww^s - w^{s+1}$ which is equal to zero. Hence the last equation $\prod_{j \in Adj(i)} (wx_i - x_j) = 0$, for all $i \in V(G)$, is also satisfied. Conversely, assume that the system of equations has a solution, and w is an n^{th} primitive root of unity. By the equation $x_i^n - 1 = 0$, we get every variable x_i $\big($associated with the vertex $i \in V(G)\big)$ is equal to a root of unity. From the last equation $\prod_{j \in Adj(i)} (wx_i - x_j) = 0$, we obtain $x_j = wx_i$ for vertices j which are adjacent to the vertex i for every $i \in V(G)$. We have n vertices in total, so there must be a variable which equals

to $w^n = 1$. Since we already have $x_j = wx_i$ for vertices j which are adjacent to the vertex i for every $i \in V(G)$, the vertex associated with the variable that is assigned to w^n must be adjacent to the vertex associated with the variable w. Therefore, if we assign the values $w, w^2, \ldots, w^n = 1$ to the variables $i_1, i_2, \ldots, i_n$ respectively, we obtain a Hamiltonian cycle in the graph G passing through the vertices $i_1, i_2, \ldots, i_n$ respectively. □

4.3 Graph Planarity Problem

A graph is said to be a planar graph if it can be drawn on the plane such that no two edges intersect with each other. One example of planar graphs is the following complete graph K_4:



(a) (b)

Figure 4.1: Complete Graph K_4

As you notice, drawing of K_4 in (b) satisfies the properties of a planar graph.

In this section we introduce two encodings. First one will be for testing the poset (partially ordered set) dimension of a poset P. The next one will be for determining whether a given graph G has a planar subgraph. As in the previous sections, you can find the details of these encodings in [8]. Before presenting these encodings we first give some definitions, and introduce the Schnyder's Theorem in [13] about graph planarity.

Definition 4.3.1. *A partial order is a binary relation $\leq$ on a set, which satisfies reflexivity, antisymmetry, and transitivity.*

A set P with partial order is called as a partially ordered set (poset).

Definition 4.3.2 (**Linear Extension**)**.** *A linear extension, for a partially ordered set P with n elements, is an order preserving bijection $l : P \to \{1, 2, \ldots, n\}$.*

Definition 4.3.3. *The dimension of a partially ordered set P is the smallest integer t for which there is a set of t linear extensions $l_1, \ldots, l_t$ for the poset P, provided that $x < y$ in P if and only if $l_i(x) < l_i(y)$ for every l_i.*

Definition 4.3.4 (**Incidence Poset**)**.** *Let G be a graph. The incidence poset of G, denoted by $P(G)$, is the partially ordered set which takes $V(G) \cup E(G)$ as its ground set, with the property that $x < y$ in $P(G)$ if y is incident to x, where x denotes a vertex and y denotes an edge in G.*

Example: The following figure shows the planar triangle graph G (left figure) and its incidence poset $P(G)$ (right figure).

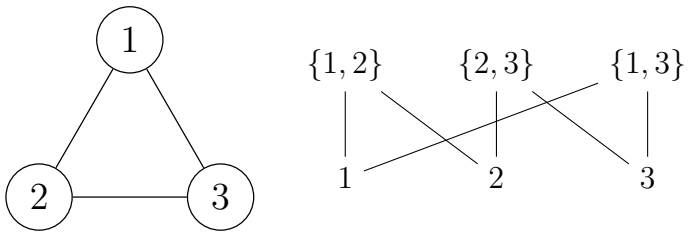


Figure 4.2: Triangle Graph G and Incidence Poset $P(G)$

Three linear extensions corresponding to incidence poset $P(G)$ are:

- $1 < 2 < \{1, 2\} < 3 < \{2, 3\} < \{1, 3\}$
- $2 < 3 < \{2, 3\} < 1 < \{1, 2\} < \{1, 3\}$
- $3 < 1 < \{1, 3\} < 2 < \{2, 3\} < \{1, 2\}$

Theorem 4.3.5 (**Schnyder [13]**)**.** *Let G be a graph. The graph G is planar if and only if the incidence poset $P(G)$ has a poset dimension at most 3.*

Now we are ready to present the fist result of this section which tests the poset dimension of a given poset P. Once we obtain the dimension of P, we will be able to conclude whether a given graph is planar or not by checking the dimension of the associated poset of that graph with the help of Schnyder's theorem given in the previous page.

Lemma 4.3.6. *Let $P = (E, >)$ be a poset. Let $\mathbb{C}[x_{\{i\}k}, \Delta_{\{ij\}k}, s_k]$ be a polynomial ring with $p|E| + p(|E|^2 - |E|) + p$ variables where $1 \leq i, j \leq |E|$, $i \neq j$, and $1 \leq k \leq p$. Then the poset dimension of P is at most p if and only if the below polynomial equations system has a solution over $\mathbb{C}$.*

For $k = 1, 2, \ldots, p$ and for every $i \in 1, \ldots, |E|$:

$$\prod_{s=1}^{|E|} (x_{\{i\}k} - s) = 0, \tag{4.1}$$

$$s_k \left(\prod_{1 \leq i < j \leq |E|} (x_{\{i\}k} - x_{\{j\}k}) \right) - 1 = 0. \tag{4.2}$$

For every ordered pair of comparable elements $e_i > e_j$ in poset P, and $k = 1, 2, \ldots, p$:

$$x_{\{i\}k} - x_{\{j\}k} - \Delta_{\{ij\}k} = 0. \tag{4.3}$$

For every ordered pair of incomparable elements in poset P:

$$\prod_{k=1}^{p} (x_{\{i\}k} - x_{\{j\}k} - \Delta_{\{ij\}k}) = 0, \ \prod_{k=1}^{p} (x_{\{j\}k} - x_{\{i\}k} - \Delta_{\{ji\}k}) = 0 \tag{4.4}$$

For every pair $\{i, j\}$ in $\{1, \ldots, |E|\}$, $k = 1, 2, \ldots, p$, and $\Delta(\Delta_{\{ij\}k}, \Delta_{\{ji\}k})$:

$$\prod_{d=1}^{|E|-1} (\Delta - d) = 0 \tag{4.5}$$

Proof. Assume that the given system of equations has a solution. Let the variable $x_{\{i\}k}$ denote the value of the poset element e_i in the k^{th} linear extension l_k, i.e.,

$l_k(e_i)$. From the equation 4.5, we obtain that $\Delta \in \{1, 2, \ldots, |E| - 1\}$ which are positive. The equations 4.1, and 4.2 guarantees that each $x_{\{i\}k}$ take distinct values between 1 and $|E|$. This means that poset elements are assigned to different values from 1 to $|E|$. From the equation 4.3, we get $x_{\{i\}k} > x_{\{j\}k}$ for every comparable elements $e_i > e_j$ in P. Hence the first three equations (4.1, 4.2, 4.3) satisfy the linear extension properties. Since these equations are reiterated p times (since $k = 1, 2, \ldots, p$), there are p linear extensions. Moreover, the equation 4.4 provides for incomparable elements in P that $x_{\{i\}l} > x_{\{j\}l}$ (and $x_{\{j\}l} \not> x_{\{i\}l}$) in one extension ($l^{th}$ extension in this case), while $x_{\{j\}t} > x_{\{i\}t}$ in another extension (t^{th} extension). Thus, the incomparable pair of elements can be detected by at least two of the p linear extensions. It follows that the intersection of all p linear extensions is equal to the poset P. We know that the dimension of a poset P is the smallest integer t for which there is a set of t linear extensions $\{l_i\}_1^t$ such that the intersection of these t linear extensions is equal to the poset P. Therefore, the dimension of the poset P is at most p. Conversely, assume that the dimension of the poset P is at most p. So there are at most p linear extensions $\{l_t\}_{t \leq p}$ such that the intersection of these t linear extensions is equal to the poset P. Let the variable $x_{\{i\}k}$ denote the value of the poset element e_i in the k^{th} linear extension l_k. Since the poset P has $|E|$ elements, each $x_{\{i\}k}$ must take distinct values from $\{1, 2, \ldots, |E|\}$. Thus the equations 4.1, and 4.5 are satisfied. Since a linear extension is an order preserving bijection, the equations 4.2, and 4.3 are also satisfied. We know for an incomparable pair of elements in a poset P that $x_{\{i\}l} > x_{\{j\}l}$ in an extension, while $x_{\{j\}t} > x_{\{i\}t}$ in another extension. The equation 4.4 tells exactly this, so it is also satisfied. □

The next lemma tests whether a given simple graph has a planar subgraph.

Lemma 4.3.7. *Let $G(V, E)$ be a simple graph with n vertices and m edges and $\mathbb{C}[z_{ij}, x_{\{i\}k}, y_{\{ij\}k}, \Delta_{\{ij,i\}k}, \Delta_{\{ij,uv\}k}, s_k]$ be a polynomial ring in $(m + 3(2m + m(m-1)) + m + n + 1)$ variables where $1 \leq i \leq n$, $k = 1, 2, 3$, and $\{i, j\}, \{u, v\} \in E(G)$. Then G has a planar subgraph with K edges if and only if the following polynomial equations system has a solution over $\mathbb{C}$.*

For every edge $\{i,j\} \in E(G)$*:*

$$z_{ij}^2 - z_{ij} = 0, \text{ and } \left(\sum_{\{i,j\} \in E(G)} (z_{ij}) \right) - K = 0. \tag{4.6}$$

For every vertex $i \in V(G)$*, every edge* $\{i,j\} \in E(G)$*, and for* $1 \leq k \leq 3$*:*

$$\prod_{s=1}^{n+m} (x_{\{i\}k} - s) = 0, \quad \prod_{s=1}^{n+m} (y_{\{ij\}k} - s) = 0, \tag{4.7}$$

$$s_k \left(\prod_{i<j} (x_{\{i\}k} - x_{\{j\}k}) \prod_{\{u,v\} \in E(G)} (x_{\{i\}k} - y_{\{uv\}k}) \prod_{\{i,j\},\{u,v\} \in E(G)} (y_{\{ij\}k} - y_{\{uv\}k}) \right) = 1.$$

For $1 \leq k \leq 3$*, and for every pair of vertex* $i \in V(G)$ *and edge* $\{i,j\} \in E(G)$*:*

$$z_{ij}(y_{\{ij\}k} - x_{\{i\}k} - \Delta_{\{ij,i\}k}) = 0. \tag{4.8}$$

For every pair of vertex $i \in V(G)$ *and edge* $\{u,v\} \in E(G)$ *which is not incident on* i*:*

$$z_{uv} \prod_{k=1}^{3} (y_{\{uv\}k} - x_{\{i\}k} - \Delta_{\{uv,i\}k}) = 0, \tag{4.9}$$

$$z_{uv} \prod_{k=1}^{3} (x_{\{i\}k} - y_{\{uv\}k} - \Delta_{\{i,uv\}k}) = 0.$$

For every pair of edges $\{i,j\}, \{u,v\} \in E(G)$ *(It is not important if they share a vertex as the endpoint or not):*

$$z_{ij} z_{uv} \prod_{k=1}^{3} (y_{\{ij\}k} - y_{\{uv\}k} - \Delta_{\{ij,uv\}k}) = 0, \tag{4.10}$$

$$z_{uv} z_{ij} \prod_{k=1}^{3} (y_{\{uv\}k} - y_{\{ij\}k} - \Delta_{\{uv,ij\}k}) = 0.$$

For every pair of vertices $i, j \in V(G)$ (It is not important if they are adjacent or not):

$$\prod_{k=1}^{3} (x_{\{i\}k} - x_{\{j\}k} - \Delta_{\{ij\}k}) = 0, \tag{4.11}$$

$$\prod_{k=1}^{3} (x_{\{j\}k} - x_{\{i\}k} - \Delta_{\{ji\}k}) = 0.$$

For every Δ $\big(\Delta_{\{ij,i\}k}, \Delta_{\{uv,i\}k}, \Delta_{\{i,uv\}k}, \Delta_{\{ij,uv\}k}, \Delta_{\{uv,ij\}k}, \Delta_{\{ij\}k}, \Delta_{\{ji\}k}\big)$*:*

$$\prod_{d=1}^{n+m-1} (\Delta - d) = 0. \tag{4.12}$$

Proof. Assume that the above system of equations has a solution. Let z_{ij} denote the variable associated with the edge $\{i, j\}$. Equation 4.6 guarantees that the variable z_{ij} is either equal to 0 or 1, and there are K many z_{ij} that are equal to 1. Suppose that these K edges $\{i, j\}$ with $z_{ij} = 1$ form a subgraph of G. We will show that this subgraph, say G', of G with K edges is planar. Recall that Schnyder's theorem (4.3.5) states that a graph is planar if the dimension of the incidence poset of that graph is at most 3. Therefore, we need to show that the incidence poset of the subgraph G' has dimension at most 3 to get that G' is planar. Recall also that we have vertices and edges in the incidence poset of G'. As in the proof of previous lemma, let the variable $x_{\{i\}k}$ denote the value of the poset element i (vertex) in the k^{th} linear extension l_k. Since we also have edges as poset elements, let $y_{\{ij\}k}$ denote the value of the edge $\{i, j\}$ of the incidence poset of G' in the k^{th} linear extension l_k. By applying the same process as in the proof of the previous lemma, we obtain that the dimension of the incidence poset is at most 3 (p -in the previous lemma- is 3 in this case since $k \in \{1, 2, 3\}$). Hence the subgraph G' is planar. Conversely assume that G has a planar subgraph, say G', with K edges. Then from the Schnyder's theorem, the dimension of the incidence poset of G' is at most 3. Now let z_{ij} denote the variable associated with the edge $\{i, j\}$ in G. Assign the value 1 to the K edges of the subgraph G', and 0 to the other edges of G. So the first equations (4.6) are satisfied. Suppose also that

the variable $x_{\{i\}k}$ denotes the value of the poset element i ($i \in V(G')$), and $y_{\{ij\}k}$ denotes the value of the edge $\{i, j\}$ of the incidence poset of G' in the k^{th} linear extension l_k where $k \in \{1, 2, 3\}$. Again, if we follow the same procedure as in the proof of the previous lemma, we see that all the equations are satisfied. □

4.4 Edge-Chromatic Number Problem

The minimum number of colors which are needed to color all of the edges of a graph G where no edges incident on the same vertex will have the same color is said to be the edge-chromatic number of G, which is denoted by $\chi'(G)$.

Definition 4.4.1. *The degree of a vertex in a graph is the number of edges which are incident on that vertex.*

Clearly, the edge-chromatic number of a graph G can be at least the highest vertex degree of G which is denoted by $\Delta(G)$. Moreover, Vizing's theorem ([14], Theorem 7.6.5) states that the edge-chromatic number can be at most $\Delta(G)+1$. Therefore, we can conclude that the edge-chromatic number is either $\Delta(G)$ or $\Delta(G)+1$. In this section, we introduce an encoding to determine whether the given graph G has the edge-chromatic number Δ which is the highest vertex degree of the graph G. For the details, yo can see [8].

Lemma 4.4.2. *Let Δ be the highest vertex degree of a simple graph G. G has edge-chromatic number Δ if and only if the following zero-dimensional polynomial equations system has a solution.*

$$s_i\left(\prod_{\substack{j,k\in Adj(i)\\ j<k}}(x_{ij}-x_{ik})\right)-1=0,\ \textit{for every vertex } i\in V(G),$$

$$x_{ij}^{\Delta}-1=0,\ \textit{for every edge } \{i,j\}\in E(G).$$

Proof. Assume that G has edge-chromatic number Δ. Then assign Δ colors to the Δ roots of unity. Clearly, the second equation, $x_{ij}^{\Delta}-1=0$, holds. Since G has

an edge-chromatic number, no two edges incident on the same vertex are colored with the same color. Then we get $x_{ij} \neq x_{ik}$ where $j, k \in Adj(i)$. Thus, the first equation $s_i\left(\prod_{j,k\in Adj(i),j<k}(x_{ij} - x_{ik})\right) - 1 = 0$ can also be satisfied by choosing an appropriate s_i. Now assume that the given system of polynomial equations has a solution. Then the second equation guarantees that the variables x_{ij} take values of Δ roots of unity. Then by the first equation, we see that $x_{ij} \neq x_{ik}$ where $j, k \in Adj(i)$ which means that no two edges, which are incident on the same vertex, are colored with the same color. Moreover, since Δ is the highest vertex degree in G, we know that the edge-chromatic number can be at least Δ (We also know that it can be either Δ or Δ+1, by the Vizing's Theorem). Since we have Δ roots of unity by the second equation, the edge-chromatic number must be equal to exactly Δ. Hence G has edge-chromatic number Δ as desired. □

Note also that if the given polynomial equations system has no solution, then the graph G has edge-chromatic number $\Delta + 1$ since the Vizing's theorem says that the edge-chromatic number of a graph could be either Δ, or $\Delta(G) + 1$.

Chapter 5

Groebner Basis Methods in Graph Colorability and Hamiltonian Cycle Problems

Groebner bases are very useful to determine whether a system of polynomial equations has a solution, or whether a combinatorial problem encoded by a system of polynomial equations is feasible/infeasible over a given field. In this chapter, we inspect the graph-coloring encoding, and Hamiltonian cycle encoding over $\mathbb{C}$ presented in chapter 4 (Lemma 4.1.2, and Lemma 4.2.2).

Our first combinatorial problem is graph-colorability. After some preliminary results, we will determine whether a given graph is 3-colorable or not over $\mathbb{C}$ by using Groebner basis.

5.1 Graph Colorability

Recall that the encodings stated in Lemma 4.1.2, and 4.1.5 say that a given graph is k-colorable if and only if the given system of polynomial equations has a solution

over $\mathbb{C}$, and $\overline{\mathbb{F}_p}$ respectively, where p, k are relatively prime. By the Theorem 3.2.1 (Another form of the Hilbert's Nullstellensatz), we know that the given system of polynomial equations $f_1 = f_2 = \ldots = f_s = 0$ has no solution if and only if $\sum_{i=1}^{s} \beta_i f_i = 1$ with $\beta_1, \beta_2, \ldots, \beta_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is an algebraically closed field. Thus, we can say that graphs encoded by the systems given in Lemma 4.1.2, and 4.1.5 are k-colorable, if 1 is not in the ideal generated by the polynomials in those encodings.

Recall also that the polynomial system given in the Lemma 4.1.2, and 4.1.5 is the following:

$$x_i^k - 1 = 0, \text{ for every vertex } i \in V(G),$$

$$\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = 0, \text{ for every edge } \{i, j\} \in E(G).$$

Now we summarize all we said up to now in a proposition.

Proposition 5.1.1. *A graph G is k-colorable if and only if the identity 1 is not in the graph k-coloring ideal $I_{G,k} \subset \mathbb{C}[x_i \mid i \in V(G)]$ which is generated by the polynomials $x_i^k - 1$ for every vertex $i \in V(G)$, and $\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d$ for every edge $\{i, j\} \in E(G)$.*

In other words, A graph G is k-colorable if and only if the following graph k-coloring ideal:

$$I_{G,k} = \left\langle x_i^k - 1, \sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d \right\rangle$$

is proper.

Proof. Assume that the graph k-coloring ideal $I_{G,k}$ does not contain the identity 1. Then $I_{G,k}$ is proper, and by Hilbert's Weak Nullstellensatz (Theorem 3.1.7)

(Note that we can apply the Hilbert's Nullstellensatz since $\mathbb{C}$ is algebraically closed.), we conclude that $\mathbf{V}(I_{G,k}) \neq \emptyset$. Note that $\mathbf{V}(I_{G,k})$ contains the solutions of the system $x_i^k - 1 = 0$ for every vertex $i \in V(G)$, and $\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = 0$ for every edge $\{i, j\} \in E(G)$. By Lemma 4.1.2, we know that solutions of the system of polynomial equations corresponds to valid k-colorings. Hence, $\mathbf{V}(I_{G,k})$ includes all of the valid k-colorings, which implies that G is k-colorable. Conversely, assume that G is k-colorable. Then it is certain that there exists a k-coloring of the graph G. Since all of the valid k-colorings are included in $\mathbf{V}(I_{G,k})$, $\mathbf{V}(I_{G,k})$ is non-empty. Then again by Hilbert's Weak Nullstellensatz (Theorem 3.1.7), $I_{G,k}$ is proper which also implies $I_{G,k}$ does not contain the identity 1. □

The following example shows that the given graph is 3-colorable.

Example: Consider the following graph G, with 5 vertices and 6 edges. We will check that whether G is 3-colorable or not over $\mathbb{C}$.

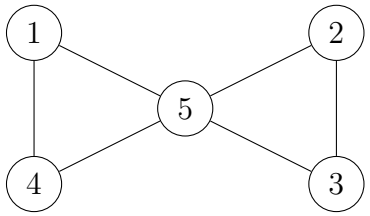


Figure 5.1

Note that if we color the vertex 1 and 2 with red, vertex 3 and 4 with blue, and vertex 5 with green, then we can easily see that this graph is 3-colorable. However, determining the colorability of a given graph is not as easy as in this example when there are many vertices and edges in the graph. Therefore, in order to conclude that a graph is k-colorable, for some k, we can utilize Groebner bases.

In order to check the 3-colorability of this graph G, we first form the graph 3-coloring ideal. We know that (by the previous proposition) the graph k-coloring ideal is generated by the polynomials $x_i^k - 1$ for every vertex $i \in V(G)$, and

$\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d$ for every edge $\{i,j\} \in E(G)$. Thus, in our case the graph 3-coloring ideal $I_{G,3} \in \mathbb{C}[x_1, x_2, \ldots, x_5]$ is generated by $x_i^3 - 1$ for $i = 1,2,3,4,5$ and $x_i^2 + x_i x_j + x_j^2$ for edges $\{1,4\},\{1,5\},\{4,5\},\{2,3\},\{2,5\},\{3,5\}$. Then we compute the Groebner basis of the ideal $I_{G,3}$. By using the computer algebra software CoCoA [15], we find the reduced Groebner basis G' of $I_{G,3}$ with respect to the lexicographic order as the following:

$$G' = \{x_5^3 - 1, x_4^2 + x_4 x_5 + x_5^2, x_3^2 + x_3 x_5 + x_5^2, x_2 + x_3 + x_5, x_1 + x_4 + x_5\}.$$

Since the reduced Groebner basis of $I_{G,3}$ is not $\{1\}$, $\mathbf{V}(I) \neq \emptyset$, and hence $I_{G,3}$ is a proper ideal by the Hilbert's Nullstellensatz. Since $I_{G,3}$ is proper, graph G is 3-colorable by Proposition 5.1.1.

Now we will find how many distinct 3-colorings there are for the graph G. Recall that Lemma 4.1.5 also states that the number of distinct k-colorings is equal to the number of solutions (of the given system) divided by $k!$. Thus, we first need to find the number of solutions of the system $x_i^k - 1 = 0$ for every vertex $i \in V(G)$, and $\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = 0$ for every edge $\{i,j\} \in E(G)$. Since solutions of that system are the elements of $\mathbf{V}(I_{G,3})$, it is enough to find the cardinality of $\mathbf{V}(I_{G,3})$. Recall also that Lemma 4.1.1, states that $\dim(\mathbb{C}[x_1, \ldots, x_n]/I) = |\mathbf{V}(I)|$ for the ideal $I = \left\langle x_1^k - 1, \ldots, x_n^k - 1, \sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d \right\rangle$ in $\mathbb{C}[x_1, \ldots, x_n]$. As you can easily notice, this ideal I is the same as the graph k-coloring ideal $I_{G,k}$ for k-colorability. Therefore, when we compute $\dim(\mathbb{C}[x_1, \ldots, x_n]/I_{G,k})$ for $k = 3$, and $n = 5$, we obtain the number of solutions for the graph G.

By the software system CoCoA [15], we find that $\dim(\mathbb{C}[x_1, \ldots, x_5]/I_{G,3}) = |\mathbf{V}(I_{G,3})| = 12$. Hence, there are 12 solutions of the system $x_i^3 - 1 = 0$ for $i = 1,2,3,4,5$ and $x_i^2 + x_i x_j + x_j^2 = 0$ for edges $\{1,4\},\{1,5\},\{4,5\},\{2,3\},\{2,5\},\{3,5\}$.

Note also that the number of monomials that are not contained in the leading term ideal of $I_{G,3}$ equals to $\dim(\mathbb{C}[x_1, \ldots, x_5]/I_{G,3})$. Thus, we can find $\dim(\mathbb{C}[x_1, \ldots, x_5]/I_{G,3}) = |\mathbf{V}(I_{G,3})|$ by examining the Groebner basis for

the ideal $I_{G,3}$ since the leading terms of the Groebner basis elements generate the leading term ideal of $I_{G,3}$. In this example, the leading term ideal is $\langle LT(I_{G,3})\rangle = \langle x_5^3, x_4^2, x_3^2, x_2, x_1\rangle$. Hence the number of points in $\mathbf{V}(I_{G,3})$ is $3 \times 2 \times 2 \times 1 \times 1 = 12$.

The 12 solutions (valid 3-colorings) are shown below:

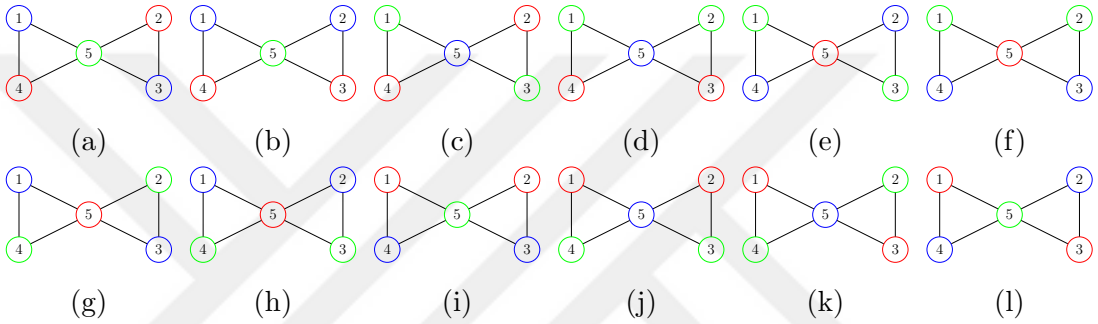


Figure 5.2: Valid 3-colorings

Recall that we assign k roots of unity as colors for graph-coloring (Lemma 4.1.2). Clearly, we may assign k roots of unity to k colors in $k!$ ways. Since we check 3-colorability in this example, $\zeta, \zeta^2, 1$ are the cubic roots of unity, where $\zeta = e^{\frac{2\pi i}{3}}$ and let *green*, *red*, *blue* be the 3 colors. Then the assignment between the cubic roots of unity and colors can be done as shown below:

$$
\begin{aligned}
&green \to \zeta^2 \quad red \to \zeta \quad blue \to 1,\\
&green \to \zeta^2 \quad red \to 1 \quad blue \to \zeta,\\
&green \to \zeta \quad red \to \zeta^2 \quad blue \to 1,\\
&green \to \zeta \quad red \to 1 \quad blue \to \zeta^2,\\
&green \to 1 \quad red \to \zeta \quad blue \to \zeta^2,\\
&green \to 1 \quad red \to \zeta^2 \quad blue \to \zeta.
\end{aligned}
$$

As we have previously shown, we have 12 valid 3-colorings. Since $k = 3$, we can assign 3 colors to the 3 roots of unity in 6 ways, and hence we have 2 distinct 3-colorings for the graph G in Figure 5.1 by Lemma 4.1.2. Note that in Figure

5.2, the 3-colorings (a), (c), (e), (g), (k), (l) are the same, and (b), (d), (f), (h), (i), (j) are the same different than the first 6 ones.

The next example shows a non-3-colorable graph. Again we exploit the Groebner bases and use the Proposition 5.1.1 to determine that the following graph is non-3-colorable.

Example: Consider the following graph G with 6 vertices and 10 edges:

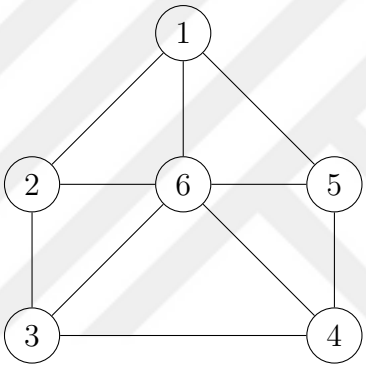


Figure 5.3

We first construct the graph 3-coloring ideal $I_{G,3}$ of $\mathbb{C}[x_1, x_2, \ldots, x_6]$. The graph 3-coloring ideal is generated by $x_i^3 - 1$ for $i = 1, 2, 3, 4, 5, 6$ and $x_i^2 + x_i x_j + x_j^2$ for edges $\{1,2\}, \{1,5\}, \{1,6\}, \{2,3\}, \{2,6\}, \{3,4\}, \{3,6\}, \{4,5\}, \{4,6\}, \{5,6\}$. Then we compute the reduced Groebner basis of the ideal $I_{G,3}$ with respect to the lexicographic order, and we find that the reduced Groebner basis of $I_{G,3}$ as $\{1\}$ which implies $\mathbf{V}(I_{G,3}) = \emptyset$. Therefore, by Proposition 5.1.1, we conclude that the graph G is not 3-colorable over $\mathbb{C}$.

In the next subsection, we will investigate the Hamiltonian cycle problem.

5.2 Hamiltonian Cycle

In this section we will seek an answer whether there exists a Hamiltonian cycle in a given graph. Since the Hamiltonian cycle problem is encoded by a system of polynomial equations, we can still benefit from Groebner bases to see the existence of a Hamiltonian cycle in the given graph.

Recall that Lemma 4.2.2 states that there exists a Hamiltonian cycle in a given graph if the following system of polynomial equations has a solution over $\mathbb{C}$.

$$\prod_{s=1}^{n} x_i - s = 0, \text{ for every vertex } i \in V(G),$$

$$\prod_{j \in Adj(i)} (x_i - x_j + 1)(x_i - x_j - (n-1)) = 0, \text{ for every vertex } i \in V(G).$$

Similar to the process we followed in the Graph Colorability section (Section 5.1), by the Theorem 3.2.1, we can write the following proposition:

Proposition 5.2.1. *There exists a Hamiltonian cycle in a graph G having n vertices if and only if the identity 1 is not in the Hamiltonian cycle ideal in $\mathbb{C}[x_1, \ldots, x_n]$, which is denoted by I_{HC} and generated by the polynomials $\prod_{s=1}^{n} x_i - s$, and $\prod_{j \in Adj(i)} (x_i - x_j + 1)(x_i - x_j - (n-1))$ for each vertex $i \in V(G)$.*

In other words, there exists a Hamiltonian cycle in a graph G if and only if the following Hamiltonian cycle ideal

$$I_{HC} = \left\langle \prod_{s=1}^{n} x_i - s, \prod_{j \in Adj(i)} (x_i - x_j + 1)(x_i - x_j - (n-1)) \right\rangle$$

is proper.

Proof. Assume that there exists a Hamiltonian cycle in a graph G with n vertices. Then by Lemma 4.2.2, the polynomial equations system $\prod_{s=1}^{n} x_i - s = 0$,

and $\prod_{j\in Adj(i)}(x_i - x_j + 1)(x_i - x_j - (n-1)) = 0$ for each vertex $i \in V(G)$ has a solution. Thus, $\mathbf{V}(I_{HG}) \neq \emptyset$. Hence, by the Hilbert's Nullstellensatz, the Hamiltonian cycle ideal I_{HG} does not contain the identity 1. Conversely, assume that $1 \notin I_{HG}$. Note that since I_{HG} is an ideal of $\mathbb{C}[x_1, \ldots, x_n]$ and $\mathbb{C}$ is algebraically closed, we can use the Hilbert's Nullstellensatz. Thus, by the Hilbert's Nullstellensatz, $\mathbf{V}(I_{HG}) \neq \emptyset$, which means the system $\prod_{s=1}^{n} x_i - s = 0$, and $\prod_{j\in Adj(i)}(x_i - x_j + 1)(x_i - x_j - (n-1)) = 0$ for each vertex $i \in V(G)$ has a solution. Then, by the Lemma 4.2.2, there exists a Hamiltonian cycle in a graph with n vertices. □

The following example presents a graph in which there exists an Hamiltonian cycle.

Example: Consider the following graph G with 4 vertices.

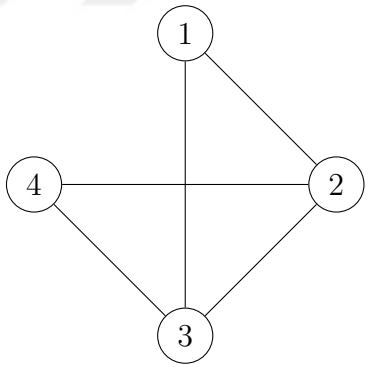


Figure 5.4

In this example, it is easy to see that $\{1, 2, 4, 3, 1\}$ is a Hamiltonian cycle in this graph. However, to see if there exists a Hamiltonian cycle in a graph with large numbers of vertices and edges may not be as easy as this example.

Now we will again use the Groebner bases to see whether the graph G has at least one Hamiltonian cycle. First we need to construct the Hamiltonian cycle ideal $I_{HC} \subset \mathbb{C}[x_1, \ldots, x_n]$. Since $n = 4$ in this example, by the Proposition 5.2.1, we can write

$$I_{HC} = \left\langle \prod_{s=1}^{4} x_i - s, \prod_{j \in Adj(i)} (x_i - x_j + 1)(x_i - x_j - 3) \text{ for } i = 1, 2, 3, 4 \right\rangle.$$

Then we find the Groebner basis of I_{HC}. With the help of the software CoCoA [15], we compute the reduced Groebner basis G'' of I_{HC} with respect to the lexicographic order as the following:

$$G'' = \Big\{ x_4^4 - 10x_4^3 + 35x_4^2 - 50x_4 + 24, \tfrac{4}{3}x_3x_4^3 - 10x_3x_4^2 - \tfrac{10}{3}x_4^3 + x_3^2 + \tfrac{68}{3}x_3x_4 + 25x_4^2 - 20x_3 - \tfrac{170}{3}x_4 + 43, \tfrac{4}{3}x_4^3 - 10x_4^2 + x_2 + x_3 + \tfrac{68}{3}x_4 - 20, -\tfrac{4}{3}x_4^3 + 10x_4^2 + x_1 - \tfrac{65}{3}x_4 + 10 \Big\}.$$

Since the reduced Groebner basis of I_{HC} is not $\{1\}$, 1 is not in the ideal I_{HC}, so by the Proposition 5.2.1, there exists a Hamiltonian cycle in the graph G.

Before deciding how many Hamiltonian cycles there are in this graph, we give the following lemma:

Lemma 5.2.2. *Let G be a graph having n vertices and $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be the ideal defined as:*

$$I = \left\langle \prod_{s=1}^{n} x_i - s, \prod_{j \in Adj(i)} (x_i - x_j + 1)(x_i - x_j - (n-1)) \right\rangle$$

Then I is a radical ideal and $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$ is equal to the number of points in $\mathbf{V}(I)$.

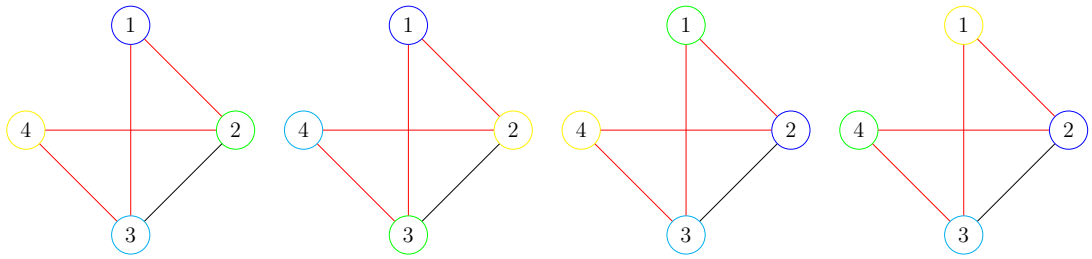
Proof. The proof is same as the proof of Lemma 4.1.1. As you notice, for each x_i, the square-free polynomial $\prod_{s=1}^{n} x_i - s$ is included in I. Then by the Proposition 3.3.3 in chapter 3, we obtain that

$$\sqrt{I} = I + \left\langle \prod_{s=1}^{n} x_i - s \right\rangle.$$

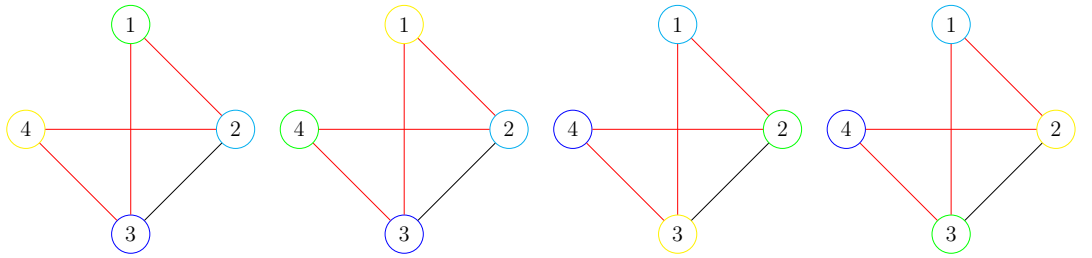
Since the ideal $\left\langle \prod_{s=1}^{n} x_i - s \right\rangle$ is included in I, we have $I + \left\langle \prod_{s=1}^{n} x_i - s \right\rangle = I$.

Hence, $\sqrt{I} = I$ which proves I is a radical ideal. Then by the Proposition 3.3.4 in chapter 3, we get $\dim(\mathbb{C}[x_1, \ldots, x_n]/I) = \mathbf{V}(I)$. □

Now let us decide how many Hamiltonian cycles there are in this graph. Note that the ideal in the previous lemma is exactly the same as the Hamiltonian cycle ideal I_{HC} for a graph with n vertices. Hence we can find the number solutions to the system given in this example by using the previous lemma. Again by the software system CoCoA [15], we find that $\dim(\mathbb{C}[x_1, \ldots, x_4]/I_{HC}) = |\mathbf{V}(I_{HC})| = 8$. Hence there are 8 solutions of the system $\prod_{s=1}^{4} x_i - s$, $\prod_{j \in Adj(i)} (x_i - x_j + 1)(x_i - x_j - 3)$ for $i = 1, 2, 3, 4$. These 8 solutions correspond to all Hamiltonian cycles in the graph G in Figure 5.4. The following figure (5.5) shows all of the Hamiltonian cycles. Note that the blue colored vertex is the starting vertex, green colored vertex is the second, cyan colored vertex is the third, and yellow colored vertex is the last vertex. Then we return to the first (blue) vertex again.



(a) $\{1, 2, 4, 3, 1\}$ (b) $\{1, 3, 4, 2, 1\}$ (c) $\{2, 1, 3, 4, 2\}$ (d) $\{2, 4, 3, 1, 2\}$



(e) $\{3, 1, 2, 4, 3\}$ (f) $\{3, 4, 2, 1, 3\}$ (g) $\{4, 2, 1, 3, 4\}$ (h) $\{4, 3, 1, 2, 4\}$

Figure 5.5: All Hamiltonian Cycles

Now it is left to determine that how many distinct Hamiltonian cycles there are in the graph. By Lemma 4.2.2, we know that the number of solutions divided

by $2n$ equals to the number of distinct Hamiltonian cycles. Hence, we conclude that there is 1 distinct Hamiltonian cycle in our graph. (When we look at the valid Hamiltonian cycles in 5.5, we can easily see that all the cycles are the same.)

The following is an example of a graph that does not have any Hamiltonian cycles.

Example: Consider the following graph with 7 vertices.

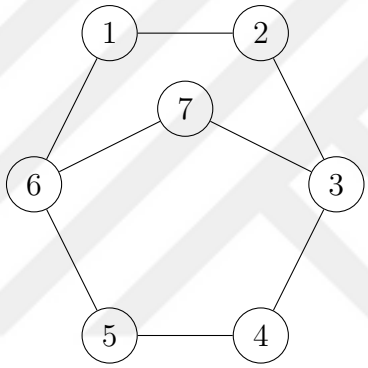


Figure 5.6

To determine whether this graph has a Hamiltonian cycle, we first form the Hamiltonian cycle ideal, $I_{HC} \subset \mathbb{C}[x_1, \ldots, x_7]$. By the Proposition 5.2.1, we write

$$I_{HC} = \left\langle \prod_{s=1}^{7} x_i - s, \prod_{j \in Adj(i)} (x_i - x_j + 1)(x_i - x_j - 6) \text{ for } i = 1, 2, 3, 4, 5, 6, 7 \right\rangle.$$

Now we need to compute the reduced Groebner basis for the ideal I_{HC}. Again with the software CoCoA [15], we find that the reduced Groebner basis is equal to $\{1\}$. Hence, by Proposition 5.1.1, we conclude that there does not exist a Hamiltonian cycle in this graph.

Bibliography

[1] "Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal," *Journal of Symbolic Computation*, vol. 41, no. 3–4, pp. 475 – 511, 2006.

[2] B. Buchberger and M. Kauers, "Groebner basis," vol. 5, no. 10, p. 7763, 2010. revision 128998.

[3] D. A. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag New York, 3rd ed., 2007.

[4] D. Dummit and R. Foote, *Abstract Algebra*. Wiley, 2004.

[5] D. Hilbert, "Ueber die vollen invariantensysteme," *Mathematische Annalen*, vol. 42, pp. 313–373, 1893.

[6] E. Arrondo, "Another elementary proof of the nullstellensatz," *The American Mathematical Monthly*, vol. 113, no. 2, pp. 169–171, 2006.

[7] J. A. De Loera, J. Lee, P. N. Malkin, and S. Margulies, "Hilbert's nullstellensatz and an algorithm for proving combinatorial infeasibility," in *Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation*, ISSAC '08, (New York, NY, USA), pp. 197–206, ACM, 2008.

[8] S. Margulies, *Computer algebra, combinatorics, and complexity: Hilbert's Nullstellensatz and NP-complete problems*. PhD thesis, UNIVERSITY OF CALIFORNIA, DAVIS, 2008.

[9] J. Kollár, "Sharp effective nullstellensatz," *Journal of the American Mathematical Society*, vol. 1, no. 4, pp. 963–975, 1988.

[10] D. Lazard, "Algèbre linéaire sur $K[X_1, \cdots, X_n]$, et élimination," *Bull. Soc. Math. France*, vol. 105, no. 2, pp. 165–190, 1977.

[11] D. A. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, vol. 185. Springer-Verlag New York, 1998.

[12] D. A. Bayer, *The Division Algorithm and the Hilbert Scheme*. PhD thesis, Cambridge, MA, USA, 1982. AAI8222588.

[13] W. Schnyder, "Planar graphs and poset dimension," *Order*, vol. 5, no. 4, pp. 323–343.

[14] R. Balakrishnan and K. Ranganathan, *A Textbook of Graph Theory*. Universitext (Berlin. Print), Springer New York, 2012.

[15] J. Abbott, A. M. Bigatti, and G. Lagorio, "CoCoA-5: a system for doing Computations in Commutative Algebra." Available at `http://cocoa.dima.unige.it`.