

Applied Hilbert's Nullstellensatz for Combinatorial Optimization

by

Julián Romero Barbosa

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2016

© Julián Romero Barbosa 2016

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Various feasibility problems in Combinatorial Optimization can be stated using systems of polynomial equations. Determining the existence of a *stable set* of a given size, finding the *chromatic number* of a graph or more generally, determining the feasibility of an *Integer Programming problem* are classical examples of this. In this thesis we study a powerful tool from Algebraic Geometry, called *Hilbert's Nullstellensatz*. It characterizes the *infeasibility* of a system of polynomial equations by the *feasibility* of a possibly very large system of *linear equations*. The solutions to this linear system provide *certificates* for the infeasibility of the polynomial system, called *Nullstellensatz Certificates*.

In this thesis we focus on the study of Nullstellensatz Certificates for the existence of *proper colorings* of graphs. We use basic ideas from *duality theory* to determine various properties of the Nullstellensatz Certificates. We give new proofs to several known results in the current literature and present some new results that shed some light on the relationship between the sparsity of a graph and the *size* of the Nullstellensatz Certificates for *k-colorability*.

Acknowledgements

I would like to thank my supervisor, Levent Tunçel, for his guidance and patience. He has taught me how to be a better mathematician, co-worker and researcher. I am profoundly grateful to him for his valuable comments, both in a mathematical and a spiritual level.

I thank my wife, Diana, who has been always supportive. She has been there in my time of need and has helped me to keep focused beside my many fears and struggles. Diana, eres mi inspiración, mi alma y mi alegría. Gracias por esos momentos tan bellos que hemos pasado juntos. Te has aventurado conmigo a salir, vivir y conocer por el mundo. Te amo transfinitamente!!

I also wish to thank my friends, Alan, Arash, Luis and Saman. Thanks for the laughs and support. I wish you the best for your future!

The material in this thesis is based upon research supported in part by NSERC Discovery Grants, Tuttle Scholarship, U.S. Office of Naval Research under award number: N00014-15-1-2171. This financial support is gratefully acknowledged.

Dedication

This thesis is dedicated to my family. My wife, Diana, my mother, Clara, my father, Jairo and my sisters Andrea and Rosy.

Gracias por su apoyo incondicional. Gracias por su comprensión y cariño. Los amo.

Table of Contents

List of Figures	viii
1 Introduction	1
2 Hilbert’s Nullstellensatz	7
2.1 From Linear Algebra To Algebraic Geometry	8
2.2 An important case: Polynomials in one variable.	11
2.3 Hilbert’s Nullstellensatz	16
3 Fourier Analysis for Finite Abelian Groups	25
3.1 Characters and the Dual Group	26
3.2 The Fourier Transform	29
3.3 Cayley Graphs	34
4 Applied Hilbert’s Nullstellensatz for Combinatorial Problems	38
4.1 Nullstellensatz Linear Algebra (NulLA) Algorithm	38
4.2 Nullstellensatz Dual Certificates and the Maximum Stable Set Problem . .	45
5 Hilbert’s Nullstellensatz and Graph Coloring Problems	54
5.1 Graph Colorability	55
5.2 Nullstellensatz Dual Certificates and k -colorability	63
5.2.1 Using symmetries to find Nullstellensatz Certificates	69

5.2.2	Fourier Analysis and Nullstellensatz Certificates	73
5.3	Girth and Nullstellensatz Certificates	77
5.4	Using Degree-Cutter Equations	90
6	Final Remarks and Future Work	98
	References	102

List of Figures

3.1	The graph $Cay(\mathbb{Z}_6, \mathcal{S})$	35
4.1	The Generalized Petersen Graph $GP(7, 2)$	46
5.1	The graph H	55
5.2	A 3-star	69
5.3	The graph H	93
5.4	H has a degree six Nullstellensatz Certificate for (FCOL). Each labelled graph represents a multi-index (except for the first one).	96

Chapter 1

Introduction

Linear Algebra is probably one of the most useful mathematical tools to solve a wide range of theoretical and applied problems in mathematics and other sciences. Either in real world applications or pure theoretical questions, Linear Algebra has found its way to contribute to the development and the deep understanding of a variety of mathematical objects and structures of study. One of the main reasons for such a great impact in science is the fact that, the Theory of Linear Algebra has characterized when a *system of linear equations* has a solution and has provided *efficient* algorithms to solve such systems. To phrase it on Edmonds' terms ([23], [13]), Linear Algebra provides us with a *good characterization* for the existence of solutions of linear systems. Such characterization is often called *Fredholm's Theorem of the Alternative*: for every matrix $A \in \mathbb{R}^{m \times n}$ and every vector $b \in \mathbb{R}^m$,

$$\begin{array}{l} Ax = b \\ \text{has no solution,} \end{array} \iff \begin{array}{l} A^\top y = 0, b^\top y = 1 \\ \text{has a solution.} \end{array} \quad (1.0.1)$$

Fredholm's Theorem of the Alternative lets us *certify* the nonexistence of solutions of systems of linear equations with the existence of solutions of another system of linear equations. More concretely, if one wishes to convince someone that the system $Ax = b$ has no solution, then we can provide a solution $y \in \mathbb{R}^m$ to (1.0.1) as a *certificate* of such assertion. Of course, among all possible certificates, one would like to provide the *best* (in some suitable sense) certificate. For example, in the context of systems of linear equations, one would like to provide a certificate y with as few non-zero entries as possible.

Even though linear systems are very powerful, numerous problems of great interest cannot, at a first glance be modeled using systems of linear equations. For instance, problems of a discrete nature such as *Integer Programming* feasibility problems, where the

variables are required to be integers, are examples of this. For these types of problems a more elaborate machinery needs to be constructed. A natural generalization is to consider *systems of polynomial equations* instead of linear systems. More concretely, given a set of multivariate polynomials p_1, p_2, \dots, p_m over the complex numbers with n variables, we consider the system:

$$p_1(x) = p_2(x) = \dots = p_m(x) = 0, \quad x \in \mathbb{C}^n. \quad (1.0.2)$$

Clearly, systems like (1.0.2) are more powerful than linear systems. For example, they can model much harder problems such as 0, 1 Integer Programming feasibility problems. This, since a polynomial equation like $x_j^2 - x_j = 0$ would force the variable x_j to be either zero or one. In particular, the problem of deciding the existence of solutions to (1.0.2) lies in the complexity class of *NP-hard* problems ([29]).

Despite the difficulty of solving systems of polynomial equations, their theoretical importance is astonishing. For instance, David Hilbert ([31]), while studying the Theory of Algebraic Invariants, proved in 1893 the following good characterization for the existence of solutions to (1.0.2):

$$\begin{array}{l} p_1(x) = \dots = p_m(x) = 0 \\ \text{has no solution } x \in \mathbb{C}^n, \end{array} \iff \begin{array}{l} r_1(x)p_1(x) + \dots + r_m(x)p_m(x) = 1 \\ \text{for some polynomials } r_1, \dots, r_m. \end{array} \quad (1.0.3)$$

This characterization, called *Hilbert's Nullstellensatz* or *Hilbert's Theorem of Zeros*, is one of the building blocks of Algebraic Geometry and Commutative Algebra as it shows a deep connection between algebraic objects (*ideals of polynomials*, cf. Definition 2.1.5) and geometric objects (*affine varieties*, cf. Definition 2.1.1). The polynomials r_1, r_2, \dots, r_m on the right hand side of (1.0.3) provide a certificate for the non-solubility of (1.0.2). Such certificate is called a *Nullstellensatz Certificate* and its degree is the maximum degree of the polynomials r_i with $i \in \{1, 2, \dots, m\}$. Determining the existence of a Nullstellensatz Certificate of a given degree can be done using a *system of linear equations*. Indeed, if we fix the degree of the polynomials r_1, \dots, r_m , then the equation

$$r_1(x)p_1(x) + \dots + r_m(x)p_m(x) = 1 \quad (\text{NCERT})$$

becomes nothing but a system of linear equations, where the variables are the coefficients of the polynomials r_i with $i \in \{1, 2, \dots, m\}$. Thus, Hilbert's Nullstellensatz transforms the non-solubility of (1.0.2) into a family of (possibly large) systems of *linear equations*.

János Kollar ([34]) in 1988 proved that if (1.0.2) has no solution and the polynomials p_i with $i \in \{1, 2, \dots, m\}$ have degree at most d , then there exists a Nullstellensatz Certificate r_1, r_2, \dots, r_m having degree at most $\max(3, d)^{\min(n, m)}$. Moreover, Kollar showed that his

bounds were sharp and as a consequence the linear system induced by (NCERT) might end up being enormous.

Nonetheless, for many important classes of polynomial equations the bounds found by Kollar are far from being optimal. For instance, Daniel Lazard [37] showed that if the polynomials p_1, p_2, \dots, p_m have no common roots and no common *roots at infinity* (cf. Definition 2.3.9), then the bound on the degree of the certificates can be lowered to $n(d-1)$. Examples of such systems of polynomials are the ones containing the equations $x_j(x_j-1) = 0$ or $x_j^k - 1 = 0$ for every $j \in \{1, 2, \dots, n\}$ and any $k \geq 1$. Thus, when dealing with *combinatorial problems* that can be encoded as systems of polynomial equations, better bounds can be expected and the linear system (NCERT) might gain some computational interest.

These observations were carried out by Jesús de Loera and many of his coworkers ([20], [17]). They implemented an algorithm, known as the Nullstellensatz Linear Algebra (NulLA) Algorithm, which uses the linear system derived from (NCERT) to detect the feasibility of (1.0.2) (cf. Algorithm 4.1.1). Several graph theoretic problems such as finding a stable set of a given size, determining whether a graph can be colored with k -colors and determining the existence of a hamiltonian cycle, among others were tested with NulLA ([20]). Although for some of these problems Lazard's bounds were sharp, their computer experiments showed that NulLA outperformed several other known algorithms for checking the non-3-colorability of a graphs ([21]). Moreover, the degrees of the certificates for non-3-colorability seemed to be much smaller than Lazard's bounds.

The polynomial encoding that De Loera and his co-authors used for graph coloring is due to David Bayer in 1982 ([5]) who noted that a graph $G = (V, E)$ is k -colorable if and only if the system of polynomial equations

$$\begin{aligned} x_v^k - 1 &= 0 \quad \forall v \in V, \\ x_u^{k-1} + x_u^{k-2}x_v + \dots + x_u x_v^{k-2} + x_v^{k-1} &= 0 \quad \forall uv \in E, \end{aligned} \tag{BCOL}$$

has a solution $x \in \mathbb{K}^V$ over any closed field \mathbb{K} of characteristic p not dividing k . Indeed, the first equation in (BCOL) assigns a k -root of the unity to each variable x_v with $v \in V$ and the second equation guarantees that $x_u \neq x_v$ for every edge $\{u, v\} \in E$ (cf. Theorem 5.1.3).

Besides its apparent practical value as a computational tool for detecting the k -colorability of graphs, only few results about the properties of the Nullstellensatz Certificates for (BCOL) are known and many problems are still open. Recently, Bo Li, Benjamin Lowenstein and Mohamed Omar [39] gave a clean combinatorial characterization of all graphs that have Nullstellensatz Certificate of degree *one* for (BCOL) with $k = 3$ over the finite

field \mathbb{F}_2 (see also [19]). Moreover, they showed (via exhaustive computations) that every non-3-colorable graph with at most *twelve vertices* has a Nullstellensatz Certificate of degree at most *four* for (BCOL) over \mathbb{F}_2 .

Jesús De Loera, Jon Lee, Peter Malkin and Susan Margulies [20] proved that unless $P = NP$, for every integer $d \geq 1$ there exists a non-3-colorable graph with minimal Nullstellensatz Certificate for (BCOL) (over any field \mathbb{K} as above) of degree greater than or equal to d . However, it is still an open problem to find a graph whose minimal Nullstellensatz Certificate has degree greater than *four* for (BCOL) (over any field \mathbb{K} as above).

The main purpose of this thesis is to study (BCOL) and other systems of polynomial equations from a *dual point of view*. That is, instead of trying to show the existence of Nullstellensatz Certificates using the system of *linear equations* derived from (NCERT) directly, we will use Fredholm's Theorem of the Alternative to study the *non-existence* of Nullstellensatz Certificates of certain degree. More concretely, an infeasible system of polynomial equations (1.0.2) over some closed field \mathbb{K} has a Nullstellensatz Certificate of degree \bar{d} if and only if the constant polynomial 1 lies in the finite dimensional vector space

$$\mathbf{V}_{\bar{d}} := \{r_1(x)p_1(x) + \cdots + r_m(x)p_m(x) : \text{each polynomial } r_i \text{ has degree at most } \bar{d}\}.$$

We can see $\mathbf{V}_{\bar{d}}$ as a subspace of the vector space \mathbf{V} of all polynomials on n variables with coefficients in \mathbb{K} . Thus, (1.0.2) *does not have* a Nullstellensatz Certificate of degree \bar{d} if and only if there exists a linear functional $\lambda \in \mathbf{V}^*$ in the *dual space* of \mathbf{V} such that

$$\lambda(p) = 0, \quad \forall p \in \mathbf{V}_{\bar{d}}, \quad (\text{DNCERT})$$

and $\lambda(1) \neq 0$. Such linear functionals λ are called *Dual Nullstellensatz Certificates* of degree d (cf. Definition 4.2.7). These dual certificates (sometimes referred as *Designs* [9],[10]) were introduced by Stephen Cook et. al. ([6]) to find lower bounds for Nullstellensatz Certificates of systems describing a version of the Pigeon Principle. Later, Jesus De Loera, Peter Malkin and Pablo Parrilo ([22]) did a very general study of the set of all $\lambda \in \mathbf{V}^*$ satisfying (DNCERT), i.e. the *annihilator* of $\mathbf{V}_{\bar{d}}$ (cf. Definition 4.2.5). However, no specific study of Dual Nullstellensatz Certificates of the systems like (BCOL) or other systems of polynomial equations arising from combinatorial problems has been done until now.

Our contributions are the following. First, using this dual approach, we found new proofs to many of the results found in the current literature. For instance, we give a shorter and combinatorial proof to the following result due to De Loera et. al. [20] (see Theorem 4.2.11).

Theorem A. *Let $G = (V, E)$ be a graph with maximum stable set of size $\alpha(G)$. Then, for any $k \geq \alpha(G) + 1$ the system*

$$\begin{aligned} \sum_{i \in V} x_i - k &= 0, \\ x_i x_j &= 0, \quad \forall \{i, j\} \in E, \\ x_i(x_i - 1) &= 0, \quad \forall i \in V, \end{aligned} \tag{STAB}$$

has a minimal Nullstellensatz Certificate of degree $\alpha(G)$.

We also give a new proof of the following recent result due to De Loera et. al. [18] (see Corollary 5.2.4)

Theorem B. *Let $G = (V, E)$ be a non- k -colorable graph with $k > 3$ and suppose that (BCOL) has minimal Nullstellensatz Certificate of degree d^* . Then,*

$$d^* \cong 1 \pmod{k}. \tag{1.0.4}$$

Moreover, $d^ \geq k + 1$.*

Systems like (BCOL) have the great advantage of having its set of solutions contained in a *finite abelian group*: each coordinate of any solution x to (BCOL) lie in the multiplicative group generated by the k -th roots of the unity. We use this basic observation throughout the thesis to derive beautiful connections between *Fourier Analysis* of finite abelian groups and the Nullstellensatz (cf. Chapter 3 and Section 5.2.2). In particular, this connection leads to the study of the following equivalent system of polynomial equations

$$\begin{aligned} x_u^k - 1 &= 0 \quad \forall u \in V, \\ 1 + x_u x_v^{k-1} + x_u^2 x_v^{k-2} + \dots + x_u^{k-1} x_v &= 0 \quad \forall \{u, v\} \in E. \end{aligned} \tag{FCOL}$$

The system (FCOL) can be seen as a relaxation of the system (BCOL). More concretely, if a non- k -colorable graph has a Nullstellensatz Certificate for (FCOL) of degree d , then it has a Nullstellensatz Certificate for (BCOL) of degree $d + 1$ or $d - k + 1$ (cf. Proposition 5.1.5). We prove the following theorem (see Theorem 5.3.7).

Theorem C. *Let $G = (V, E)$ be non-3-colorable graph with minimal Nullstellensatz Certificate for (FCOL) of degree d^* . If G has girth at least six, then*

$$d^* \geq 6.$$

We believe that the techniques used to prove the above theorem may work for the case (BCOL) as well and we could possibly derive a more general statement.

Next, we use the theory of Dual Nullstellensatz Certificates to find instances on which it is possible to guarantee the existence of Nullstellensatz Certificate of some degree. In particular we prove the following theorem relating the k -colorability of a graph and the set of cliques of size k contained in them (see Theorem 5.4.3).

Theorem D. *Let $G = (V, E)$ be a graph and let $k \geq 3$ be an odd integer. Consider the group*

$$\Gamma_k := \langle e_{u_1} + \cdots + e_{u_k} : u_1, \dots, u_k \in V \text{ form a } k\text{-clique} \rangle \subseteq \mathbb{Z}_k^V,$$

where $e_u \in \mathbb{Z}_k^V$ with $u \in V$ are the canonical vectors of the group \mathbb{Z}_k^V . If there exists an edge $\{u, v\} \in E$ such that $e_u - e_v \in \Gamma_k$, then G is not k -colorable.

It is possible to use Theorem D to find Nullstellensatz Certificates for the non-3-colorability of graphs that have a rich triangle structure (cf. Lemma 5.4.5). In particular, we can use it to prove that every odd wheel has a Nullstellensatz Certificate of degree 4 for (BCOL) (see [20] and Proposition 5.4.7).

This dissertation is organized as follows. In Chapter 2 we give a quick introduction to the basics of Algebraic Geometry. Several examples and comments are provided. At the end of this chapter we give a simple proof of Hilbert's Nullstellensatz due to Enrique Arrondo ([4]). In Chapter 3, we study the theory of Fourier Analysis for Finite Abelian Groups. We introduce the dual group and construct the Fourier Transform. We also study some basic properties of Cayley Graphs and their spectra. In Chapter 4, we study some upper bounds for the degree of Nullstellensatz Certificates. We prove a slightly weaker version of Lazard's bound using Fourier Analysis. Then, we introduce the concept of Dual Nullstellensatz Certificate and use it to derive lower and upper bounds for (STAB). In Chapter 5 we use Fourier Analysis to derive an alternative formulation to (BCOL). Using this formulation, along with Dual Nullstellensatz Certificates, we prove the main results in our thesis, namely Theorem B, Theorem C and Theorem D. Finally, in Chapter 6 we give some final remarks and discuss some open problems.

Chapter 2

Hilbert's Nullstellensatz

In this chapter we introduce a well known result in Algebraic Geometry due to Hilbert called *Hilbert's Nullstellensatz* ([31]). This theorem is a mathematical tool to certify insolubility of system of polynomial equations by transforming the original problem into a system of linear equations. Later on, we will see that this transformation allows us to create algorithms for deciding the existence of combinatorial structures using systems of linear equations.

Throughout this thesis, we let $\mathbb{K}[x_1, x_2, \dots, x_n]$ be the set of polynomials on n variables with coefficients in the the field \mathbb{K} . Common choices for \mathbb{K} are the fields of complex numbers \mathbb{C} , real numbers \mathbb{R} or finite fields \mathbb{F}_q with $q = p^m$ for some prime $p \in \mathbb{Z}$ and some integer $m \geq 1$. A field \mathbb{K} is *algebraically closed* if every non-constant polynomial $p \in \mathbb{K}[x]$ has a root, i.e. there exists some $\bar{x} \in \mathbb{K}$ such that $p(\bar{x}) = 0$. The Fundamental Theorem of Algebra is the statement asserting that \mathbb{C} is a closed field.

We will often use the multi-index notation for polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$. A *multi-index* $\alpha \in \mathbb{Z}^n$ is a vector of non-negative integers and its *size* or *degree* is defined to be the sum

$$|\alpha| := \alpha_1 + \alpha_2 + \dots + \alpha_n.$$

Every monomial in $\mathbb{K}[x_1, x_2, \dots, x_n]$ can be written as $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ for some multi-index $\alpha \in \mathbb{Z}^n$ and every polynomial $p \in \mathbb{K}[x_1, x_2, \dots, x_n]$ can be written as

$$p(x) = \sum_{\alpha \in A} p_\alpha x^\alpha,$$

where A is a finite subset of multi-indexes. If $p_\alpha \neq 0$ for every $\alpha \in A$, then we say that A is the *support* of p and we denote such set by $\text{supp}(p)$. The degree of the polynomial p ,

denoted by $\deg(p)$ is the maximum size of the multi-indexes in its support. The degree of the zero polynomial is equal to -1 by convention.

2.1 From Linear Algebra To Algebraic Geometry

Probably the most important theorem in linear algebra is that of characterizing whether a system of linear equations has a solution or not. Given a matrix $A \in \mathbb{K}^{n \times m}$ and a vector $b \in \mathbb{K}^n$, the system of linear equations

$$Ax = b, \tag{2.1.1}$$

has a solution if and only if the b lies in the linear span of the columns of A . If we have access to an inner product on \mathbb{K}^n , then (2.1.1) has a solution if and only if every vector $y \in \mathbb{K}^n$ orthogonal to the columns of A is orthogonal to the vector b . In particular, this implies that if the system (2.1.1) has no solution, then there exists some y orthogonal to the columns of A satisfying $\langle y, b \rangle = 1$. Such y is called a *certificate* for the infeasibility of the system (2.1.1) and can be found by solving the system of linear equations

$$\begin{aligned} A^*y &= 0, \\ \langle b, y \rangle &= 1. \end{aligned} \tag{2.1.2}$$

Here, A^* is the *adjoint* of A with respect to the inner product $\langle \cdot, \cdot \rangle$, that is the unique matrix satisfying the equality $\langle A^*y, x \rangle = \langle y, Ax \rangle$ for every $x \in \mathbb{R}^m$ and $y \in \mathbb{R}^n$.

Notice that a system of linear equations is nothing but a system of polynomial equations where each polynomial has degree equal to one. Can we find certificates for the infeasibility of *systems of polynomial equations*? More concretely, let p_1, p_2, \dots, p_m be polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$ such that the system

$$p_j(x) = 0, \quad j \in [m] := \{1, 2, \dots, m\}, \tag{2.1.3}$$

has no solution $x \in \mathbb{K}^n$. *Does there exist* some polynomial or polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$ that certify the infeasibility of (2.1.3)? If so, *is there an algorithm* to find such certificate? In order to solve this problem let us go back to the linear case once more. Notice that for the system (2.1.1) there were two objects in play: the affine space of all vectors $x \in \mathbb{K}^m$ satisfying $Ax = b$ (a geometric object) and the vector space generated by the columns of A (an algebraic object). We can generalize these two objects for polynomials as follows:

Definition 2.1.1. Let p_1, p_2, \dots, p_m be polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$. The **affine variety defined by the polynomials** p_1, \dots, p_m , denoted by $\mathcal{V}_{\mathbb{K}}(p_1, \dots, p_m)$, is the set of all points $x \in \mathbb{K}^n$ satisfying the equalities

$$p_1(x) = p_2(x) = \dots = p_m(x) = 0. \quad (2.1.4)$$

Example 2.1.2. Let us consider the problem

$$\begin{aligned} \min \quad & f(x, y) := x^4 + y^2x + 1, \\ \text{s.t.} \quad & g(x, y) := x^2 + y^2 = 1, \\ & x, y \in \mathbb{R}. \end{aligned} \quad (2.1.5)$$

A common way of solving this type of optimization problem is, in fact, by studying certain affine algebraic variety. More concretely, one can use the method of Lagrange multipliers: if (2.1.5) has an optimal solution (\bar{x}, \bar{y}) and the gradient $\nabla g(\bar{x}, \bar{y})$ is not equal to zero, then there exists some $\bar{\lambda} \in \mathbb{R}$ such that $(\bar{x}, \bar{y}, \bar{\lambda})$ is a solution to

$$\begin{cases} \nabla f(x, y) - \lambda \nabla g(x, y) = 0, \\ g(x, y) = 1, \end{cases} \iff \begin{cases} 4x^3 + y^2 - 2\lambda x = 0, \\ 2y(x - \lambda) = 0, \\ x^2 + y^2 - 1 = 0. \end{cases} \quad (2.1.6)$$

The affine variety $\mathcal{V}_{\mathbb{R}}(4x^3 + y^2 - 2\lambda x, 2y(x - \lambda), x^2 + y^2 - 1)$ consists of four points in \mathbb{R}^3 . Indeed, if $y = 0$ in (2.1.6) then $x \in \{-1, 1\}$ and the first equation in (2.1.6) implies that $\lambda = 2$. If $y \neq 0$, then the second equation in (2.1.6) implies that $x = \lambda$. Thus, every triple (x, y, λ) with $y \neq 0$ satisfies

$$\begin{cases} 4x^3 - 3x^2 + 1 = 0, \\ x - \lambda = 0, \\ x^2 + y^2 - 1 = 0. \end{cases} \quad (2.1.7)$$

The polynomial $4x^3 - 3x^2 + 1$ has only one real root given by $x_0 := -\frac{a^2 - a + 1}{4a}$ where $a := (7 - \sqrt{3})^{\frac{1}{3}}$. Moreover, $|x_0| \leq 1$ which implies that $(x_0, \pm\sqrt{1 - x_0^2}, x_0)$ are the other two solutions to (2.1.6). It is not hard to see that $f(x_0, \pm\sqrt{1 - x_0^2}) < 2$ and it gives us an optimal solution to the problem.

Remark 2.1.3. The problem (2.1.5) is a particular example of a Polynomial Optimization Problem (POP), that is problems of the form

$$\begin{aligned} \max \quad & f(x) \quad , \\ \text{s.t.} \quad & h_i(x) = 0, \forall i \in [s], \\ & g_j(x) \leq 0, \forall j \in [t], \\ & x \in \mathbb{R}^n. \end{aligned} \quad (2.1.8)$$

where the functions f, h_1, \dots, h_s and g_1, \dots, g_t are polynomials in $\mathbb{R}[x_1, x_2, \dots, x_n]$. Under some mild conditions (constraint qualifications), one would use the Karush-Kuhn-Tucker Theorem to transform (2.1.8) into a system of polynomial inequalities (see Chapter 12 of [47]).

Example 2.1.4. Every Integer Programming (IP) feasibility problem of the form

$$\begin{cases} Ax = b, \\ x \in \{0, 1\}^n, \end{cases} \quad (2.1.9)$$

where A is an $m \times n$ real matrix and $b \in \mathbb{R}^m$ is equivalent to the system of polynomial equations

$$\begin{cases} Ax = b, \\ x_i^2 - x_i = 0, \quad \forall i \in [n]. \end{cases} \quad (2.1.10)$$

Hence, checking the feasibility of these problems is equivalent to determining whether some affine algebraic variety (defined by polynomials of degree at most two) is empty or not.

Let us now introduce the analog of vector spaces for polynomials:

Definition 2.1.5. Let p_1, p_2, \dots, p_m be polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$. The **ideal generated by** p_1, \dots, p_m is the set of all of its polynomial combinations with coefficients from $\mathbb{K}[x_1, x_2, \dots, x_n]$, i.e. it is the set defined by

$$\langle p_1, \dots, p_m \rangle_{\mathbb{K}} := \left\{ \sum_i r_i(x) p_i(x) : r_i \in \mathbb{K}[x_1, \dots, x_n] \text{ for all } i \in \{1, \dots, m\} \right\}. \quad (2.1.11)$$

Ideals $\mathcal{I} := \langle p_1, \dots, p_m \rangle_{\mathbb{K}}$ are called *finitely generated ideals* (e.g. Definition 2.1.8) and the set $\{p_1, \dots, p_m\}$ of polynomials is said to be a *basis* for \mathcal{I} . An ideal can have many different bases and not all of them may have the same number of elements. For example, take the polynomials $p_1(x, y) := x^2y + 1$ and $p_2(x, y) := x$ in \mathbb{R} . The ideal $\langle p_1, p_2 \rangle_{\mathbb{R}}$ contains the polynomial

$$1 \cdot (x^2y + 1) - xy \cdot (x) = 1.$$

Therefore, $\langle p_1, p_2 \rangle_{\mathbb{R}} = \langle 1 \rangle_{\mathbb{R}} = \mathbb{R}[x, y]$. However, as the following lemma shows, all bases for a polynomial ideal always define the same affine variety.

Lemma 2.1.6. Let \mathcal{I} be an ideal with bases $\{p_1, \dots, p_m\}$ and $\{q_1, \dots, q_\ell\}$ in $\mathbb{K}[x_1, \dots, x_n]$. Then,

$$\mathcal{V}_{\mathbb{K}}(p_1, \dots, p_m) = \mathcal{V}_{\mathbb{K}}(q_1, \dots, q_\ell).$$

Proof. Since the polynomials p_1, \dots, p_m and q_1, \dots, q_ℓ generate the same ideal, there exist some polynomials $r_{ij} \in \mathbb{K}[x_1, \dots, x_n]$ for each $i \in [m]$ and $j \in [\ell]$, such that

$$q_j = \sum_{i \in [m]} r_{ij} p_i, \quad \forall j \in [\ell].$$

In particular, if $x \in \mathcal{V}_{\mathbb{K}}(p_1, \dots, p_m)$, then $p_i(x) = 0$ for all $i \in [m]$. However, this implies that $q_j(x) = 0$ for each $j \in [\ell]$ and $x \in \mathcal{V}_{\mathbb{K}}(q_1, \dots, q_\ell)$. The reverse inclusion can be proven similarly. \square

Example 2.1.7. *An affine variety may come from different ideals. For example, the ideals $\langle x - 1, x + 1 \rangle_{\mathbb{C}}$ and $\langle x^2 - 1 \rangle_{\mathbb{C}}$ define the same variety:*

$$\mathcal{V}_{\mathbb{C}}(x - 1, x + 1) = \mathcal{V}_{\mathbb{C}}(x^2 - 1) = \{1, -1\}.$$

However, the ideal $\langle x^2 - 1 \rangle_{\mathbb{C}}$ does not contain polynomials of degree less than two, whereas $x - 1 \in \langle x - 1, x + 1 \rangle_{\mathbb{C}}$.

We end this section with a more general definition of ideal that will be useful later.

Definition 2.1.8. *A subset \mathcal{I} of $\mathbb{K}[x_1, \dots, x_n]$ is an **ideal** if it satisfies all of the following:*

1. *The zero polynomial is in I .*
2. *If p and q are polynomials in I , then $p + q$ is in I .*
3. *If p is in I , then for every polynomial $h \in \mathbb{K}[x_1, \dots, x_n]$, the polynomial $h \cdot p$ is in I .*

Remark 2.1.9. *Clearly, every finitely generated ideal is an ideal in the sense of Definition 2.1.8. Moreover, Hilbert's Basis Theorem states that every ideal in the sense of Definition 2.1.8 is finitely generated (see Chapter 2 of [14]).*

2.2 An important case: Polynomials in one variable.

Let us study the case of systems of polynomials with only one indeterminate, i.e. univariate polynomials. The *leading term* of a polynomial $p \in \mathbb{K}[x]$, denoted by $\text{LT}(p)$, is the monomial with highest degree appearing in p . For example, the leading term of $p(x) = 2x^2 + x - 1$ is the polynomial $\text{LT}(p) = 2x^2$. A remarkable property of polynomials in one variable is that we have access to a *division algorithm*. The idea of the algorithm, originally due to Euclid (300 BC) and called the Euclidean Division Algorithm, is given in the following proposition.

Proposition 2.2.1. *Let $p, q \in \mathbb{K}[x]$ be any two given polynomials with $q \neq 0$. Then, there exist polynomials s and $r \in \mathbb{K}[x]$ such that*

$$p = sq + r \quad \text{and} \quad \deg(r) < \deg(q). \quad (2.2.1)$$

Proof. If the degree of p is smaller than the degree of q , then we can set $s = 0$ and $r = p$. Therefore we may assume that $\deg(p) \geq \deg(q)$ and as a consequence the polynomial $\text{LT}(q)$ divides $\text{LT}(p)$. Let us define the polynomials $s = -\frac{\text{LT}(p)}{\text{LT}(q)}$ and $r = p - sq$. Notice that $\deg(r)$ is strictly smaller than $\deg(p)$. If $\deg(r)$ is greater than or equal to $\deg(q)$, then we continue this process with r instead of p until we obtain a polynomial with degree less than $\deg(q)$. This process terminates in a finite number of steps as we are strictly decreasing the degree of r on each iteration of the algorithm. \square

The following pseudo code shows the division algorithm for a pair of given univariate polynomials p and $q \neq 0$. Notice that the coefficients of the polynomials s and r in the algorithm are polynomial functions on the coefficients of p and q divided by some power of the coefficient of $\text{LT}(q)$.

Algorithm 2.2.1: Division Algorithm (DIV)

Data: Polynomials p and $q \neq 0$ in $\mathbb{K}[x]$

Result: Polynomials s, r such that $p = sq + r$ and $\deg(r) < \deg(q)$

```

1  $\tilde{p} = p;$ 
2  $s = \text{LT}(\tilde{p});$ 
3 while  $\deg(\tilde{p}) \geq \deg(q)$  do
4    $r = \tilde{p};$ 
5    $\tilde{p} = \tilde{p} - \frac{\text{LT}(\tilde{p})}{\text{LT}(q)}q;$ 
6    $s = s + \text{LT}(\tilde{p});$ 
7  $s = \frac{s}{\text{LT}(q)};$ 

```

We have the following corollary:

Corollary 2.2.2. *Let $\mathcal{I} = \langle p_1, \dots, p_m \rangle_{\mathbb{K}}$ be a given ideal of $\mathbb{K}[x]$. Then,*

$$\mathcal{I} = \langle p \rangle_{\mathbb{K}}$$

for some polynomial p in $\mathbb{K}[x]$. Moreover, p is unique up to multiplication by constants in \mathbb{K} .

Proof. We use induction on m with the base case $m = 1$ being trivial. Suppose that for any $m - 1$ set of polynomials p_1, \dots, p_{m-1} in $\mathbb{K}[x]$, there exists some other polynomial q such that

$$\langle p_1, \dots, p_{m-1} \rangle_{\mathbb{K}} = \langle q \rangle_{\mathbb{K}}.$$

Let p_m be any other polynomial in $\mathbb{K}[x]$. Clearly, the ideals $\langle p_1, \dots, p_{m-1}, p_m \rangle_{\mathbb{K}}$ and $\langle q, p_m \rangle_{\mathbb{K}}$ are the same by our definition of ideal. If $q = 0$ then the result follows trivially. Hence, without loss of generality we may assume that $0 \leq \deg(q) \leq \deg(p_m)$. By Proposition 2.2.1 there exists a pair of polynomials r and s such that $p_m = sq + r$ and $\deg(r) < \deg(q)$. As a consequence, the ideals $\langle q, p_m \rangle_{\mathbb{K}}$ and $\langle q, r \rangle_{\mathbb{K}}$ are the same, but with

$$\deg(p_m) + \deg(q) > \deg(r) + \deg(q).$$

If $r = 0$, then q divides p_m and the result follows. Otherwise, we can use Proposition 2.2.1 again to find some polynomial r' such that

$$\langle q, r \rangle_{\mathbb{K}} = \langle r', r \rangle_{\mathbb{K}} \quad \text{and} \quad \deg(q) + \deg(r) > \deg(r') + \deg(r).$$

We can continue this process until one of the two polynomials generating the ideal is zero and the ideal $\langle p_1, \dots, p_m \rangle_{\mathbb{K}}$ is generated by some polynomial p . It remains to prove that p is unique up to multiplication by constants, but this is easy. Indeed, suppose that $\langle p \rangle_{\mathbb{K}} = \langle p' \rangle_{\mathbb{K}}$, then p divides p' and p' divides p . This only happens when $p = cp'$ for some $c \in \mathbb{K}$. \square

The unique polynomial p (up to multiplication by constants in \mathbb{K}) found in Corollary 2.2.2 is called the *greatest common divisor* (GCD) of the polynomials p_1, p_2, \dots, p_m . Notice that any polynomial r that divides all of p_1, p_2, \dots, p_m , divides p as well. Indeed, since $p \in \langle p_1, \dots, p_m \rangle_{\mathbb{K}}$, there exist polynomials s_1, \dots, s_m such that $p = s_1p_1 + \dots + s_m p_m$. If each of the p_i is divisible by r , then there exists some r_i such that $p_i = r_i r$ and

$$p = (s_1 r_1 + \dots + s_m r_m) r,$$

proving our claim. Notice that the proof of Corollary 2.2.2 gives us an algorithm to determine the GCD of a given set of polynomials. However, it does not express the GCD as a polynomial combination of the original polynomials. We can modify the proof of Corollary 2.2.2 to obtain the following algorithm:

Algorithm 2.2.2: The Extended Euclidean Algorithm (GCD)

Data: $p_1, p_2, \dots, p_m \in \mathbb{K}[x]$

Result: Their GCD p and polynomials r_1, \dots, r_m such that $p = r_1p_1 + \dots + r_mp_m$.

```
1  $p := p_1; r_1 := 1;$ 
2  $i := 2;$ 
3 while  $i \leq m$  do
4   if  $p_i = 0$  then
5      $r_i = 0, i := i + 1;$ 
6     if  $i > m$  then
7       return:  $p, r_1, \dots, r_m;$ 
8   else
9      $q := p_i;$ 
10     $s_1 := 1; s_2 := 0; t_1 := 0; t_2 := 1;$ 
11     $j = 2;$ 
12    while  $\deg(q) \geq 0$  do
13       $j := j + 1;$ 
14       $[s, r] := \text{DIV}(p, q);$ 
15       $p := q;$ 
16       $q := r;$ 
17       $s_j := s_{j-2} - ss_{j-1};$ 
18       $t_j := t_{j-2} - st_{j-1};$ 
19       $r_1 := s_j r_1, \dots, r_{i-1} := s_j r_{i-1};$ 
20       $r_i := t_j;$ 
21       $i := i + 1;$ 
```

Corollary 2.2.2 implies that every affine variety in \mathbb{K} is equal to the set of zeros of a single polynomial in $\mathbb{K}[x]$. Hence, in an algebraically closed field \mathbb{K} , every system of univariate polynomial equations $p_1(x) = p_2(x) = \dots = p_m(x) = 0$ has no solution if and only if the constant polynomial 1 is in the ideal $\langle p_1, \dots, p_m \rangle_{\mathbb{K}}$. In particular, we can guarantee the existence of polynomials r_1, \dots, r_m such that

$$1 = r_1p_1 + \dots + r_mp_m.$$

These polynomials will be our *certificate* for the infeasibility of the system $p_1(x) = p_2(x) = \dots = p_m(x) = 0$. In fact, we have the following slightly stronger result:

Theorem 2.2.3 (The Univariate Nullstellensatz). *Let p_1, p_2, \dots, p_m and q be non-zero polynomials in $\mathbb{K}[x]$ with \mathbb{K} algebraically closed. Exactly one of the following holds:*

1. The system of equations $p_1(x) = p_2(x) = \cdots = p_m(x) = 0, q(x) \neq 0$ has a solution in \mathbb{K} .
2. There exist polynomials r_1, r_2, \dots, r_m in $\mathbb{K}[x]$ and some integer $\ell \geq 1$ such that

$$q^\ell = r_1 p_1 + r_2 p_2 + \cdots + r_m p_m.$$

Proof. Let p be the GCD of the polynomials p_1, p_2, \dots, p_m and let \tilde{g} be the GCD of p and q . Clearly, if (2) holds, then (1) has no solution. Hence, let us assume that (2) does not hold. Thus, we have that $\deg(p) \geq 1$ and p does not divide any power of q .

By Corollary 2.2.2, if $\tilde{g} = 1$ then every root $x \in \mathbb{K}$ of p satisfies $q(x) \neq 0$. Such $x \in \mathbb{K}$ exists by the Fundamental Theorem of Algebra and it is a solution to (1). If $\deg(\tilde{g}) \geq 1$, then let \tilde{p} and s be polynomials such that $p = \tilde{q}\tilde{p}$ and $q = \tilde{q}s$.

We claim that $\deg(\tilde{p}) \geq 1$ and \tilde{p} does not divide any power of \tilde{q} . Indeed, if $\deg(\tilde{p}) = 0$ then \tilde{p} is a constant and p divides \tilde{q} , whence p divides q which is a contradiction. Now, if \tilde{p} divides $(\tilde{q})^\ell$ for some integer $\ell \geq 1$, then $p = \tilde{p}\tilde{q}$ divides $q^{\ell+1} = \tilde{q}(\tilde{q})^\ell s^{\ell+1}$ which is a contradiction.

Notice that $\deg(p) + \deg(q) > \deg(\tilde{p}) + \deg(\tilde{q})$. Moreover, if $x \in \mathbb{K}$ is a solution to the system $\tilde{p}(x) = 0, \tilde{q}(x) \neq 0$, then $p(x) = 0$ and $q(x) \neq 0$. This follows from the fact that \tilde{q} is the GCD of p and q . Hence, we have reduced the problem to a problem involving polynomials of smaller degree. We continue this process by setting $p := \tilde{p}$ and $q := \tilde{q}$ until the GCD of p and q equals the constant 1. In this final instance, any root of p will be a solution to (1). □

Example 2.2.4. The results of Theorem 2.2.3 may not be true if \mathbb{K} is not algebraically closed or if the integer ℓ is fixed to some constant. For example, let $p = (x^2 + 1)^{\ell+1}$ and $q = (x^2 + 1)$, then the system $p(x) = 0, q(x) \neq 0$ has no solution in \mathbb{R} and there is not a polynomial $r(x)$ such that

$$(x^2 + 1)^{\ell+1} r(x) = (x^2 + 1)^\ell.$$

It is important to mention that the proof of Theorem 2.2.3 gives us an algorithm to detect whether a system of univariate polynomial equations has a solution or not, in which case, finds a certificate of infeasibility:

Algorithm 2.2.3: Univariate Nullstellensatz Algorithm (UniNull)

Data: Polynomials $p_1, p_2, \dots, p_m, q \in \mathbb{K}[x]$

Result: A certificate of infeasibility $r_1, \dots, r_m \in \mathbb{K}[x], \ell \geq 1$ or statement that the system is feasible.

```
1  $[p, r_1, \dots, r_m] := \text{GCD}(p_1, p_2, \dots, p_m)$ ;
2 if  $p = 0$  then
3   if  $q = 0$  then
4     return:  $\ell = 1, r_1 = \dots = r_m = 0$ ;
5   else
6     return: The system is feasible. Some integer  $x \in [\text{deg}(g) + 1]$  is a solution. ;
7 else
8    $\tilde{p} := p; \tilde{q} := q; \ell = 1$ ;
9   while  $STOP = 0$  do
10    if  $\text{deg}(\tilde{p}) = 0$  then
11       $r := \frac{q^\ell}{p}$ ;
12       $r_1 := rr_1, r_2 := rr_2, \dots, r_m := rr_m$ ;
13      return:  $r_1, \dots, r_m, \ell; STOP = 1$ ;
14    else if  $\text{deg}(\tilde{q}) = 0$  then
15      return: System is feasible, any root of  $\tilde{p}$  gives a solution;  $STOP = 1$ ;
16    else
17       $[\tilde{q}, q_1, q_2] := \text{GCD}(\tilde{p}, \tilde{q})$ ;
18       $\tilde{p} := \frac{\tilde{p}}{\tilde{q}}$ ;
19       $\ell := \ell + 1$ ;
```

2.3 Hilbert's Nullstellensatz

In this section we will prove the multivariate version of Theorem 2.2.3. The proof we are presenting here is due to Enrique Arrondo ([4]) and it is one of the simplest proofs found in the literature. For the proof we will need two easy technical lemmas. The first of them is the *Noether Normalization Lemma*:

Lemma 2.3.1. *Let p be a polynomial in $\mathbb{K}[x_1, x_2, \dots, x_n]$ of degree $d \geq 1$ with \mathbb{K} alge-*

braically closed. Then, there exist some $\lambda_1, \lambda_2, \dots, \lambda_{n-1}$ in \mathbb{K} such that

$$p(x_1 + \lambda_1 x_n, x_2 + \lambda_2 x_n, \dots, x_{n-1} + \lambda_{n-1} x_n, x_n) = cx_n^d + \dots \text{ other terms where degree of } x_n \text{ is less than } d, \quad (2.3.1)$$

where c is a nonzero constant in \mathbb{K} .

Proof. Suppose that

$$p(x_1, \dots, x_n) = \sum_{|\alpha| \leq d} c_\alpha x^\alpha,$$

for some $c_\alpha \in \mathbb{K}$ and multi-indexes $\alpha \in \mathbb{Z}^n$. Then,

$$\begin{aligned} p(x_1 + \lambda_1 x_n, \dots, x_{n-1} + \lambda_{n-1} x_n, x_n) &= \sum_{|\alpha|=d} c_\alpha (x_1 + \lambda_1 x_n)^{\alpha_1} \cdots (x_{n-1} + \lambda_{n-1} x_n)^{\alpha_{n-1}} x_n^{\alpha_n} + \dots \\ &\quad \cdots + \text{other terms where degree of } x_n \text{ is less than } d, \\ &= \left(\sum_{|\alpha|=d} c_\alpha \lambda_1^{\alpha_1} \cdots \lambda_{n-1}^{\alpha_{n-1}} \right) x_n^d + \dots \\ &\quad \cdots + \text{other terms where degree of } x_n \text{ is less than } d. \end{aligned}$$

Now, the polynomial $q(\lambda_1, \dots, \lambda_{n-1}) = \sum_{|\alpha|=d} c_\alpha \lambda_1^{\alpha_1} \cdots \lambda_{n-1}^{\alpha_{n-1}}$ in $\mathbb{K}[\lambda_1, \dots, \lambda_{n-1}]$ has at least one non-zero coefficient and hence it is non-zero at some constants $\lambda_1^*, \dots, \lambda_{n-1}^* \in \mathbb{K}$. This can be proven by induction on n and using the fact that \mathbb{K} is not finite (since it is algebraically closed). \square

The second result involves the *resultant* of two polynomials. Given two polynomials

$$\begin{aligned} p &= p_d x_n^d + p_{d-1} x_n^{d-1} + \cdots + p_1 x_n + p_0, \\ q &= q_e x_n^e + q_{e-1} x_n^{e-1} + \cdots + q_1 x_n + q_0, \end{aligned}$$

for some $p_0, \dots, p_d, q_0, \dots, q_e \in \mathbb{K}[x_1, x_2, \dots, x_{n-1}]$ and $d, e \geq 0$, the resultant of p and q is

the polynomial in $\mathbb{K}[x_1, x_2, \dots, x_{n-1}]$ defined as

$$R_{p,q} := \det \begin{pmatrix} p_0 & p_1 & \dots & p_d & 0 & 0 & \dots & 0 \\ 0 & p_0 & \dots & p_{d-1} & p_d & 0 & \dots & 0 \\ & & \ddots & & & & & \\ 0 & \dots & 0 & p_0 & p_1 & \dots & p_{d-1} & p_d \\ q_0 & q_1 & \dots & q_{e-1} & q_e & 0 & \dots & 0 \\ 0 & q_0 & \dots & q_{e-2} & q_{e-1} & q_e & \dots & 0 \\ & & \ddots & & & & & \\ 0 & \dots & 0 & q_0 & q_1 & \dots & q_{e-1} & q_e \end{pmatrix}_{(d+e) \times (d+e)}. \quad (2.3.2)$$

The resultant has many applications in algebraic geometry. It is a useful tool if one wants to determine whether two multivariate polynomials have a common factor: $R_{p,q} = 0$ if and only if there exist some polynomials s, r_1, r_2 such that $p = sr_1$ and $q = sr_2$ (see Chapter 3 of [14] for this and some more properties of the resultant).

Lemma 2.3.2. *Let p and q be two polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$. Then, the resultant of p and q belongs to the ideal $\langle p, q \rangle_{\mathbb{K}}$.*

Proof. For every $j \in [d+e]$ multiply the j -th column of the matrix in (2.3.2) by x_n^{j-1} and add it to the first column. After these column operations, the i -th component of the first column will be equal to $x_n^{i-1}p$ for $1 \leq i \leq e$ and equal to $x_n^{i-1}q$ for $e+1 \leq i \leq e+d$. Clearly, these column operations don't affect the determinant of the matrix (2.3.2) and as a result

$$R_{p,q} = \det \begin{pmatrix} p & p_1 & \dots & p_d & 0 & 0 & \dots & 0 \\ x_n p & p_0 & \dots & p_{d-1} & p_d & 0 & \dots & 0 \\ & & \ddots & & & & & \\ x_n^{e-1} p & \dots & 0 & p_0 & p_1 & \dots & p_{d-1} & p_d \\ x_n^e q & q_1 & \dots & q_{e-1} & q_e & 0 & \dots & 0 \\ x_n^{e+1} q & q_0 & \dots & q_{e-2} & q_{e-1} & q_e & \dots & 0 \\ & & \ddots & & & & & \\ x_n^{e+d-1} q & \dots & 0 & q_0 & q_1 & \dots & q_{e-1} & q_e \end{pmatrix}_{(d+e) \times (d+e)}. \quad (2.3.3)$$

If we expand the determinant (2.3.3) over the first column, we obtain that

$$R_{p,q} = \sum_{i=1}^e x_n^{i-1} p s_i + \sum_{i=e+1}^{e+d} x_n^{i-1} q s_i,$$

for some polynomials $s_i \in \mathbb{K}[x_1, x_2, \dots, x_{n-1}]$. Therefore, $R_{p,q} \in \langle p, q \rangle_{\mathbb{K}}$ and the result follows. \square

Now, we are ready to prove the Nullstellensatz:

Theorem 2.3.3 (Weak Hilbert's Nullstellensatz). *Let I be an ideal of $\mathbb{K}[x_1, x_2, \dots, x_n]$ with \mathbb{K} algebraically closed. Then, exactly one of the following holds:*

1. *There exist some $x \in \mathbb{K}$ such that $p(x) = 0$ for all $p \in I$.*
2. *$I = \mathbb{K}[x_1, x_2, \dots, x_n]$.*

Proof. The proof is by induction on the number of variables. The case $n = 1$ is easy due to Theorem 2.2.3. Indeed, let I be any ideal of $\mathbb{K}[x]$ and let q be a non-zero polynomial in I with the smallest degree possible (if $I = \{0\}$ the result is trivial). Then, given any other polynomial $p \in I$, the division algorithm (Proposition 2.2.1) states that $p = sq + r$ for some $r \in \mathbb{K}[x]$ with $\deg(r) < \deg(q)$. By the minimality of q , r has to be equal to zero and $I = \langle q \rangle_{\mathbb{K}}$. Since I is a finitely generated ideal, we can use Theorem 2.2.3.

Now, suppose that we have proven the statement for any ideal of $\mathbb{K}[x_1, \dots, x_{n-1}]$ and let I be any ideal in $\mathbb{K}[x_1, \dots, x_n]$. Moreover, suppose that $I \neq \mathbb{K}[x_1, \dots, x_n]$ (i.e. it is a proper ideal) and let us prove the existence of some $x \in \mathbb{K}^n$ such that $p(x) = 0$ for all $p \in I$.

Since $I \neq \mathbb{K}[x_1, \dots, x_n]$, there exists some polynomial $q \in I$ of degree $e \geq 1$. By Lemma 2.3.1, we can make a change of variables $y_1 := x_1 + \lambda_1 x_n$, $y_2 := x_2 + \lambda_2 x_n$, \dots , $y_{n-1} = x_{n-1} + \lambda_{n-1} x_n$, $y_n = \lambda_n x_n$ such that

$$q(y_1, \dots, y_n) = y_n^e + (\text{other terms where degree of } y_n \text{ is less than } e)$$

for some $\lambda_1, \dots, \lambda_n$ in \mathbb{K} . Let \tilde{I} be the ideal of all polynomials of the form $p(y_1, \dots, y_n)$ with $p \in I$. Then, if we prove the existence of some $y \in \mathbb{K}^n$ such that $p(y) = 0$ for all $p \in \tilde{I}$, then $x_i = y_i - \frac{\lambda_i}{\lambda_n} y_n$ for $i \in [n-1]$ and $x_n = \frac{1}{\lambda_n} y_n$ will be our desired solution (notice that $\lambda_n \neq 0$ by construction).

Let \tilde{J} be the ideal of all polynomials $p \in \tilde{I} \cap \mathbb{K}[y_1, \dots, y_{n-1}]$. Clearly, the constant polynomial 1 is not in \tilde{J} since this would imply that $1 \in \tilde{I}$ and as a consequence $1 \in I$, contradicting our assumptions on I . In particular, \tilde{J} is a proper ideal of $\mathbb{K}[y_1, \dots, y_{n-1}]$ and by our induction hypothesis, there is some y_1^*, \dots, y_{n-1}^* such that

$$p(y_1^*, \dots, y_{n-1}^*) = 0, \quad \forall p \in \tilde{J}.$$

We claim that there exists some $y_n^* \in \mathbb{K}$ such that $p(y_1^*, \dots, y_{n-1}^*, y_n^*) = 0$ for all $p \in \tilde{I}$. Indeed, if no such $y_n^* \in \mathbb{K}$ exists, then by the case $n = 1$, there is some $p \in \tilde{I}$ of degree d

such that $p(y_1^*, \dots, y_{n-1}^*, y_n) = 1$ for all $y_n \in \mathbb{K}$. By Lemma 2.3.2, the resultant $R_{p,q}$ of p and q is an element of \tilde{J} . Moreover, by the way we chose q ,

$$R_{p,q} = \det \begin{pmatrix} p_0 & p_1 & \dots & p_d & 0 & 0 & \dots & 0 \\ 0 & p_0 & \dots & p_{d-1} & p_d & 0 & \dots & 0 \\ & & \ddots & & & & & \\ 0 & \dots & 0 & p_0 & p_1 & \dots & p_{d-1} & p_d \\ q_0 & q_1 & \dots & q_{e-1} & 1 & 0 & \dots & 0 \\ 0 & q_0 & \dots & q_{e-2} & q_{e-1} & 1 & \dots & 0 \\ & & \ddots & & & & & \\ 0 & \dots & 0 & q_0 & q_1 & \dots & q_{e-1} & 1 \end{pmatrix}_{(d+e) \times (d+e)}, \quad (2.3.4)$$

for some $p_0, \dots, p_d, q_0, \dots, q_{e-1} \in \mathbb{K}[y_1, y_2, \dots, y_{n-1}]$ such that

$$\begin{aligned} p &= p_d y_n^d + p_{d-1} y_n^{d-1} + \dots + p_1 y_n + p_0, \\ q &= y_n^e + q_{e-1} y_n^{e-1} + \dots + q_1 y_n + q_0. \end{aligned}$$

However, if we plug in the values y_1^*, \dots, y_{n-1}^* in equation (2.3.4), we will obtain a lower triangular matrix with diagonal entries equal to 1. In particular, $R_{p,q}(y_1^*, \dots, y_{n-1}^*) = 1$ and this contradicts our induction hypothesis. The proof follows. \square

Remark 2.3.4. Notice that the above proof needed the second definition of ideal (Definition 2.1.8). We used it strongly when stating that the set \tilde{J} was an ideal of $\mathbb{K}[y_1, \dots, y_n]$. Of course, as we mentioned before, this technicality can be omitted since every ideal is a finitely generated ideal by Hilbert's Basis Theorem.

Now, let us prove a more general version of the Nullstellensatz:

Theorem 2.3.5 (Hilbert's Nullstellensatz). *Let p_1, p_2, \dots, p_m and q be non-zero polynomials in $\mathbb{K}[x_1, \dots, x_n]$ with \mathbb{K} algebraically closed. Then, exactly one of the following holds:*

1. *The system of equations $p_1(x) = p_2(x) = \dots = p_m(x) = 0, q(x) \neq 0$ has a solution in \mathbb{K}^n .*
2. *There exist polynomials r_1, r_2, \dots, r_m in $\mathbb{K}[x_1, \dots, x_n]$ and some integer $\ell \geq 1$ such that*

$$q^\ell = r_1 p_1 + r_2 p_2 + \dots + r_m p_m. \quad (2.3.5)$$

Proof. Suppose that (1) does not hold and consider the ideal

$$I := \langle p_1, p_2, \dots, p_m, 1 - tq \rangle_{\mathbb{K}} \subseteq \mathbb{K}[x_1, \dots, x_n, t].$$

We claim that $I = \mathbb{K}[x_1, \dots, x_n, t]$. Indeed, suppose that I is a proper ideal of $\mathbb{K}[x_1, \dots, x_n, t]$. Then, by the Weak Nullstellensatz (Theorem 2.3.3), there exist some $x^* \in \mathbb{K}^n$ and $t^* \in \mathbb{K}$ such that

$$p_1(x^*) = p_2(x^*) = \dots = p_m(x^*) = 1 - t^*q(x^*) = 0.$$

However, this implies that $q(x^*) \neq 0$ contradicting our initial hypothesis. Therefore, there exist polynomials $r_1, r_2, \dots, r_m, s \in \mathbb{K}[x_1, \dots, x_n, t]$ such that

$$r_1(x, t)p_1(x) + r_2(x, t)p_2(x) + \dots + r_m(x, t)p_m(x) + s(x, t)(1 - tq(x)) = 1, \quad \forall x \in \mathbb{K}^n, t \in \mathbb{K}. \quad (2.3.6)$$

But then, setting $t = \frac{1}{q(x)}$ and multiplying both sides by a proper power of $q(x)$ we obtain the desired equality. \square

Remark 2.3.6. *Hilbert proved the Nullstellensatz in the context of the Theory of Algebraic Invariants. His original proof (in German) can be found in [31]. An English translation can be found in [32]. See also [38] for a very nice historical note on Hilbert's contributions to algebraic invariants.*

The set of polynomials r_1, \dots, r_m appearing in (2.3.5) is called a **Nullstellensatz Certificate** for the insolubility of the system $p_1(x) = p_2(x) = \dots = p_m(x) = 0, g(x) \neq 0$. Notice that the constant $\ell \geq 1$ found in the proof of Theorem 2.3.5 is bounded above by the maximum degree of the polynomials r_1, \dots, r_m in (2.3.6). We say that a system of polynomial equalities has a Nullstellensatz certificate of degree d if there exists a Nullstellensatz certificate r_1, \dots, r_m of polynomials of degree at most d .

Our main goal throughout this thesis is to study Nullstellensatz certificates of small degree for certain systems of polynomial equations arising from combinatorial problems. At a first glance, there is no reason to think that the degrees of the Nullstellensatz certificates are uniformly bounded for systems of a given dimension. Surprisingly, the following deep result by Kollar shows that this is the case:

Theorem 2.3.7 (Kollar [34]). *Let $p_1, \dots, p_m \in \mathbb{K}[x_1, \dots, x_n]$ polynomials with no common zeros with \mathbb{K} algebraically closed. Let $d := \max\{\deg(p_i) : i \in \{1, \dots, m\}\}$ be the maximum degree of these polynomials. Then, there exists a Nullstellensatz certificate of degree*

$$d_B := \max(3, d)^{\min(n, m)} \quad (2.3.7)$$

In particular, Theorem 2.3.7 implies that we can determine whether a system of polynomial equations over the complex numbers has a solution or not, by using a large but finite system of *linear* equations. Indeed, if we set polynomials $r_i = \sum_{|\alpha| \leq d_B} c_{i,\alpha} x^\alpha$ for $i \in [m]$, then the equation

$$r_1 p_1 + r_2 p_2 + \cdots + r_m p_m = 1,$$

will be a system of linear equations over the variables $c_{i,\alpha}$.

Example 2.3.8. Consider the following system of polynomial equations over \mathbb{C}^3 :

$$\begin{aligned} p_1(x, y, z) &:= xy - 1 = 0, \\ p_2(x, y, z) &:= xz - 1 = 0, \\ p_3(x, y, z) &:= y - z - 1 = 0. \end{aligned} \tag{2.3.8}$$

Then, we see that (2.3.8) has no solution as the equations $p_1(x, y, z) = p_2(x, y, z) = 0$ imply $y = z$, but the equation $p_3(x, y, z) = 0$ implies $y \neq z$. Let us see if (2.3.8) has a Nullstellensatz Certificate of degree at most one. In order to do this, we create the following system of equations:

$$\begin{aligned} (a_1 + a_x x + a_y y + a_z z)(xy - 1) + (b_1 + b_x x + b_y y + b_z z)(xz - 1) + \cdots \\ \cdots + (c_1 + c_x x + c_y y + c_z z)(y - z - 1) = 1. \end{aligned} \tag{2.3.9}$$

Which can be written in tableau (zeros omitted) form as follows

	a_1	a_x	a_y	a_z	b_1	b_x	b_y	b_z	c_1	c_x	c_y	c_z			Cert.
1	-1				-1				-1				1		1
x		-1				-1				-1					
y			-1				-1		1		-1				$\frac{1}{2}$
z				-1				-1	-1			-1			$-\frac{1}{2}$
y^2											1				
z^2												-1			
xy	1									1					1
xz					1					-1					1
yz											-1	1			$-\frac{1}{2}$
$x^2 y$		1													
$x^2 z$						1									
xy^2			1												$\frac{1}{2}$
xz^2				1				1							$-\frac{1}{2}$
xyz							1								$\frac{1}{2}$

This system is infeasible and the rightmost column of the tableau shows a certificate of infeasibility of the system. Thus, we need to increase the degree of the polynomials defining our system and consider polynomials of degree at most two,

$$(a_1 + a_x x + \cdots + a_{yz} yz +)(xy - 1) + (b_1 + b_x x + \cdots + b_{yz} yz +)(xz - 1) + \cdots \\ (c_1 + c_x x + \cdots + c_{yz} yz +)(y - z - 1) = 1. \quad (2.3.10)$$

This system has size 20×30 and it is too big to show here. However, the following tableau shows a few columns of this system,

	a_1	a_y	b_y	c_{xy}	
1	-1				1
y		-1	1		
xy	1			1	
xy^2		1		1	
xyz			-1	-1	
	-1	1	-1	-1	

Thus, (2.3.8) has a Nullstellensatz Certificate of degree two given by

$$(-1 + y)(xy - 1) - y(xz - 1) - xy(y - z - 1) = 1.$$

We need to point out that Kollar's bounds are in fact sharp and thus, the system of linear equations used to find a Nullstellensatz Certificates might end up being huge. However, for some special cases, namely when the polynomials do not have a *common root at infinity*, Lazard [8] proved that it is possible to obtain much better bounds for the degrees of the certificates.

Definition 2.3.9. Let p be a polynomial in $\mathbb{K}[x_1, x_2, \dots, x_n]$ of degree d . The **homogenization** of p is the polynomial $\tilde{p} \in \mathbb{K}[x_0, x_1, \dots, x_n]$ defined by

$$\tilde{p}(x) = x_0^d p\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

A point $x \in \mathbb{K}^n \setminus \{0\}$ is called a **root of p at infinity** if $\tilde{p}(0, x) = 0$.

Example 2.3.10. Consider the polynomial $p(x_1, x_2) := x_1^2 - x_2$ in $\mathbb{C}[x_1, x_2]$. Then, the homogenization of p is the polynomial

$$\tilde{p}(x_0, x_1, x_2) := x_1^2 - x_2 x_0.$$

Moreover, for every $y \in \mathbb{C} \setminus \{0\}$ the point $(0, y)$ is a root of p at infinity since $\tilde{p}(0, y, 0) = 0$.

Theorem 2.3.11 (Lazard, see [8]). *Let $p_1, \dots, p_m \in \mathbb{C}[x_1, \dots, x_n]$ be polynomials having no common roots and no common roots at infinity. Let $d := \max\{\deg(p_i) : i \in \{1, \dots, m\}\}$. Then, there exists a Nullstellensatz certificate of degree*

$$d_L := n(d - 1). \tag{2.3.11}$$

The proof of Lazard's theorem uses advance techniques from Algebraic Geometry and Cohomological Algebra that go beyond the scope of this thesis. Nevertheless, it is not hard to prove Lazard's theorem for systems of polynomial equations coming from combinatorial problems (see Proposition 4.1.1).

Notice that Theorem 2.3.11 is more restrictive than Theorem 2.3.7 as two polynomials may have common roots at infinity while having no roots in common. For instance, consider the polynomials $p(x_1, x_2) := x_1^2 - x_2$ and $q(x_1, x_2) := x_1^2 x_2 - x_2^2 + 1$. Then, p and q have no common roots as $q = x_2 p + 1$. However, after homogenization, we have that $\tilde{p}(0, x, y) = x^2$ and $\tilde{q}(0, x, y) = x^2 y$, thus every $(0, y)$ with $y \neq 0$ is a root of p and q at infinity.

This great improvement on the upper bound d_B is still very useful. As we will see in Chapter 4 and Chapter 5, this theorem applies to systems of polynomials coming from the combinatorial optimization problems studied in this thesis.

Chapter 3

Fourier Analysis for Finite Abelian Groups

In this chapter we develop an important tool to understand Nullstellensatz Certificates arising from some special types of varieties (see Chapter 5). Since every monomial x^α of $\mathbb{K}[x_1, \dots, x_n]$ is completely characterized by the multi-index $\alpha \in \mathbb{Z}^n$, it will be useful to study the set of multi-indexes appearing in a given polynomial. An example of this relationship was given by Bruce Reznick ([49]), who showed that the convex hull $C(p)$ of all the multi-indexes appearing in a given *homogeneous polynomial* $p = \sum_j h_j^2$ satisfies the inclusions $C(h_j) \subseteq \frac{1}{2}C(p)$ for every j . This result has a great practical use when one wants to determine if a non-negative polynomial is a sum of squares (see [48]). As we will see in the following chapters, the strong connection between multi-indexes and polynomials will allow us to transform a system of polynomial equations into a system of functions over abelian groups and vice-versa.

Throughout this chapter $(\Gamma, +, 0)$ will denote a finite additive abelian group with identity equal to 0. Simple examples of finite abelian groups are the group \mathbb{Z}_k of integers modulo k and direct products of these. In fact, it is a well known result of group theory that up to isomorphism, these are the only examples of finite abelian groups. That is, every finite abelian group Γ is isomorphic to a direct product

$$\Gamma \simeq \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n},$$

for some integers $k_1, \dots, k_n \geq 1$. Thus, the elements of an abelian group Γ will be denoted in the same way as multi-indices, i.e. we will use Greek letters $\alpha, \beta, \gamma, \dots$ to denote them. The *multiplicative group of complex numbers* is the group $(\mathbb{C}^\times, \cdot, 1)$ where $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$

and \cdot is the usual multiplication of complex numbers. For a complex number $c = a + ib$ with $a, b \in \mathbb{R}$ we let $\bar{c} = a - ib$ be its *complex conjugate*.

Most of the results and definitions found in this chapter are taken from the books [56] and [28]. Nevertheless, the idea of using Fourier Analysis for the study of Hilbert Nullstellensatz was inspired by a recent work of Hamza Fawzi, Pablo Parrilo and James Saunderson ([25]). They used Fourier transform techniques along with some chordal coverings of Cayley graphs to obtain sparse sum of squares certificates for non-negative functions over the hypercube \mathbb{Z}_2^n and the groups \mathbb{Z}_k with $k \geq 1$.

3.1 Characters and the Dual Group

A powerful tool often used in mathematics is the notion of suitably defined *dual spaces*. For example, given a vector space V over the field \mathbb{C} , the dual space V^* is defined as the vector space of all linear functions $f : V \rightarrow \mathbb{C}$ over the field \mathbb{C} . It is a well known fact, that many problems involving structures in the space V usually have some “dual” interpretation concerning structures over the space V^* . This new interpretation often lead to simpler solutions to the problem and a more deeper understanding of the structures involved on it. For instance, using duality arguments one can show very easily that every bounded *polyhedron* (the intersection of finitely many closed half-spaces) is equal to the convex hull of a finite set of points, i.e. a *polytope*.

The main task of the this section is to construct a notion of duality for finite abelian groups. As in vector spaces, we will construct such dual using the vector space $L^2(\Gamma)$ of complex-valued functions $f : \Gamma \rightarrow \mathbb{C}$ as follows:

Definition 3.1.1. A *character* of Γ is a complex-valued function $\kappa \in L^2(\Gamma)$ such that:

1. $\kappa(\alpha) \neq 0$ for every $\alpha \in \Gamma$,
2. $\kappa(\alpha + \beta) = \kappa(\alpha)\kappa(\beta)$ for all $\alpha, \beta \in \Gamma$.

In other words, characters are group homomorphisms from $(\Gamma, +, 0)$ to the multiplicative group $(\mathbb{C}^\times, \cdot, 1)$. We let $\widehat{\Gamma}$ be the set of characters of Γ .

Clearly, $\widehat{\Gamma}$ is non-empty since the function κ_0 , defined as $\kappa_0(\alpha) := 1$ for all $\alpha \in \Gamma$, is a character of Γ .

Example 3.1.2. Let $(\Gamma, +, 0) := (\mathbb{Z}_3, +, 0)$ be the group of integers modulo 3. Then, for every $\kappa \in \widehat{\mathbb{Z}_3}$ and every element $\alpha \in \mathbb{Z}_3$ we have $\kappa(\alpha) = \kappa(\alpha + 0) = \kappa(\alpha)\kappa(0)$ and $\kappa(0) = \kappa(3\alpha) = [\kappa(\alpha)]^3$. Hence, $\kappa(0) = 1$ and $\kappa(\alpha)$ is a 3-th root of the unity for every $\alpha \in \mathbb{Z}_3$. If $\kappa(1) = e^{r\frac{2\pi i}{3}}$, then $\kappa(2) = [\kappa(1)]^2 = e^{2r\frac{2\pi i}{3}}$. In particular,

$$\widehat{\mathbb{Z}_3} = \left\{ e^{r\cdot\alpha\frac{2\pi i}{3}} : r \in \mathbb{Z}_3 \right\}.$$

From the above example we see that $\widehat{\mathbb{Z}_3}$ can be seen as a finite abelian group. This is no coincidence as the following lemma shows

Lemma 3.1.3. Let $\widehat{\Gamma}$ be the set of characters of a finite abelian group Γ . Then, $(\widehat{\Gamma}, \cdot, \kappa_0)$ is a finite abelian group, called the **dual group** of Γ , where \cdot denotes the usual product of complex-valued functions and κ_0 is the constant character defined as above.

Proof. Let $(\Gamma, +, 0)$ be a finite abelian group. Then, for every $\alpha \in \Gamma$ we have that

$$|\Gamma|\alpha = \underbrace{\alpha + \cdots + \alpha}_{|\Gamma| \text{ times}} = 0.$$

Since for every $\alpha \in \Gamma$ and $\kappa \in \widehat{\Gamma}$ we have that $\kappa(\alpha) \neq 0$, the equalities $\kappa(0) = 1$ and $[\kappa(\alpha)]^{|\Gamma|} = 1$ must hold. This implies that the image of every character is a subset of the $|\Gamma|$ -roots of the unity and $\widehat{\Gamma}$ must be finite.

For every pair of characters $\kappa, \kappa' \in \widehat{\Gamma}$ their multiplication $\kappa\kappa'$ is clearly a character. For every character $\kappa \in \widehat{\Gamma}$, the conjugate $\bar{\kappa}$ is also a character. Since $|\kappa(\alpha)| = 1$ for every $\alpha \in \Gamma$, then $\kappa\bar{\kappa} = \kappa_0$. Thus, every character has an inverse.

The fact that $\widehat{\Gamma}$ is an abelian group easily follows from the commutativity of $(\mathbb{C}^\times, \cdot, 1)$. \square

A very useful property of characters is that they separate points. That is, for every pair of distinct α and β in Γ , one can find some character κ such that $\kappa(\alpha) \neq \kappa(\beta)$. This property will be useful to prove that in fact $\widehat{\Gamma}$ forms an *orthonormal basis* for $L^2(\Gamma)$ (see Theorem 3.2.1).

Lemma 3.1.4. Suppose that $|\Gamma| \geq 2$. Then, for every $\alpha \in \Gamma \setminus \{0\}$ there exists some character $\kappa \in \widehat{\Gamma}$ satisfying $\kappa(\alpha) \neq 1$.

Proof. Let α be any non-zero element of Γ . We will prove the existence of the desired character by induction over the size of all subgroups of Γ containing α . The base case is easy, as for the subgroup $\Gamma_0 = \{k\alpha : k \in \{1, 2, \dots, |\Gamma|\}\}$ the function

$$\kappa(k\alpha) := e^{k\frac{2\pi i}{|\Gamma_0|}} \quad \forall k\alpha \in \Gamma_0,$$

defines a character of Γ_0 with $\kappa(\alpha) \neq 1$. Notice that κ is well defined since given any pair $k, k' \in \{1, 2, \dots, |\Gamma|\}$ satisfying $k\alpha = k'\alpha$, the congruence $k \equiv k' \pmod{|\Gamma_0|}$ must hold.

Now, suppose that for some proper subgroup $\Gamma_0 \subset \Gamma$ containing α , we have proved the existence of some $\kappa \in \widehat{\Gamma}_0$ with $\kappa(\alpha) \neq 1$. Let β be any element of $\Gamma \setminus \Gamma_0$ and consider the subgroup

$$\Gamma_1 := \{\eta + k\beta : \eta \in \Gamma_0, k \in \{1, 2, \dots, |\Gamma|\}\}.$$

Notice that Γ_1 is the smallest subgroup containing both β and the elements of Γ_0 .

Let $\ell \geq 1$ be the smallest integer such that $\ell\beta \in \Gamma_0$. Clearly, ℓ is well defined as $|\Gamma|\beta = 0 \in \Gamma_0$. Let $z \in \mathbb{C}$ be any ℓ -root of $\kappa(\ell\beta)$ and define

$$\tilde{\kappa}(\eta + k\beta) := \kappa(\eta)z^k.$$

We claim that $\tilde{\kappa}$ is a character of Γ_1 with $\tilde{\kappa}(\alpha) \neq 1$. First, let us show that $\tilde{\kappa}$ is well defined. Indeed, suppose that $\eta + k\beta = \eta' + k'\beta$ for some $\eta, \eta' \in \Gamma_0$ and $k, k' \in \{1, 2, \dots, |\Gamma|\}$. Thus, $(k - k')\beta = (\eta - \eta') \in \Gamma_1$ and by the minimality of ℓ , we can write $k = k' + r\ell$ and $\eta = \eta' + r\ell\beta$ for some integer $r \in \mathbb{Z}$. In particular,

$$\begin{aligned} \tilde{\kappa}(\eta' + k'\beta) &= \kappa(\eta')z^{k'}, \\ &= \kappa(\eta')\kappa(r\ell\beta)z^k, \\ &= \kappa(\eta)z^k = \tilde{\kappa}(\eta + k\beta), \end{aligned} \tag{3.1.1}$$

and $\tilde{\kappa}$ is well defined. It is straightforward to check that $\tilde{\kappa}$ satisfies conditions 1. and 2. of Definition 3.1.1. Moreover, $\tilde{\kappa}(\alpha) = \kappa(\alpha) \neq 1$ and hence, it defines a character of Γ_1 . The proof follows. \square

Corollary 3.1.5. *Let α and β be two distinct elements of Γ . Then, there exists some $\kappa \in \widehat{\Gamma}$ such that $\kappa(\alpha) \neq \kappa(\beta)$.*

Proof. By Lemma 3.1.4, there is some $\kappa \in \widehat{\Gamma}$ such that $\kappa(\alpha - \beta) \neq 1$. Then, $\kappa(\alpha) \neq \kappa(\beta)$. \square

We have to point out that the proof of Lemma 3.1.4 gives us a general technique to lift characters of proper subgroups into the group itself. More concretely, given any subgroup Γ_0 of Γ and any character $\kappa \in \widehat{\Gamma}_0$, we can generate some $\tilde{\kappa} \in \widehat{\Gamma}$ such that $\tilde{\kappa}(\alpha) = \kappa(\alpha)$ for every $\alpha \in \Gamma_0$. Clearly, the way $\tilde{\kappa}$ was constructed in the proof of Lemma 3.1.4 is not unique, since in the process of its construction, we selected arbitrary roots of some previously determined complex number (e.g. the number $z \in \mathbb{C}$ in the proof). However, we can enumerate the number of such lifts as follows.

Corollary 3.1.6. *Let Γ_0 be a subgroup of Γ and let $\kappa \in \widehat{\Gamma}_0$. The number of lifts $\tilde{\kappa} \in \widehat{\Gamma}$ satisfying $\tilde{\kappa}(\alpha) = \kappa(\alpha)$ for every $\alpha \in \Gamma_0$ is equal to*

$$\frac{|\Gamma|}{|\Gamma_0|}.$$

Proof. The proof is by backwards induction on the size of Γ_0 , with the case $\Gamma_0 = \Gamma$ being trivial. Now, suppose that Γ_0 is any proper subgroup of Γ and let $\beta \in \Gamma \setminus \Gamma_0$. As in the proof of Lemma 3.1.4 let

$$\Gamma_1 := \{\eta + k\beta : \eta \in \Gamma_0, k \in \{1, 2, \dots, |\Gamma|\}\},$$

and suppose that $\ell\beta \in \Gamma_0$ for some minimal $\ell \geq 0$. Then, it is easy to see from the proof of Lemma 3.1.4 that the number of lifts from any character of Γ_0 to Γ_1 is equal to

$$\ell = \frac{|\Gamma_1|}{|\Gamma_0|}.$$

By our inductive hypothesis, the number of lifts from any character of Γ_1 to Γ is equal to $\frac{|\Gamma|}{|\Gamma_1|}$. Hence, the number of lifts from any character of Γ_0 to Γ is equal to $\frac{|\Gamma|}{|\Gamma_0|}$ and the proof follows. \square

3.2 The Fourier Transform

In order to have a better understanding of the dual group, it is useful to give $L^2(\Gamma)$ a more algebraic structure. Notice that $L^2(\Gamma)$ is a finite dimensional vector space over \mathbb{C} isomorphic to $\mathbb{C}^{|\Gamma|}$. The canonical basis of $L^2(\Gamma)$ is given by the set of all *Dirac Delta* functions

$$\delta_\beta(\alpha) := \begin{cases} 1 & \text{if } \alpha = \beta, \\ 0 & \text{otherwise,} \end{cases}$$

defined for each $\beta \in \Gamma$. If we let μ be the uniform measure over the group Γ , then for every function $f \in L^2(\Gamma)$ we can define its integral as

$$\int_{\Gamma} f(\alpha) d\mu(\alpha) = \frac{1}{|\Gamma|} \sum_{\alpha \in \Gamma} f(\alpha).$$

This integral induces an inner product on $L^2(\Gamma)$ given by

$$\langle f, g \rangle := \int_{\Gamma} f(\alpha) \overline{g(\alpha)} d\mu(\alpha), \quad f, g \in L^2(\Gamma).$$

It turns out that the set of characters behaves well under this inner product.

Theorem 3.2.1. *The dual group $\widehat{\Gamma}$ forms an orthonormal basis for $L^2(\Gamma)$. In particular, $|\Gamma| = |\widehat{\Gamma}|$.*

Proof. Let $\kappa \in \widehat{\Gamma}$ be any character of Γ . From the proof of Lemma 3.1.3, we know that $|\kappa(\alpha)| = 1$ for every $\alpha \in \Gamma$. Therefore,

$$\langle \kappa, \kappa \rangle = \int_{\Gamma} \kappa(\alpha) \overline{\kappa(\alpha)} d\mu(\alpha) = \int_{\Gamma} |\kappa(\alpha)| d\mu(\alpha) = 1.$$

Now, let κ and κ' be different characters of Γ and let $\beta \in \Gamma$ be such that $\kappa'(\beta) \neq \kappa(\beta)$. Thus,

$$\begin{aligned} \langle \kappa', \kappa \rangle &= \int_{\Gamma} \kappa'(\alpha) \overline{\kappa(\alpha)} d\mu(\alpha) = \int_{\Gamma} \kappa'(\beta\alpha) \overline{\kappa(\beta\alpha)} d\mu(\alpha), \\ &= \kappa'(\beta) \overline{\kappa(\beta)} \langle \kappa', \kappa \rangle. \end{aligned}$$

Since $\kappa'(\beta)$ and $\kappa(\beta)$ are different non-zero complex numbers, the above equality can only hold when $\langle \kappa', \kappa \rangle = 0$. This proves that the characters are orthonormal under the inner product $\langle \cdot, \cdot \rangle$. It only remains to show that the dual group spans the whole space $L^2(\Gamma)$. To that end, let us prove that any Dirac Delta function can be written as a linear combination of characters. Moreover, we claim that

$$\delta_{\beta}(\alpha) = \frac{1}{|\widehat{\Gamma}|} \sum_{\kappa \in \widehat{\Gamma}} \overline{\kappa(\beta)} \kappa(\alpha), \quad \forall \beta \in \Gamma. \quad (3.2.1)$$

In order to see this, take any $\alpha \in \Gamma$ different from β . By Corollary 3.1.5, there exists some $\kappa' \in \widehat{\Gamma}$ such that $\kappa'(\alpha - \beta) \neq 1$. Hence,

$$\begin{aligned} \frac{1}{|\widehat{\Gamma}|} \sum_{\kappa \in \widehat{\Gamma}} \overline{\kappa(\beta)} \kappa(\alpha) &= \frac{1}{|\widehat{\Gamma}|} \sum_{\kappa \in \widehat{\Gamma}} \kappa(\alpha - \beta) \\ &= \frac{1}{|\widehat{\Gamma}|} \sum_{\kappa \in \widehat{\Gamma}} \kappa'(\alpha - \beta) \kappa(\alpha - \beta), \\ &= \kappa'(\alpha - \beta) \left(\frac{1}{|\widehat{\Gamma}|} \sum_{\kappa \in \widehat{\Gamma}} \overline{\kappa(\beta)} \kappa(\alpha) \right). \end{aligned}$$

Therefore, the right hand side of (3.2.1) is zero whenever $\alpha \neq \beta$. The claim follows since $\overline{\kappa(\beta)} \kappa(\beta) = 1$ for every $\kappa \in \widehat{\Gamma}$. \square

The above theorem tells us that every function in $L^2(\Gamma)$ can be written as a linear combination of characters of Γ . This re-parametrization of functions has a very special name:

Definition 3.2.2. Let $f \in L^2(\Gamma)$ be any complex-valued function. The **Fourier transform** of f is the function $\hat{f} \in L^2(\hat{\Gamma})$ defined by the equality

$$f(\alpha) = \sum_{\kappa \in \hat{\Gamma}} \hat{f}(\kappa) \kappa(\alpha). \quad (3.2.2)$$

The value $\hat{f}(\kappa)$ is called the **Fourier coefficient** of f in κ .

Example 3.2.3. Let us consider the function $f \in L^2(\mathbb{Z}_3)$ given by $f(\alpha) = 2^\alpha$ for every $\alpha \in \mathbb{Z}_3$. By the orthonormality of the characters, we know that $\langle f, \kappa \rangle = \hat{f}(\kappa)$. In Example 3.1.2 we showed that the characters of \mathbb{Z}_3 are $\kappa_\beta(\alpha) := e^{\beta\alpha\frac{2\pi i}{3}}$ for every $\alpha, \beta \in \mathbb{Z}_3$. Hence,

$$\begin{aligned} \hat{f}(\kappa_0) &= \frac{1}{3} \sum_{\alpha \in \mathbb{Z}_3} 2^\alpha e^{-0 \cdot \alpha \frac{2\pi i}{3}} = \frac{7}{3}, \\ \hat{f}(\kappa_1) &= \frac{1}{3} \sum_{\alpha \in \mathbb{Z}_3} 2^\alpha e^{-\alpha \frac{2\pi i}{3}} = \frac{1}{3} \sum_{\alpha \in \mathbb{Z}_3} 2^\alpha \frac{(-1 + \sqrt{3}i)^{2\alpha}}{2^{2\alpha}} = -\frac{2 + \sqrt{3}i}{3}, \\ \hat{f}(\kappa_2) &= \frac{1}{3} \sum_{\alpha \in \mathbb{Z}_3} 2^\alpha e^{-2\alpha \frac{2\pi i}{3}} = \frac{1}{3} \sum_{\alpha \in \mathbb{Z}_3} 2^\alpha \frac{(-1 + \sqrt{3}i)^\alpha}{2^\alpha} = -\frac{2 - \sqrt{3}i}{3}. \end{aligned}$$

In the above example we used the orthonormality of the characters to obtain the following equality, which is called the *Fourier Transform formula*:

$$\hat{f}(\kappa) = \int_{\Gamma} f(\alpha) \overline{\kappa(\alpha)} d\mu(\alpha) = \frac{1}{|\Gamma|} \sum_{\alpha \in \Gamma} f(\alpha) \overline{\kappa(\alpha)}. \quad (3.2.3)$$

Similarly, the equation (3.2.2) is called the *Fourier Inversion formula* as we can recover f from \hat{f} using such formula. The Fourier Transform defines a linear isomorphism from $L^2(\Gamma)$ to $L^2(\hat{\Gamma})$ given by $f \mapsto \hat{f}$. This isomorphism let us transform problems involving structures of $L^2(\Gamma)$ into problems involving structures in $L^2(\hat{\Gamma})$ (see Chapter 5). Next, we define the *convolution* of functions:

Definition 3.2.4. For any two functions $f, g \in L^2(\Gamma)$ their **convolution** is the function $f * g \in L^2(\Gamma)$ defined by

$$f * g(\alpha) := \int_{\Gamma} f(\beta)g(\alpha - \beta) d\mu(\alpha).$$

As the following lemma shows, the Fourier Transform behaves well under convolution:

Lemma 3.2.5 (Convolution Theorem). *Let $f, g \in L^2(\Gamma)$, then*

$$\widehat{f * g}(\kappa) = \widehat{f}(\kappa)\widehat{g}(\kappa), \quad \forall \kappa \in \widehat{\Gamma}.$$

Proof. The proof follows by the equalities

$$\begin{aligned} f * g(\alpha) &= \int_{\Gamma} f(\beta)g(\alpha - \beta) d\mu(\alpha), \\ &= \sum_{\kappa \in \widehat{\Gamma}} \widehat{g}(\kappa) \int_{\Gamma} f(\beta)\kappa(\alpha - \beta) d\mu(\alpha), \\ &= \sum_{\kappa \in \widehat{\Gamma}} \widehat{g}(\kappa)\kappa(\alpha) \int_{\Gamma} f(\beta)\overline{\kappa(\beta)} d\mu(\alpha), \\ &= \sum_{\kappa \in \widehat{\Gamma}} \widehat{g}(\kappa)\widehat{f}(\kappa)\kappa(\alpha). \end{aligned}$$

□

Another beautiful consequence of Theorem 3.2.1 is the connection between Abelian Groups, Roots of the Unity and Polynomials:

Theorem 3.2.6. *Let $\Gamma \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \dots \times \mathbb{Z}_{k_n}$ be an abelian group. Then,*

1. *The dual group $\widehat{\Gamma}$ is equal to the set of all functions $\kappa_{\alpha} \in L^2(\Gamma)$ with $\alpha \in \Gamma$, defined by*

$$\kappa_{\alpha}(\beta) := e^{\beta_1 \alpha_1 \frac{2\pi i}{k_1}} e^{\beta_2 \alpha_2 \frac{2\pi i}{k_2}} \dots e^{\beta_n \alpha_n \frac{2\pi i}{k_n}}, \quad \forall \beta \in \Gamma. \quad (3.2.4)$$

2. *The double dual group $\widehat{\widehat{\Gamma}}$, that is, the dual group of the dual group of Γ is equal to the set of all monomials $x^{\beta} = x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n} \in L^2(\widehat{\Gamma})$ with $\beta \in \Gamma$, defined by*

$$x^{\beta}(\kappa_{\alpha}) := (e^{\alpha_1 \frac{2\pi i}{k_1}})^{\beta_1} (e^{\alpha_2 \frac{2\pi i}{k_2}})^{\beta_2} \dots (e^{\alpha_n \frac{2\pi i}{k_n}})^{\beta_n}, \quad \forall \kappa_{\alpha} \in \widehat{\Gamma}. \quad (3.2.5)$$

Proof. 1. It is clear that the functions κ_α are characters of Γ . We claim that $\kappa_\alpha \neq \kappa_{\alpha'}$ whenever $\alpha \neq \alpha'$. Indeed, suppose that $\alpha_j \neq \alpha'_j$ for some $j \in [n]$. Then, as there are exactly k_j different k_j -roots of the unity, $e^{\alpha_j \frac{2\pi i}{k_j}} \neq e^{\alpha'_j \frac{2\pi i}{k_j}}$. If we let $\beta = e_j$ be the multi-index which equals one in the j -th coordinate and zero elsewhere, then

$$\kappa_\alpha(\beta) \neq \kappa_{\alpha'}(\beta).$$

The proof follows by Theorem 3.2.1 as the number of elements of $\widehat{\Gamma}$ and Γ are the same.

2. The proof is similar to part 1. of this theorem as the product of two monomials x^α and x^β as elements of $L^2(\widehat{\Gamma})$ equals the monomial $x^{\alpha+\beta}$ for every $\alpha, \beta \in \Gamma$.

□

We finish this section with a nice application of the Nullstellensatz to functions over groups:

Theorem 3.2.7 (Group Nullstellensatz). *Let Γ be a finite abelian group and let f_1, f_2, \dots, f_m be functions in $L^2(\Gamma)$. Then, exactly one of the following holds:*

1. *There exists some $\alpha \in \Gamma$ such that*

$$f_1(\alpha) = f_2(\alpha) = \dots = f_m(\alpha) = 0.$$

2. *There exist some $r_1, r_2, \dots, r_m \in L^2(\Gamma)$ such that*

$$r_1 f_1 + r_2 f_2 + \dots + r_m f_m = 1.$$

Proof. Without loss of generality, we may assume that

$$\Gamma = \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \dots \times \mathbb{Z}_{k_n},$$

for some integers k_1, k_2, \dots, k_n . Now, for each $j \in [m]$ let us define the polynomials $p_j \in \mathbb{C}[x_1, x_2, \dots, x_n]$ given by

$$p_j(x) := \sum_{\alpha \in \Gamma} \widehat{f}_j(\kappa_\alpha) x^\alpha.$$

We claim that there is a solution to $f_1(\alpha) = f_2(\alpha) = \dots = f_m(\alpha) = 0$ if and only if the system of polynomial equations

$$\begin{aligned} p_1(x) = p_2(x) = \dots = p_m(x) &= 0, \\ x_i^{k_i} - 1 &= 0, \quad i \in [n], \end{aligned} \tag{3.2.6}$$

has a solution. Indeed, for every $\beta \in \Gamma$ and $j \in [m]$ we have that

$$\begin{aligned} f_j(\beta) &= \sum_{\alpha \in \Gamma} \widehat{f}_j(\kappa_\alpha) \kappa_\alpha(\beta), \\ &= \sum_{\alpha \in \Gamma} \widehat{f}_j(\kappa_\alpha) (e^{\beta_1 \frac{2\pi i}{k_1}})^{\alpha_1} (e^{\beta_2 \frac{2\pi i}{k_2}})^{\alpha_2} \dots (e^{\beta_n \frac{2\pi i}{k_n}})^{\alpha_n}, \\ &= p_j(e^{\beta_1 \frac{2\pi i}{k_1}}, e^{\beta_2 \frac{2\pi i}{k_2}}, \dots, e^{\beta_n \frac{2\pi i}{k_n}}). \end{aligned} \tag{3.2.7}$$

The claim follows as every solution $\bar{x} \in \mathbb{C}^n$ to (3.2.6) the scalars $\bar{x}_i \in \mathbb{C}$ are k_i -roots of the unity for every $i \in [n]$. Now, if system (3.2.6) has no solution, then by Hilbert's Nullstellensatz, there exists polynomials s_1, \dots, s_m and t_1, \dots, t_n in $\mathbb{C}[x_1, \dots, x_n]$ such that

$$\sum_{j \in [m]} s_j(x) p_j(x) + \sum_{i \in [n]} t_i(x) (x_i^{k_i} - 1) = 1.$$

The proof follows since the functions $r_1, r_2, \dots, r_m \in L^2(\Gamma)$ defined by the equation

$$r_j(\beta) := s_j(e^{\beta_1 \frac{2\pi i}{k_1}}, e^{\beta_2 \frac{2\pi i}{k_2}}, \dots, e^{\beta_n \frac{2\pi i}{k_n}}), \quad \forall \beta \in \Gamma,$$

satisfy the required property. □

3.3 Cayley Graphs

Another aspect of Fourier Analysis is that it lets us calculate the spectra of some well known graphs called *Cayley Graphs*. Recall that a set $\mathcal{S} \subseteq \Gamma$ is *symmetric* if $\alpha \in \mathcal{S}$ implies that $-\alpha \in \mathcal{S}$.

Definition 3.3.1. *Let \mathcal{S} be a symmetric subset of Γ . The Cayley Graph $\text{Cay}(\Gamma, \mathcal{S})$ is the graph with vertex set Γ and edge set formed by all pairs $\{\alpha, \beta\} \subseteq \Gamma$ satisfying $\alpha - \beta \in \mathcal{S}$.*

Remark 3.3.2. *The classical definition of Cayley Graphs does not allow symmetric sets to contain the identity of the group ([28]). We have chosen to remove this extra constraint in order to simplify some of the discussion in Chapter 5.*

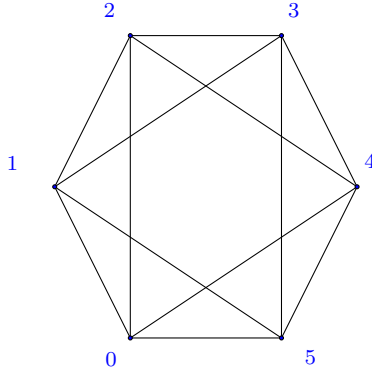


Figure 3.1: The graph $\text{Cay}(\mathbb{Z}_6, \mathcal{S})$

Example 3.3.3. Let $\Gamma = \mathbb{Z}_6$ and let $\mathcal{S} = \{-2, -1, 0, 1, 2\}$. Then, the Cayley Graph $\text{Cay}(\mathbb{Z}_6, \mathcal{S})$ is the graph shown in Figure 3.1 (we have omitted loops).

The adjacency matrix of the Cayley Graph $\text{Cay}(\Gamma, \mathcal{S})$ is the matrix $A_{\Gamma, \mathcal{S}}$ with entries

$$A_{\Gamma, \mathcal{S}}(\alpha, \beta) = \begin{cases} 1 & \text{if } \beta - \alpha \in \mathcal{S}, \\ 0 & \text{otherwise.} \end{cases} \quad (3.3.1)$$

As the following lemma shows, we can calculate the eigenvalues of the adjacency matrix of Cayley Graphs very easily:

Lemma 3.3.4. Consider the function

$$\delta_{\mathcal{S}}(\alpha) := \begin{cases} 1 & \text{if } \alpha \in \mathcal{S}, \\ 0 & \text{otherwise.} \end{cases} \quad (3.3.2)$$

Then, for every function $f \in L^2(\Gamma)$ we have

$$A_{\Gamma, \mathcal{S}}f = |\Gamma|\delta_{\mathcal{S}} * f. \quad (3.3.3)$$

Proof. Let $f \in L^2(\Gamma)$ be any given function and let $g := A_{\Gamma, \mathcal{S}}f$. Then,

$$\begin{aligned} g(\alpha) &= \sum_{\beta \in \Gamma} A_{\Gamma, \mathcal{S}}(\alpha, \beta)f(\beta) = \sum_{\beta \in \Gamma} \delta_{\mathcal{S}}(\alpha - \beta)f(\beta), \\ &= |\Gamma|\delta_{\mathcal{S}} * f(\alpha). \end{aligned}$$

□

Theorem 3.3.5. *The characters of Γ form a basis for the eigenspace of $A_{\Gamma, \mathcal{S}}$. Moreover, for every $\kappa \in \widehat{\Gamma}$ we have that*

$$A_{\Gamma, \mathcal{S}} \kappa = |\Gamma| \widehat{\delta}_{\mathcal{S}}(\kappa) \kappa.$$

Proof. By the above lemma, for any character $\kappa \in \widehat{\Gamma}$ and any $\alpha \in \Gamma$ we have that

$$\begin{aligned} A_{\Gamma, \mathcal{S}} \kappa(\alpha) &= |\Gamma| \delta_{\mathcal{S}} * \kappa(\alpha), \\ &= \sum_{\beta \in \Gamma} \delta_{\mathcal{S}}(\beta) \kappa(\alpha - \beta), \\ &= \kappa(\alpha) \sum_{\beta \in \Gamma} \delta_{\mathcal{S}}(\beta) \overline{\kappa(\beta)} = |\Gamma| \widehat{\delta}_{\mathcal{S}}(\kappa) \kappa(\alpha). \end{aligned} \tag{3.3.4}$$

The proof follows by the fact that the dual group $\widehat{\Gamma}$ form a basis for $L^2(\Gamma)$. \square

Example 3.3.6. *Let $\Gamma = \mathbb{Z}_6$ and let $\mathcal{S} = \{-2, -1, 0, 1, 2\}$ be as in Example 3.3.3. Then, the adjacency matrix of the graph $\text{Cay}(\mathbb{Z}_6, \mathcal{S})$ is*

$$A_{\mathbb{Z}_6, \mathcal{S}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

In order to calculate the eigenvalues of $A_{\mathbb{Z}_6, \mathcal{S}}$ we need first to calculate the Fourier Transform of $\delta_{\mathcal{S}}$. By Theorem 3.2.6 we know that the characters of \mathbb{Z}_6 are $\kappa_{\alpha}(\beta) = e^{\alpha\beta\frac{2\pi i}{6}}$ with $\alpha \in \mathbb{Z}_6$. Hence,

$$\begin{aligned} \langle \delta_{\mathcal{S}}, \kappa_0 \rangle &= \frac{5}{6}, \\ \langle \delta_{\mathcal{S}}, \kappa_1 \rangle &= e^{2\frac{2\pi i}{6}} + e^{\frac{2\pi i}{6}} + 1 + e^{-\frac{2\pi i}{6}} + e^{-2\frac{2\pi i}{6}} = \frac{1}{6}, \\ \langle \delta_{\mathcal{S}}, \kappa_2 \rangle &= e^{4\frac{2\pi i}{6}} + e^{2\frac{2\pi i}{6}} + 1 + e^{-2\frac{2\pi i}{6}} + e^{-4\frac{2\pi i}{6}} = -\frac{1}{6}, \\ \langle \delta_{\mathcal{S}}, \kappa_3 \rangle &= e^{6\frac{2\pi i}{6}} + e^{3\frac{2\pi i}{6}} + 1 + e^{-3\frac{2\pi i}{6}} + e^{-6\frac{2\pi i}{6}} = \frac{1}{6}, \\ \langle \delta_{\mathcal{S}}, \kappa_4 \rangle &= \overline{\langle \delta_{\mathcal{S}}, \kappa_2 \rangle} = -\frac{1}{6}, \\ \langle \delta_{\mathcal{S}}, \kappa_5 \rangle &= \overline{\langle \delta_{\mathcal{S}}, \kappa_1 \rangle} = \frac{1}{6}. \end{aligned} \tag{3.3.5}$$

In particular

$$\delta_{\mathcal{S}} = \frac{5}{6}\kappa_0 + \frac{1}{6}\kappa_1 - \frac{1}{6}\kappa_2 + \frac{1}{6}\kappa_3 - \frac{1}{6}\kappa_4 + \frac{1}{6}\kappa_5,$$

and the eigenvalues of $A_{\mathbb{Z}_6, \mathcal{S}}$ are $-1, 1$ and 5 .

Remark 3.3.7. *The matrix $A_{\mathbb{Z}_6, \mathcal{S}}$ of the above example is a **circulant matrix**, i.e. for every $i \geq 2$, the i -th row of the matrix is obtained after $i - 1$ shifts to the right of the first row. Moreover, it is not hard to show that the adjacency matrix of the Cayley graph $\text{Cay}(\Gamma, \mathcal{S})$ is circulant when Γ is a cyclic group.*

Chapter 4

Applied Hilbert's Nullstellensatz for Combinatorial Problems

In this chapter we will apply the algebraic geometry tools we developed in Chapter 2 and Chapter 3 to create algorithms for determining the existence of combinatorial objects. Examples of such problems in graphs are determining the existence of cycles of a given length, determining if a graph is k -colorable or determining the existence of stable sets of a given size. The main idea will be to associate a given combinatorial problem P with an ideal of polynomials \mathcal{I}_P over some field \mathbb{K} . This will be done in a way that the problem P will have a solution if and only if the variety $\mathcal{V}_{\mathbb{K}}(\mathcal{I}_P)$ is non-empty. Therefore, the Nullstellensatz will detect if the problem P has no feasible solution. In fact, as we mention at the end of Chapter 2, there exists an algorithm that uses the Nullstellensatz to detect if a given variety is empty or not. Such algorithm is called *Nullstellensatz Linear Algebra* (NulLA) algorithm and it will be the central topic of this chapter.

The use of the Nullstellensatz for proving the existence of combinatorial objects is sometimes referred as the *Polynomial Method* and it was popularized by Noga Alon's seminal paper [1]. Nevertheless, Jesus De Loera, Jon Lee, Peter Mankin and Susan Margulies ([20]) were the first to give a concrete computational study of the method.

4.1 Nullstellensatz Linear Algebra (NulLA) Algorithm

Let p_1, p_2, \dots, p_m be given polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$ of degree at most d with \mathbb{K} algebraically closed. As we saw in Chapter 2, if the system $p_1(x) = \dots = p_m(x) = 0$

has no solution, then by Kollar's Theorem (see Theorem 2.3.7), there exist polynomials $r_1, \dots, r_m \in \mathbb{K}[x_1, x_2, \dots, x_n]$ of degree at most $d_B = \max(3, d)^n$ such that

$$r_1(x)p_1(x) + r_2(x)p_2(x) + \dots + r_m(x)p_m(x) = 1. \quad (4.1.1)$$

Clearly, if we set

$$r_i(x) = \sum_{|\alpha| \leq d_B} a_{i,\alpha} x^\alpha, \quad i \in [m],$$

then equation (4.1.1) will be equivalent to a system of linear equations on the variables $a_{i,\alpha} \in \mathbb{K}$ (a concrete instance of this system can be found in Example 4.1.6 below). However, the size of this system is considerably large. The number of rows is equal to the number of monomials of degree at most $d_B + d$ in n variables, which equals $\binom{n+d_B+d}{n}$. Hence, the size of the system is doubly exponential in d, n and m . Although Kollar's bounds are sharp ([34]), for some specific families of systems of polynomial equations we can obtain much better bounds:

Proposition 4.1.1. *Consider the system*

$$\begin{aligned} p_1(x) = p_2(x) = \dots = p_m(x) &= 0, \\ x_j^{k_j} - 1 &= 0, \quad \forall j \in J \subseteq [n], \\ x_j(x_j - 1) &= 0, \quad \forall j \in [n] \setminus J \end{aligned} \quad (4.1.2)$$

for some polynomials $p_k \in \mathbb{C}[x_1, \dots, x_n]$ of degree at most d and integers $k_j \geq 1$ with $j \in J$. Let $d^* := \max\{2, d, k_j : j \in J\}$ be the maximum degree of the polynomials in the system. If (4.1.2) has no solution, then it has a Nullstellensatz certificate of degree

$$\tilde{d}_L = 2n(d^* - 1). \quad (4.1.3)$$

Proof. Without loss of generality we may assume that $J = [n]$, otherwise we can make the change of variables $x_j =: \frac{1}{2}(y_j + 1)$ for every $j \in [n] \setminus J$ and end up with a new system of polynomials containing the equation $y_j^2 - 1 = 0$. Since this change of variables is linear and invertible, the new system has a solution if and only if the original system has a solution. Moreover, in the case that they do not have a solution, both will have Nullstellensatz certificates of same degree.

Now, let $k_1, k_2, \dots, k_n \geq 1$ as in the statement and define the finite abelian group $\Gamma := \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \dots \times \mathbb{Z}_{k_n}$. Then, for every $i \in [m]$ we can write each polynomial p_i as

$$p_i(x) = \tilde{p}_i(x) + \sum_{j \in [n]} s_{ij}(x)(x_j^{k_j} - 1),$$

where $\tilde{p}_i(x)$ is a polynomial supported on the monomials x^α with $\alpha \in \Gamma$ and the polynomials $s_{ij}(x)$ have degree at most d . In particular, system (4.1.2) is equivalent to the system

$$\begin{aligned} \tilde{p}_1(x) = \tilde{p}_2(x) = \cdots = \tilde{p}_m(x) = 0, \\ x_j^{k_j} - 1 = 0, \quad \forall j \in [n]. \end{aligned} \tag{4.1.4}$$

Clearly, by Theorem 3.2.6 we can see each polynomial \tilde{p}_i as a function in $L^2(\widehat{\Gamma})$ so that the system (4.1.4) is equivalent to the system

$$\tilde{p}_1(x) = \tilde{p}_2(x) = \cdots = \tilde{p}_m(x) = 0, \quad x \in \widehat{\Gamma}. \tag{4.1.5}$$

By the Group Nullstellensatz (Theorem 3.2.7), if (4.1.5) has no solution, then there exist functions $\tilde{r}_1, \tilde{r}_2, \dots, \tilde{r}_m \in L^2(\widehat{\Gamma})$ such that

$$\sum_{i=1}^m \tilde{r}_i(x) \tilde{p}_i(x) = 1, \quad \forall x \in \widehat{\Gamma}.$$

Again, by Theorem 3.2.6, each \tilde{r}_i can be written as a sum of the monomials x^α with $\alpha \in \Gamma$, whence they are polynomials of degree at most $\sum k_j - n$. Let us define the polynomial

$$q(x) := \sum_{i=1}^m \tilde{r}_i(x) \tilde{p}_i(x).$$

Then, q has degree at most $2(\sum_{j \in [n]} (k_j - 1))$ and it satisfies $q(\bar{x}) = 1$ for every $\bar{x} \in \mathbb{C}^n$ such that $\bar{x}_j^{k_j} = 1$ for each $j \in [n]$. Again, as we did with the polynomials p_i , we can write q as

$$q(x) = \tilde{q}(x) + \sum_{j \in [n]} t_j(x) (x_j^{k_j} - 1),$$

where \tilde{q} is a polynomial supported on the monomials x^α with $\alpha \in \Gamma$ and the polynomials $t_j(x)$ have degree at most $2(\sum_{j \in [n]} (k_j - 1))$. We claim that $\tilde{q} \equiv 1$ and as a consequence

$$\sum_{i=1}^m \tilde{r}_i(x) p_i(x) - \sum_{j=1}^n \left(\sum_{i=1}^m \tilde{r}_i(x) s_{ij}(x) + t_j(x) \right) (x_i^{k_i} - 1) = 1,$$

gives us a Nullstellensatz certificate of degree

$$\max \left\{ \sum_j (k_j - 1) + d, 2 \sum_j (k_j - 1) \right\} \leq 2n(d^* - 1).$$

We give the proof of our claim in the following lemma

Lemma 4.1.2. *Suppose that $p \in \mathbb{C}[x_1, x_2, \dots, x_n]$ is a polynomial supported on the monomials x^α with $\alpha \in \Gamma$. If $p(\bar{x}) = 0$ for every solution $\bar{x} \in \mathbb{C}^n$ to $\bar{x}_j^{k_j} = 1$ with $j \in [n]$, then p is the zero polynomial.*

Proof. We will prove the statement by induction on the number of variables. If $\Gamma = \mathbb{Z}_k$ for some integer k , then the claim follows by the fundamental theorem of algebra, as p will be a polynomial of degree $k - 1$ having k roots. Now, suppose that the statement holds for polynomials of at most $n - 1$ variables. Let $p \in \mathbb{C}[x_1, x_2, \dots, x_n]$ as in the statement. Notice that we can write the polynomial p as

$$p(x) = \sum_{r=0}^{k_n-1} x_n^r q_r(x_1, \dots, x_{n-1}),$$

for some polynomials q_r in $\mathbb{C}[x_1, \dots, x_{n-1}]$ with $r \in \mathbb{Z}_{k_n}$. We claim that $q_r(\bar{x}) = 0$ for every solution $\bar{x} \in \mathbb{C}^{n-1}$ to $\bar{x}_j^{k_j} = 1$ with $j \in [n - 1]$. Indeed, for any such \bar{x} , the univariate polynomial

$$\bar{p}(x_n) = \sum_{r=0}^{k_n-1} x_n^r q_r(\bar{x})$$

vanishes on every k_n -root of the unity. In particular, $\bar{p} \equiv 0$ and each $q_r(\bar{x}) = 0$. By our induction hypothesis, each q_r is zero and p is as well. \square

The proof that $\tilde{q} \equiv 1$ follows by using the above lemma with $p = \tilde{q} - 1$. \square

Remark 4.1.3. *We can use the use Proposition 4.1.4 to get bounds for more general problems. Indeed, suppose that*

$$\mathcal{V}_{\mathbb{C}}(p_1, p_2, \dots, p_m) \subseteq A_1 \times A_2 \times \dots \times A_n$$

where each $A_i \subset \mathbb{C}$ is finite and the polynomials p_i have degree at most d . Now, let $f_i : \widehat{\mathbb{Z}}_{|A_i|} \rightarrow A_i$ be any bijection from the dual group $\widehat{\mathbb{Z}}_{|A_i|}$ to A_i for $i \in [n]$. We can write each f_i as a univariate polynomial supported on the monomials y_i^α with $\alpha \in \mathbb{Z}_{|A_i|}$. Moreover, the variety $\mathcal{V}_{\mathbb{C}}(p_1, p_2, \dots, p_m)$ will be non-empty if and only if the system given by

$$\begin{aligned} p_1(f_1(y_1), \dots, f_n(y_n)) &= \dots = p_m(f_1(y_1), \dots, f_n(y_n)) = 0, \\ y_j^{|A_j|} - 1 &= 0, \quad \forall j \in [n], \end{aligned} \tag{4.1.6}$$

has a solution. By Proposition 4.1.4, if (4.1.6) has no solution, then we can guarantee the existence of certificates (in the variables y_i) of degree at most

$$2n(d \max\{|A_i| : i \in [n]\} - 1).$$

Notice that using simple algebraic arguments, we were able to reduce considerably the sharp bounds of Kollar. As the following proposition shows, we can also use Lazard’s Theorem (Theorem 2.3.11) to improve the bound \tilde{d}_L by a constant factor.

Proposition 4.1.4. *The statement of Proposition 4.1.1 still holds if we replace the bound \tilde{d}_L by*

$$d_L = n(d^* - 1). \tag{4.1.7}$$

Proof. By Lazard’s Theorem (Theorem 2.3.11) we only need to check that the polynomials in (4.1.2) have no common root at infinity. In order to see this, notice that the homogenization of the polynomials $x_j^{k_j} - 1$ and $x_j(x_j - 1)$ is $x_j^{k_j} - x_0^{k_j}$ for all $j \in I$ and $x_j^2 - x_j x_0$ for all $j \in [n] \setminus I$. Hence, after setting $x_0 = 0$ we see that $x_j = 0$ will be the only root of the corresponding polynomial for all $j \in [n]$. Therefore, the polynomials in (4.1.2) do not share a root at infinity. \square

We must stress the fact that Lazard’s Theorem relies on advance techniques of cohomological algebra and algebraic geometry. However, we were able to prove a very similar bound to that of Lazard using much simpler ideas. This shows that systems like (4.1.2) are not pathological and we might expect even better bounds for some systems of this type. Jesus de Loera, Jon Lee, Peter Malkin and Susan Margulies [20] made these observations and proposed Algorithm 4.1.1 (NullA) below to detect the feasibility of systems of polynomial equations.

Algorithm 4.1.1: Nullstellensatz Linear Algebra Algorithm (NullA)

Data: Polynomials $p_1, p_2, \dots, p_m \in \mathbb{K}[x_1, \dots, x_n]$

Result: A certificate of infeasibility $r_1, \dots, r_m \in \mathbb{K}[x_1, \dots, x_n]$ or a certificate y of feasibility for the system.

```
1  $d \leftarrow 0$ ;  
2 while  $d \leq d_B$  do  
3   Set  $r_i(x) = \sum_{|\alpha| \leq d} a_{i,\alpha} x^\alpha$ , for each  $i \in [m]$ ;  
4   Compute the system of linear equations  $Ma = e$  on the variables  $a_{i,\alpha}$  obtained  
   from:  $r_1(x)p_1(x) + r_2(x)p_2(x) + \dots + r_m(x)p_m(x) = 1$ ;  
5   if  $Ma = e$  has no solution then  
6     if  $d = d_B$  then  
7       Find a solution  $y$  to the system  $y^\top M = 0, y^\top e = 1$ .  
8       print:  $p_1, p_2, \dots, p_m$  have a common root, bound  $d_B$  reached;  
9       return:  $y$ .  
10      else  
11         $d \leftarrow d + 1$ .  
12      else  
13        print:  $p_1, p_2, \dots, p_m$  have no common root;  
14        return:  $r_1, r_2, \dots, r_m$ .
```

Remark 4.1.5. Notice that NullA also returns certificates of feasibility. If $d = d_B$ and $Ma = e$ has no solution, then the solution $y^\top M = 0, y^\top e = 1$ provides such certificate (see Section 4.2 for more details on this).

Example 4.1.6. Consider the system of polynomial equations

$$\begin{aligned}
x_1 + x_2 + x_3 &= 3, \\
x_1 + x_2 &= 2, \\
x_1 + x_3 &= 1, \\
x_i(x_i - 1) &= 0, \quad i \in \{1, 2, 3\}.
\end{aligned} \tag{4.1.8}$$

Clearly, the system (4.1.8) has no solution. On the one hand, Kollar's Theorem implies that this system has a Nullstellensatz certificate of degree $d_B = \max(3, 2)^{\min(3, 6)} = 27$. On the other hand, polynomials in (4.1.8) have no common root at infinity. Hence, by Lazard's Theorem, there exists a Nullstellensatz certificate of degree $d_L = n(d - 1) = 3$. Let us use NulLA to find a minimum degree Nullstellensatz certificate.

First, we must check if the system has a zero degree Nullstellensatz certificate. Therefore, we must solve the system of linear equations given by:

$$\begin{aligned}
&a_1(x_1 + x_2 + x_3 - 3) + a_2(x_1 + x_2 - 2) + a_3(x_1 + x_3 - 1) + \dots \\
&\quad \dots + a_4(x_1(x_1 - 1)) + a_5(x_2(x_2 - 1)) + a_6(x_3(x_3 - 1)) = 1, \\
&\quad a_4x_1^2 + a_5x_2^2 + a_6x_3^2 + (a_1 + a_2 + a_3 - a_4)x_1 + \dots \\
&\quad \dots + (a_1 + a_2 - a_5)x_2 + (a_1 + a_3 - a_6)x_3 + (-3a_1 - 2a_2 - a_3) = 1.
\end{aligned} \tag{4.1.9}$$

Notice that the monomials of degree two have single variables multiplying them, thus the variables a_4, a_5 and a_6 must be equal to zero. After deleting these variables, we obtain the following system (in tableau form):

	a_1	a_2	a_3		
1	-3	-2	-1		1
x_1	1	1	1		0
x_2	1	1	0		0
x_3	1	0	1		0

(4.1.10)

Clearly, this system is infeasible as the unique solution of the subsystem corresponding to the rows x_1, x_2, x_3 is zero. Since we do not have a certificate of degree zero, we need to look for certificates of degree at most one:

$$\begin{aligned}
&(a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + a_{14})(x_1 + x_2 + x_3 - 3) + \dots \\
&\quad \dots + (a_{61}x_1 + a_{62}x_2 + a_{63}x_3 + a_{64})(x_3(x_3 - 1)) = 1.
\end{aligned} \tag{4.1.11}$$

As in the previous case, the terms of degree three of the above equation appear multiplied by single variables:

$$a_{41}x_1^3 + a_{42}x_1^2x_2 + a_{43}x_1^2x_3 + a_{52}x_2^3 + a_{51}x_2^2x_1 + a_{53}x_2^2x_3 + a_{63}x_3^3 + a_{62}x_3^2x_2 + a_{61}x_3^2x_1.$$

Therefore, we can eliminate the variables $a_{41}, a_{42}, a_{43}, a_{51}, a_{52}, a_{53}, a_{61}, a_{62}$ and a_{63} , and obtain the following system (zeros omitted):

	a_{11}	a_{12}	a_{13}	a_{14}	a_{21}	a_{22}	a_{23}	a_{24}	a_{31}	a_{32}	a_{33}	a_{34}	a_{44}	a_{55}	a_{66}	
1				-3				-2				-1				1
x_1	-3			1	-2			1	-1			1	-1			
x_2		-3		1		-2		1		-1				-1		
x_3			-3	1			-2				-1	1			-1	
x_1^2	1				1				1				1			
x_2^2		1				1								1		
x_3^2			1								1				1	
x_1x_2	1	1			1	1				1						
x_1x_3	1		1				1		1		1					
x_2x_3		1	1				1			1						
	$-\frac{1}{12}$	$-\frac{7}{12}$		$-\frac{1}{3}$	$-\frac{1}{6}$	$\frac{1}{12}$	$-\frac{1}{6}$		$\frac{1}{4}$	$\frac{3}{4}$				$\frac{1}{2}$		

(4.1.12)

Using a linear system solver, we can see that (4.1.12) has a solution. Hence, the polynomial system (4.1.8) has a Nullstellensatz Certificate of degree one given by

$$\begin{aligned} & \left(-\frac{1}{12}x_1 - \frac{7}{12}x_2 - \frac{1}{3}\right)(x_1 + x_2 + x_3 - 3) + \left(-\frac{1}{6}x_1 + \frac{1}{12}x_2 - \frac{1}{6}x_3\right)(x_1 + x_2 - 2) + \dots \\ & \dots + \left(\frac{1}{4}x_1 + \frac{3}{4}x_2\right)(x_1 + x_3 - 1) + \left(\frac{1}{2}\right)(x_2^2 - x_2) = 1. \end{aligned}$$

(4.1.13)

4.2 Nullstellensatz Dual Certificates and the Maximum Stable Set Problem

As we mentioned in the introduction, for some combinatorial problems, NullLA can be inefficient as it might return certificates of degree equal or very close to Lazard's bounds. The purpose of this section is to provide an example of such bad instances, namely the Maximum Stable Set problem.

Definition 4.2.1. Let $G = (V, E)$ be a graph and let $S \subseteq V$ be any subset of vertices of the graph. We say that S is **stable** if for every pair of vertices $i, j \in S$ we have that $\{i, j\} \notin E$. The size of a stable set S is the cardinality of S .

Example 4.2.2. Consider the graph G as shown in Figure 4.1 called the Generalized Petersen Graph $GP(7, 2)$. The diamond shaped vertices of G form a stable set of size 5.

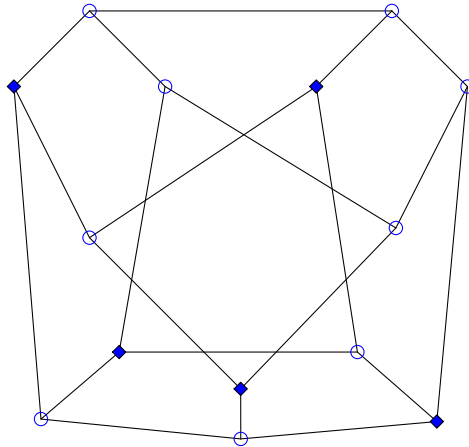


Figure 4.1: The Generalized Petersen Graph $GP(7, 2)$.

It is not hard to prove that this stable set is maximal, i.e. G has no stable set of size 6.

The *maximum stable set problem* is the problem of finding the stable set of maximum size in the graph. This value is called the stability number of G and it is denoted by $\alpha(G)$. For a given graph $G = (V, E)$ and any integer $1 \leq k \leq |V|$ the problem of determining whether G has a stable set of size k or not belongs to the complexity class *NP – hard*. László Lovász ([42]) proposed the following formulation for this problem as a system of polynomial equations:

Lemma 4.2.3. Let $G = (V, E)$ be a graph. Then, G has a stable set of size k if and only if the polynomial system

$$\begin{aligned}
 p_{V,k}(x) &:= \sum_{i \in V} x_i - k = 0, \\
 p_{ij}(x) &:= x_i x_j = 0 \quad \forall \{i, j\} \in E, \\
 q_i(x) &:= x_i(x_i - 1) = 0 \quad \forall i \in V,
 \end{aligned}
 \tag{STAB}$$

has a solution. Moreover, the number of solutions is equal to the number of stable sets of size k in G .

Proof. For every set $S \subseteq V$ consider its *incidence vector* $x^S \in \{0, 1\}^V$ given by

$$x_i^S := \begin{cases} 1 & \text{if } i \in S, \\ 0 & \text{otherwise.} \end{cases}$$

Then, it is straightforward to see that x^S is a solution to (STAB) if and only if S is a stable set of size k . The claim follows as every solution x to (STAB) is in $\{0, 1\}^V$ and hence x is the incidence vector of its support set. \square

Example 4.2.4. Let $G = (V, E)$ be the 3-cycle, that is $V := \{1, 2, 3\}$ and $E := \{\{1, 2\}, \{2, 3\}, \{1, 3\}\}$. Consider the system

$$\begin{aligned} p_{V,2}(x) &= x_1 + x_2 + x_3 - 2 = 0, \\ p_{ij}(x) &= x_i x_j = 0 \quad \forall \{i, j\} \in E, \\ q_i(x) &= x_i(x_i - 1) = 0 \quad \forall i \in \{1, 2, 3\}. \end{aligned} \tag{4.2.1}$$

Since the stability number of G is one, the above system has no solution. Again, by Lazard's Theorem, we see that the system (4.2.2) has a Nullstellenstaz Certificate of degree $d_L = 3$. We claim that G has a Nullstellensatz Certificate of degree one. As before, let us define the degree one polynomials

$$\begin{aligned} r_{V,2}(x) &:= a_{x_1}^{V,2} x_1 + a_{x_2}^{V,2} x_2 + a_{x_3}^{V,2} x_3 + a_1^{V,2}, \\ r_{ij}(x) &:= a_{x_1}^{ij} x_1 + a_{x_2}^{ij} x_2 + a_{x_3}^{ij} x_3 + a_1^{ij}, \quad \forall \{i, j\} \in E, \\ s_i(x) &:= b_{x_1}^i x_1 + b_{x_2}^i x_2 + b_{x_3}^i x_3 + b_1^i, \quad \forall i \in V, \end{aligned} \tag{4.2.2}$$

and solve the system

$$r_{V,2}(x)p_{V,2}(x) + \sum_{\{i,j\} \in E} r_{ij}(x)p_{ij}(x) + \sum_{i \in V} s_i(x)q_i(x) = 1.$$

This linear system has size $\binom{6}{3} \times \binom{4}{3} 7 = 20 \times 28$ and it is too big to show it completely here.

However, if look at some of the columns of this system we can guess its structure:

	$a_{x_1}^{V,2}$	$a_{x_2}^{V,2}$	$a_{x_3}^{V,2}$	$a_1^{V,2}$	$a_{x_1}^{12}$	$a_{x_2}^{12}$	$a_{x_3}^{12}$	a_1^{12}	$b_{x_1}^1$	$b_{x_2}^1$	$b_{x_3}^1$	b_1^1	\dots	
1				-2									\dots	1
x_1	-2			1								-1	\dots	
x_2		-2		1									\dots	
x_3			-2	1									\dots	
x_1^2	1								-1			1	\dots	
x_2^2		1											\dots	
x_3^2			1										\dots	
x_1x_2	1	1					1			-1			\dots	
x_1x_3	1		1								-1		\dots	
x_2x_3		1	1										\dots	
x_1^3									1				\dots	
x_2^3													\dots	
x_3^3													\dots	
$x_1x_2^2$						1							\dots	
$x_1x_3^2$													\dots	
$x_2x_1^2$					1					1			\dots	
$x_2x_3^2$													\dots	
$x_3x_1^2$											1		\dots	
$x_3x_2^2$													\dots	
$x_1x_2x_3$							1						\dots	

We notice that the columns of this system are very sparse. For example, the columns indexed by the variable $a_{x_r}^{ij}$ has only one non-zero entry located in the row corresponding to the monomial $x_r x_i x_j$. This tells us that it should be easier to guarantee the existence of a solution using Fredholm's Theorem of the Alternative. Thus, let $\lambda = (\lambda_1, \lambda_{x_1}, \dots, \lambda_{x_2^2 x_3}, \lambda_{x_1 x_2 x_3})$ be orthogonal to the columns of (4.2.3). Then, λ is a solution to the system of linear equations

$$\lambda_1 - \frac{1}{2}(\lambda_{x_1} + \lambda_{x_2} + \lambda_{x_3}) = 0, \quad (4.2.4)$$

$$\lambda_{x_i} - \frac{1}{2}(\lambda_{x_i x_1} + \lambda_{x_i x_2} + \lambda_{x_i x_3}) = 0 \quad \forall i \in V, \quad (4.2.5)$$

$$\lambda_{x_i x_j} = \lambda_{x_r x_i x_j} = 0 \quad \forall r \in V, \forall \{i, j\} \in E, \quad (4.2.6)$$

$$\lambda_{x_i^2} - \lambda_{x_i} = 0 \quad \forall i \in V, \quad (4.2.7)$$

$$\lambda_{x_i^2 x_j} - \lambda_{x_i x_j} = 0 \quad \forall i, j \in V. \quad (4.2.8)$$

Thus, we see that $\lambda_{p(x)} = 0$ whenever $p(x)$ is a monomial that can be divided by some $x_i x_j$ with $\{i, j\} \in E$. That is, λ is supported only on the monomials defined by the stable sets of G . Hence, any solution to the above system is a solution to the system

$$\begin{aligned} \lambda_1 - \frac{1}{2}(\lambda_{x_1} + \lambda_{x_2} + \lambda_{x_3}) &= 0, \\ \lambda_{x_i} - \frac{1}{2}(\lambda_{x_i^2}) &= 0 \quad \forall i \in V, \\ \lambda_{x_i^2} - \lambda_{x_i} &= 0 \quad \forall i \in V. \end{aligned} \tag{4.2.9}$$

It is straightforward to check that this latter system implies $\lambda_1 = 0$. Hence, λ is orthogonal to the right hand side of the system (4.2.3) and as a result the system must have a solution. Moreover, we can use the transpose of system (4.2.9) to generate a Nullstellensatz Certificate:

	$a_1^{V,2}$	$a_{x_1}^{V,2}$	$a_{x_2}^{V,2}$	$a_{x_3}^{V,2}$	b_1^1	b_1^2	b_1^3	
1	-2	0	0	0	0	0	0	1
x_1	1	-2	0	0	-1	0	0	0
x_2	1	0	-2	0	0	-1	0	0
x_3	1	0	0	-2	0	0	-1	0
x_1^2	0	1	0	0	1	0	0	0
x_2^2	0	0	1	0	0	1	0	0
x_3^2	0	0	0	1	0	0	1	0
	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	

(4.2.10)

A solution is $a_1^{V,2} = a_{x_1}^{V,2} = a_{x_2}^{V,2} = a_{x_3}^{V,2} = -\frac{1}{2}$ and $b_1^1 = b_1^2 = b_1^3 = \frac{1}{2}$. Thus, we obtain the equation

$$\begin{aligned} -\frac{1}{2}(x_1 + x_2 + x_3 + 1)(x_1 + x_2 + x_3 - 2) + \frac{1}{2}(x_1^2 - x_1) + \dots \\ \dots + \frac{1}{2}(x_2^2 - x_2) + \frac{1}{2}(x_3^2 - x_3) = 1 - x_1 x_2 - x_1 x_3 - x_2 x_3. \end{aligned} \tag{4.2.11}$$

The use of Fredholm's Theorem of the Alternative to certify the existence of certificates is sometimes referred as the *Design Method* ([9],[10]). Clearly, this technique is useful when the polynomials defining the system are formed by a small number of monomials i.e. they are sparse. Stephen Cook et. al. ([6]) were the first to use this technique to find lower bounds of Nullstellensatz Certificates of systems describing a version of the Pigeon Principle. Jesus De Loera, Peter Malkin and Pablo Parrilo ([22]) formalized these notions in terms of the *annihilator* of a set of polynomials:

Definition 4.2.5. Let \mathcal{P} be a set of polynomials of degree at most d^* in $\mathbb{K}[x_1, x_2, \dots, x_n]$ with \mathbb{K} being any algebraically closed field. The annihilator of \mathcal{P} is the set \mathcal{P}° of vectors $\lambda = (\lambda_{x^\alpha})_{|\alpha| \leq d^*}$ such that the equality

$$\sum_{|\alpha| \leq d^*} p_\alpha \lambda_{x^\alpha} = 0 \quad (4.2.12)$$

holds for every polynomial $p(x) = \sum_{|\alpha| \leq d^*} p_\alpha x^\alpha$ of \mathcal{P} .

Viewing $\mathbb{K}[x_1, x_2, \dots, x_n]$ as a vector space, we see that the annihilator of a set \mathcal{P} is equal to the annihilator of its linear span. Moreover, we see that (4.2.12) is a linear relaxation of the polynomial system

$$p(x) = 0, \quad \forall p \in \mathcal{P}. \quad (4.2.13)$$

Indeed, any solution $x \in \mathbb{K}^n$ to (4.2.13) generates an element of \mathcal{P}° by setting $\lambda_{x^\alpha} := x^\alpha$ for every multi-index $|\alpha| \leq d^*$. Clearly, the reverse direction does not hold as the variables λ_{x^α} do not take into account constraints of the type $\lambda_{x^{\alpha+\beta}} = \lambda_{x^\alpha} \lambda_{x^\beta}$.

Now, let $d \geq 1$ be any integer and consider the set

$$\mathcal{P}_d := \{x^\alpha p : |\alpha| \leq d, p \in \mathcal{P}\}.$$

Then, we see that the annihilator of \mathcal{P}_d is equal to the set of vectors λ orthogonal to the columns of the linear system derived from

$$r_1(x)p_1(x) + \dots + r_m(x)p_m(x) = 1,$$

where the polynomials r_i have degree at most d . In particular, using Fredholm's Theorem of the Alternative we obtain the following simple result.

Proposition 4.2.6. Suppose that the system (4.2.13) is infeasible. Then, this system has a Nullstellensatz Certificate of degree d if and only if every $\lambda \in \mathcal{P}_d^\circ$ satisfies $\lambda_1 = 0$.

The proposition above motivates the following definition:

Definition 4.2.7. Let \mathcal{P} and \mathcal{P}_d as above. A vector $\lambda \in \mathcal{P}_d^\circ$ with $\lambda_1 \neq 0$ is called a **Nullstellensatz Dual Certificate** of degree d .

As we mentioned before, proving the existence or non-existence of Nullstellensatz Dual Certificates is much easier than proving the existence of Nullstellensatz Certificates in cases when the polynomials are sparse. In what follows we will use these ideas to give a much shorter prove of a result due to De Loera et. al. [20] stating that if $k \geq \alpha(G) + 1$, then (STAB) has a minimum Nullstellensatz Certificate of degree $\alpha(G)$. We begin with the following theorem:

Theorem 4.2.8. *The polynomial system (STAB) has a Nullstellensatz Dual Certificate of degree d if and only if there exists a solution to the system*

$$\begin{aligned} -k\lambda_S + \sum_{i \in V} \lambda_{S \cup \{i\}} &= 0 \quad |S| \leq d, \quad S \subseteq V \text{ stable}, \\ \lambda_S &= 0 \quad |S| \leq d+2, \quad S \subseteq V \text{ not stable}, \\ \lambda_\emptyset &\neq 0. \end{aligned} \tag{4.2.14}$$

Proof. Let \mathcal{P} be the set of polynomials defined in (STAB) and let \mathcal{P}_d be defined as above. Then, every $\lambda \in \mathcal{P}_d^\circ$ satisfies the equations:

$$\begin{aligned} -k\lambda_{x^\alpha} + \sum_{i \in V} \lambda_{x_i x^\alpha} &= 0 \quad \forall |\alpha| \leq d, \\ \lambda_{x^\alpha x_i x_j} &= 0 \quad \forall \{i, j\} \in E, \quad \forall |\alpha| \leq d, \\ \lambda_{x^\alpha x_i^2} - \lambda_{x^\alpha x_i} &= 0 \quad \forall i \in V, \quad \forall |\alpha| \leq d. \end{aligned} \tag{4.2.15}$$

In particular, if a monomial x^α with $|\alpha| \leq d+2$ is divisible by some $x_i x_j$ with $\{i, j\} \in E$, then $\lambda_{x^\alpha} = 0$. Indeed, if $\alpha_i \geq 1$ and $\alpha_j \geq 1$ for some $\{i, j\} \in E$, then $\beta = \alpha - e_i - e_j$ is a multi-index of size at most $|\alpha| - 2 \leq d$ and (4.2.15) implies that

$$\lambda_{x^\alpha} = \lambda_{x^\beta x_i x_j} = 0.$$

Moreover, if two multi-indexes α and β of size at most $d+2$ are supported in the same set, then $\lambda_{x^\alpha} = \lambda_{x^\beta}$. Indeed, if $\alpha_i \geq 2$ for some $i \in V$, then $\lambda_{x^\alpha} = \lambda_{x^{\alpha-2e_i} x_i^2} = \lambda_{x^{\alpha-2e_i} x_i}$ and we have reduced the coordinate α_i by one. Repeating this process, we obtain that $\lambda_{x^\alpha} = \lambda_{x^\beta}$ where $\beta \in \mathbb{Z}_2^V$ and $\text{supp}(\alpha) = \text{supp}(\beta)$. In particular, λ is uniquely determined by the coordinates λ_{x^α} with $\alpha \in \mathbb{Z}_2^V$ and $|\alpha| \leq d+2$.

Let us use the notation $\lambda_S := \lambda_{x^\alpha}$ for every multi-index $|\alpha| \leq d+2$ supported on $S \subseteq V$. As a consequence, every solution to (4.2.15) is uniquely determined by a solution to

$$\begin{aligned} -k\lambda_S + \sum_{i \in V} \lambda_{S \cup \{i\}} &= 0 \quad |S| \leq d \text{ and } S \text{ is stable}, \\ \lambda_S &= 0 \quad |S| \leq d+2 \text{ and } S \text{ is not stable}. \end{aligned} \tag{4.2.16}$$

The theorem follows as any solution $(\lambda_S)_{|S| \leq d+2}$ to (4.2.16) with $\lambda_\emptyset \neq 0$ will generate a solution λ to (4.2.15) with $\lambda_1 \neq 0$. \square

We have the following corollaries.

Corollary 4.2.9. *Let G be a graph and let $k \geq \alpha(G) + 1$. Then, (STAB) has a Nullstellensatz Certificate of degree at most $\alpha(G)$.*

Proof. We claim that (STAB) does not have a Nullstellensatz Dual Certificate of degree $d := \alpha(G)$. Indeed, suppose that $(\lambda_S)_{|S| \leq d+2}$ is a solution to the system

$$\begin{aligned} -k\lambda_S + \sum_{i \in V} \lambda_{S \cup \{i\}} &= 0 \quad |S| \leq d \text{ and } S \text{ is stable,} \\ \lambda_S &= 0 \quad |S| \leq d+2 \text{ and } S \text{ is not stable.} \end{aligned} \tag{4.2.17}$$

We claim that $\lambda_S = 0$ for every stable set S and as a consequence $\lambda_\emptyset = 0$. We proceed by induction on $|S|$. If S is stable and $|S| = \alpha(G)$, then (4.2.17) implies that

$$-k\lambda_S + \sum_{i \in S} \lambda_{S \cup \{i\}} + \sum_{\substack{S' = S \cup \{i\} \\ i \in V, S' \text{ not stable}}} \lambda_{S'} = -k\lambda_S + |S|\lambda_S = 0 \Rightarrow \lambda_S = 0.$$

Now, suppose that $\lambda_{S'} = 0$ for every stable set S' of size greater than or equal to $m \geq 1$ and let S be a stable set of size $m - 1$. The equations in (4.2.17) imply that

$$0 = -k\lambda_S + \sum_{i \in S} \lambda_{S \cup \{i\}} = -k\lambda_S + \sum_{i \in S} \lambda_{S \cup \{i\}} + \sum_{\substack{S' = S \cup \{i\} \\ i \in V, S' \text{ stable}}} \lambda_{S'} = -k\lambda_S + |S|\lambda_S.$$

Hence, $\lambda_S = 0$ and the statement follows. \square

Corollary 4.2.10. *Let G be a graph and let $k \geq \alpha(G) + 1$. Then, (STAB) has no Nullstellensatz Certificate of degree $\alpha(G) - 1$.*

Proof. Let us show the existence of a Nullstellensatz Dual Certificate of degree $\alpha(G) - 1$. By Theorem 4.2.8, it is enough to prove the existence of some $(\lambda_S)_{|S| \leq \alpha(G)+1}$ such that

$$\begin{aligned} -k\lambda_S + \sum_{i \in V} \lambda_{S \cup \{i\}} &= 0 \quad |S| \leq \alpha(G) - 1 \text{ and } S \text{ is stable,} \\ \lambda_S &= 0 \quad |S| \leq \alpha(G) + 1 \text{ and } S \text{ is not stable,} \\ \lambda_\emptyset &\neq 0. \end{aligned} \tag{4.2.18}$$

We can create such vector as follows. Suppose that S^* is a stable set of size $\alpha(G)$. Then, set $\tilde{\lambda}_{S^*} := 1$ and $\tilde{\lambda}_S := 0$ for every set S not contained in S^* . For every stable set $S \subsetneq S^*$ define

$$\tilde{\lambda}_S := \frac{(\alpha(G) - |S|)!}{(k - |S|)!}. \tag{4.2.19}$$

We claim that $(\tilde{\lambda}_S)_{|S| \leq \alpha(G)+1}$ is a solution to (4.2.18). Indeed, for every stable set S of size at most $\alpha(G) - 1$ we have two cases. If S is not contained in S^* , then $\tilde{\lambda}_S = \tilde{\lambda}_{S \cup \{i\}} = 0$ for every $i \in V$ and as a consequence

$$-k\tilde{\lambda}_S + \sum_{i \in V} \tilde{\lambda}_{S \cup \{i\}} = 0.$$

Now, if S is contained in S^* , then

$$\begin{aligned} -k\tilde{\lambda}_S + \sum_{i \in V} \tilde{\lambda}_{S \cup \{i\}} &= -k\tilde{\lambda}_S + \sum_{i \in S} \tilde{\lambda}_S + \sum_{\substack{i \in V, S \subsetneq S' \subseteq S^* \\ S' = S \cup \{i\}}} \tilde{\lambda}_{S'}, \\ &= -k\tilde{\lambda}_S + |S|\tilde{\lambda}_S + (\alpha(G) - |S|) \frac{(\alpha(G) - |S| - 1)!}{(k - |S| - 1)!}, \\ &= -\frac{(\alpha(G) - |S|)!}{(k - |S| - 1)!} + \frac{(\alpha(G) - |S|)!}{(k - |S| - 1)!} = 0. \end{aligned} \quad (4.2.20)$$

Clearly, if S is not a stable set of G , then $\tilde{\lambda}_S = 0$. The result follows as $\tilde{\lambda}_\emptyset = \frac{\alpha(G)!}{k!} \neq 0$. \square

Let us collect these two corollaries in the following theorem:

Theorem 4.2.11 (De Loera et. al. [20]). *Let G be a graph and let $k \geq \alpha(G) + 1$. Then, (STAB) has minimal Nullstellensatz Certificate of degree $\alpha(G)$. Moreover, this Nullstellensatz Certificate contains at least one monomial per stable set of G .*

Proof. By Corollary 4.2.9 we have the existence of such certificate and by Corollary 4.2.10 we know that it is minimal. Now, let S^* be an arbitrary stable set and let us prove that there exists a monomial x^α in the certificate such that the support of α is S^* . Suppose that this is not the case, hence we can still generate a Nullstellensatz Certificate if we remove all the columns of the system of linear equations associated to monomials x^α with α having support equal to S^* . This is equivalent to saying that the system

$$\begin{aligned} -k\lambda_S + \sum_{i \in V} \lambda_{S \cup \{i\}} &= 0 \quad |S| \leq \alpha(G), S \neq S^* \text{ and } S \text{ stable,} \\ \lambda_S &= 0 \quad |S| \leq \alpha(G) + 2 \text{ and } S \text{ not stable,} \\ \lambda_\emptyset &\neq 0, \end{aligned} \quad (4.2.21)$$

has no solution. However, if we define the vector with coordinates $\tilde{\lambda}_{S^*} := 1$, $\tilde{\lambda}_S := 0$ for every set S not contained in S^* and $\tilde{\lambda}_S := \frac{(\alpha(G) - |S|)!}{(k - |S|)!}$ for every $S \subsetneq S^*$, then $(\tilde{\lambda}_S)_{|S| \leq \alpha(G)+2}$ will be a solution to (4.2.21). This is a contradiction and the proof follows. \square

Chapter 5

Hilbert's Nullstellensatz and Graph Coloring Problems

In this chapter we will study the behavior of NullA for Graph Coloring Problems. The computational studies of Jesus De Loera, Jon Lee, Peter Malkin and Susan Margulies ([20]) showed a good behavior of NullA for systems of polynomial equations derived from some graph coloring problems. They focused on graphs having no 3-coloring and considered systems of polynomial equations over the finite field \mathbb{F}_2 .

Several families of graphs were tested, these included the graphs from the DIMACS Computational Challenge (1993-2002, <http://mat.gsia.cmu.edu/COLOR03/>), Mycielski Graphs ([46]), Kneser Graphs ([41]) and randomly generated graphs. Their results showed that the majority of these graphs had *small* Nullstellensatz Certificates. In fact, no graph having a minimal Nullstellensatz Certificate of degree bigger than *four* has been found yet (see [21] and [39]).

These results showed a big potential of NullA for Graph Coloring. However, a concrete understanding of the Nullstellensatz Certificates is still missing. The main objective of this chapter is to give a concrete study of the Nullstellensatz Dual Certificates derived from these problems. As we will see, this study will allow us to derive lower bounds for the degrees of *minimal* Nullstellensatz Certificates and we will be able to improve our understanding of NullA for graph coloring problems.

5.1 Graph Colorability

Probably, one of the most beautiful and strikingly powerful concepts in Graph Theory is that of graph colorings:

Definition 5.1.1. Let G be a graph with no loops and no multiple edges. A multi-index $\alpha \in \mathbb{Z}_k^V$ is called a k -coloring of G . A k -coloring α is called **proper** if $\alpha_u \neq \alpha_v$ for every edge $\{u, v\} \in E$. We say that G is k -colorable if it has a proper k -coloring. The minimum k such that G is k -colorable is called the **chromatic number** of G and it is denoted by $\chi(G)$.

Example 5.1.2. Consider the graph H of Figure 5.1. The multi-index

$$(0, 1, 2, 0, 1, 0, 2, 1, 3, 2) \in \mathbb{Z}_4^{10}$$

is a proper 4-coloring of H . It is not hard to see that H is not 3-colorable. Indeed, suppose

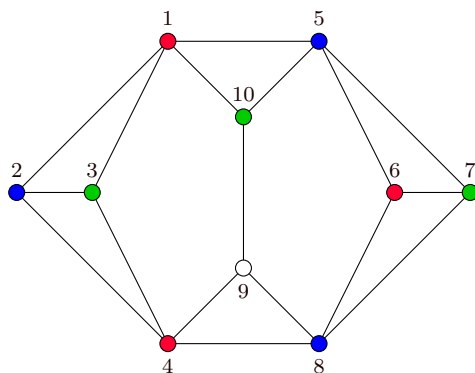


Figure 5.1: The graph H .

that $\alpha \in \mathbb{Z}_3^{10}$ is a proper 3-coloring of H . As the 3-cycles generated by the vertices 1, 2, 3 and 2, 3, 4 share the edge $\{2, 3\}$ we see that $\alpha_1 = \alpha_4$. Similarly, we see that the equality $\alpha_5 = \alpha_8$ must hold as well. But then, the 3-cycles generated by the vertices 1, 5, 10 and 4, 8, 9 imply that $\alpha_9 = \alpha_{10}$ which is a contradiction. Thus, $\kappa(H) = 4$.

Clearly, the main question we would like to answer is how to detect if a given graph is k -colorable or not. When $k = 2$ this problem is easy. Indeed, a graph is 2-colorable if and only if it is bipartite (i.e. it has no cycle of odd length), and we can check this efficiently using a simple depth-first search on the vertices of the graph. By the Four Color

Theorem ([2], [3],[52]), every planar graph is 4-colorable and as a consequence, the problem of deciding the existence of a 4-coloring for planar graphs becomes trivial. Moreover, Neil Robertson, Daniel Sanders, Paul Seymour and Robin Thomas ([50]) provided a quadratic time algorithm for finding such 4-coloring. Nevertheless, it is a hard task to detect the k -colorability of general graphs with $k \geq 3$. Richard Karp ([33]) proved that, among many other combinatorial problems, such decision problem lies in the complexity class $NP - complete$. In fact, Michael Garey, David Johnson and Larry Stockmeyer ([26]) proved that deciding the 3-colorability of a planar graph is an $NP - complete$ problem as well.

The reason why we have chosen to define colorings using multi-indexes is the following. For every graph $G = (V, E)$ and every edge $\{u, v\} \in E$ let us define the function $g_{uv} \in L^2(\mathbb{Z}_k^V)$ given by

$$g_{uv}(\alpha) := \begin{cases} 1 & \text{if } \alpha_u = \alpha_v, \\ 0 & \text{otherwise.} \end{cases} \quad (5.1.1)$$

Then, we see that G is k -colorable if and only if the system

$$g_{uv}(\alpha) = 0, \quad \forall \{u, v\} \in E, \quad (\text{COL})$$

has a solution $\alpha \in \mathbb{Z}_k^V$. Moreover, the number of solutions to (COL) is equal to the number of proper colorings of the graph G . We can use Fourier Analysis to transform (COL) into an equivalent system of polynomial equations:

Theorem 5.1.3. *A graph G is k -colorable if and only if the following system of polynomial equations has a solution over the complex numbers.*

$$\begin{aligned} q_{uv}(x) &:= 1 + x_u x_v^{k-1} + x_u^2 x_v^{k-2} + \dots + x_u^{k-1} x_v = 0 \quad \forall \{u, v\} \in E, \\ p_u(x) &:= x_u^k - 1 = 0 \quad \forall u \in V. \end{aligned} \quad (\text{FCOL})$$

Moreover, the number of solutions to (FCOL) equals the number of proper k -colorings of G .

Proof. Let $\{u, v\} \in E$ be an edge of G and let $g_{uv} \in L^2(\mathbb{Z}_k^V)$ be defined as above. Let $\beta \in \mathbb{Z}_k^V$ be any multi-index and let $\kappa_\beta \in \widehat{\mathbb{Z}_k^V}$ be the character associated to it, i.e.

$$\kappa_\beta(\alpha) := e^{\beta_1 \alpha_1 \frac{2\pi i}{k}} e^{\beta_2 \alpha_2 \frac{2\pi i}{k}} \dots e^{\beta_n \alpha_n \frac{2\pi i}{k}}, \quad \forall \alpha \in \mathbb{Z}_k^V. \quad (5.1.2)$$

By the Fourier Transform Formula (equation (3.2.3)), we know that

$$\begin{aligned}
\widehat{g}_{uv}(\kappa_\beta) &= \frac{1}{k^{|V|}} \sum_{\alpha \in \mathbb{Z}_k^V} g_{ij}(\alpha) \exp\left(\frac{2\pi i}{k} \sum_{w \in V} \alpha_w \beta_w\right), \\
&= \frac{1}{k^{|V|}} \sum_{\substack{\alpha \in \mathbb{Z}_k^V, \\ \alpha_u = \alpha_v}} \exp\left(\frac{2\pi i}{k} \sum_{w \in V} \alpha_w \beta_w\right), \\
&= \frac{1}{k^{|V|}} \left(\sum_{r \in \mathbb{Z}_k} e^{r(\beta_u + \beta_v) \frac{2\pi i}{k}} \right) \prod_{w \in V \setminus \{u, v\}} \left(\sum_{r \in \mathbb{Z}_k} e^{r\beta_w \frac{2\pi i}{k}} \right).
\end{aligned} \tag{5.1.3}$$

Recall that for every k -th root of the unity $\zeta := e^{s \frac{2\pi i}{k}}$ the equality $\sum_{r \in \mathbb{Z}_k} \zeta^r = 0$ holds. Thus, equation (5.1.3) is equivalent to

$$\widehat{g}_{uv}(\kappa_\beta) = \begin{cases} \frac{1}{k} & \text{if } \beta = r(e_u - e_v) \text{ for some } r \in \mathbb{Z}_k, \\ 0 & \text{otherwise,} \end{cases} \tag{5.1.4}$$

where $e_v \in \mathbb{Z}_k^V$ denotes the canonical multi-index having its single non-zero component in the coordinate indexed by $v \in V$. In particular, we can write (COL) as

$$g_{uv}(\alpha) = \frac{1}{k} \sum_{r \in \mathbb{Z}_k} e^{r\alpha_u \frac{2\pi i}{k}} e^{(k-r)\alpha_v \frac{2\pi i}{k}} = 0, \quad \forall \{u, v\} \in E. \tag{5.1.5}$$

The proof follows by setting $x_u := e^{\alpha_u \frac{2\pi i}{k}}$ for every $u \in V$ in the formula above. \square

We can modify (FCOL) to obtain a well known result due to Bayer in 1982:

Corollary 5.1.4 (Bayer [5]). *Theorem 5.1.3 still holds if we replace the system (FCOL) by the following polynomial system over the complex numbers.*

$$\begin{aligned}
\tilde{q}_{uv}(x) &:= x_u^{k-1} + x_u^{k-2} x_v + \cdots + x_u x_v^{k-2} + x_v^{k-1} = 0 \quad \forall \{u, v\} \in E, \\
p_u(x) &:= x_u^k - 1 = 0 \quad \forall u \in V.
\end{aligned} \tag{BCOL}$$

Proof. For each edge $\{u, v\} \in E$ multiply the polynomial q_{uv} by x_u^{k-1} to obtain

$$\begin{aligned}
x_u^{k-1} q_{uv}(x) &= x_u^{k-1} + x_u^k x_v^{k-1} + x_u^{k+1} x_v^{k-2} + \cdots + x_u^{2k-2} x_v, \\
&= \tilde{q}_{uv}(x) + \tilde{q}_{uv}(x) p_u(x).
\end{aligned}$$

Hence, for every $x \in \mathbb{C}^V$ such that $x_u^k = 1$ with $u \in V$, the equation $q_{uv}(x) = 0$ holds if and only if the equation $\tilde{q}_{uv}(x) = 0$ holds. This proves that (FCOL) is equivalent to (BCOL). \square

As a consequence of the above results, we can use NullA to detect k -colorability using either (FCOL) or (BCOL). The choice between these two systems has some advantages and disadvantages. On the one hand, the polynomials in (FCOL) are all defined by monomials of size congruent with 0 modulo k and they have a nice dual interpretation with colorings via (COL). On the other hand, the polynomials \tilde{q}_{uv} in (BCOL) have degree equal to $k - 1$ and this helps to reduce the size of the certificates (see Example 5.1.6 below). Nevertheless, as the following proposition shows, the gap between the size of the certificates for these two systems is not large.

Proposition 5.1.5. *Let G be a non- k -colorable graph. Then,*

1. *If (BCOL) has a Nullstellensatz Certificate of degree d , then (FCOL) has a Nullstellensatz Certificate of degree $d + k - 1$.*
2. *If (FCOL) has a Nullstellensatz Certificate of degree d , then (BCOL) has a Nullstellensatz Certificate of degree $d + 1$.*

Proof. 1. As in the proof of Corollary 5.1.4, for any edge $\{u, v\} \in E$ we have that

$$x_u^{k-1}q_{uv}(x) = \tilde{q}_{uv}(x) + \tilde{q}_{uv}(x)p_u(x). \quad (5.1.6)$$

Let \tilde{r}_{uv} and \tilde{s}_u be polynomials of degree d such that

$$\sum_{u \in V} \tilde{s}_u(x)p_u(x) + \sum_{\{u,v\} \in E} \tilde{r}_{uv}(x)\tilde{q}_{uv}(x) = 1.$$

Then, the equation

$$\sum_{u \in V} \tilde{s}_u(x)p_u(x) + \sum_{\{u,v\} \in E} \tilde{r}_{uv}(x) (x_u^{k-1}q_{uv}(x) - \tilde{q}_{uv}(x)p_u(x)) = 1$$

gives a Nullstellensatz Certificate of degree $d + k - 1$ for (FCOL).

2. In the same fashion, it is not hard to see that for each edge $\{u, v\} \in E$ we have the equality

$$x_u\tilde{q}_{uv}(x) = q_{uv} + p_u(x). \quad (5.1.7)$$

Hence, following the same steps as in the proof of part 1., we see that if (FCOL) has a Nullstellensatz Certificate of degree d , then (BCOL) has a Nullstellensatz Certificate of degree $d + 1$.

□

Notice that Lazard's bounds apply for both system (FCOL) and (BCOL) (see Proposition 4.1.4). Hence, in case that G is not k -colorable, there exists a Nullstellensatz Certificate of degree at most $|V|(k-1)$. Let us now look at some particular instances.

Example 5.1.6. *Let G be 3-cycle with vertex set $V = \{1, 2, 3\}$. This graph is not 2-colorable and we can certify this with a Nullstellensatz Certificate of degree $|V|(k-1) = 3$ for either (FCOL) and (BCOL). Let us use NullLA with system (BCOL) to find a minimal degree certificate. Thus, consider the system*

$$\begin{aligned} \tilde{q}_{uv}(x) &:= x_u + x_v = 0 \quad \forall \{u, v\} \in E, \\ p_u(x) &:= x_u^2 - 1 = 0 \quad \forall u \in V. \end{aligned} \tag{5.1.8}$$

It is easy to see that there is no certificate of degree zero as for each $u \in V$ the monomial x_u^2 appears in only one polynomial of the system. Hence, the scalars multiplying the polynomials p_u must be equal to zero which is impossible. Therefore, define the polynomials

$$\begin{aligned} \tilde{r}_{uv}(x) &:= b_1^{\tilde{q}_{uv}} + b_{x_1}^{\tilde{q}_{uv}} x_1 + b_{x_2}^{\tilde{q}_{uv}} x_2 + b_{x_3}^{\tilde{q}_{uv}} x_3 \quad \forall \{u, v\} \in E, \\ \tilde{s}_u(x) &:= a_1^{p_u} + a_{x_1}^{p_u} x_1 + a_{x_2}^{p_u} x_2 + a_{x_3}^{p_u} x_3 \quad \forall u \in V, \end{aligned}$$

and let us check the solubility of the system

$$\sum_{u \in V} \tilde{s}_u(x) p_u(x) + \sum_{\{u, v\} \in E} \tilde{r}_{uv}(x) \tilde{q}_{uv}(x) = 1.$$

Using NullLA, the linear system we obtain has size 20×24 and it is formed by the column concatenation of the following tableaux:

$$\begin{array}{|c|c|c|c|c|} \hline & a_1^{p_u} & a_{x_1}^{p_u} & a_{x_2}^{p_u} & a_{x_3}^{p_u} \\ \hline 1 & -1 & & & \\ x_1 & & -1 & & \\ x_2 & & & -1 & \\ x_3 & & & & -1 \\ x_u^2 & 1 & & & \\ x_u^2 x_1 & & 1 & & \\ x_u^2 x_2 & & & 1 & \\ x_u^2 x_3 & & & & 1 \\ \hline \end{array}, \begin{array}{|c|c|c|c|c|} \hline & b_1^{\tilde{q}_{uv}} & b_{x_1}^{\tilde{q}_{uv}} & b_{x_2}^{\tilde{q}_{uv}} & b_{x_3}^{\tilde{q}_{uv}} \\ \hline x_u & 1 & & & \\ x_v & 1 & & & \\ x_1 x_u & & 1 & & \\ x_2 x_u & & & 1 & \\ x_3 x_u & & & & 1 \\ x_1 x_v & & 1 & & \\ x_2 x_v & & & 1 & \\ x_3 x_v & & & & 1 \\ \hline \end{array}. \tag{5.1.9}$$

Let $\lambda := (\lambda_{x^\alpha})_{|\alpha| \leq 3}$ be an orthogonal vector to the columns of the system described by (5.1.9).

We see that λ satisfies the following system of equations:

$$\lambda_1 = \lambda_{x_u^2} \quad \forall u \in V, \quad (5.1.10)$$

$$\lambda_{x_w x_u} = -\lambda_{x_w x_v} \quad \forall w \in V, \forall \{u, w\} \in E, \quad (5.1.11)$$

$$\lambda_{x_u} = \lambda_{x_u x_v^2} \quad \forall u, v \in V, \quad (5.1.12)$$

$$\lambda_{x_u} = -\lambda_{x_v} \quad \forall w \in V, \forall \{u, w\} \in E. \quad (5.1.13)$$

Using the equations (5.1.10) and (5.1.11), we see that

$$\lambda_1 = \lambda_{x_1^2} = -\lambda_{x_1 x_2} = \lambda_{x_2 x_3} = -\lambda_{x_3^2} = -\lambda_1. \quad (5.1.14)$$

Hence, $\lambda_1 = 0$ and this shows that (5.1.8) has a Nullstellensatz Certificate of degree one. Moreover, the equations in (5.1.14) tell us which of the 20 rows and 24 columns we need to generate the certificate:

	$a_1^{p_1}$	$b_{x_1}^{\tilde{q}_{12}}$	$b_{x_2}^{\tilde{q}_{13}}$	$b_{x_3}^{\tilde{q}_{23}}$	$a_1^{p_3}$	
1	-1				-1	1
x_1^2	1	1				
$x_1 x_2$		1	1			
$x_2 x_3$			1	1		
x_3^2				1	1	
	$-\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	

(5.1.15)

As the following theorem shows, we can generalize the ideas of the above example to any non-bipartite graph G .

Theorem 5.1.7. *Let G be a non-bipartite graph. Then, (BCOL) has a minimal Nullstellensatz Certificate of degree one for the non-2-colorability of G .*

Proof. Again, let us consider the polynomials

$$\tilde{r}_{uv}(x) := b_1^{\tilde{q}_{uv}} + \sum_{w \in V} b_{x_w}^{\tilde{q}_{uv}} x_w \quad \forall \{u, v\} \in E,$$

$$\tilde{s}_u(x) := a_1^{p_u} + \sum_{v \in V} a_{x_v}^{p_u} x_v \quad \forall u \in V.$$

Let $\lambda := (\lambda_{x^\alpha})_{|\alpha| \leq 3}$ be orthogonal to the linear system associated to the equation

$$\sum_{u \in V} \tilde{s}_u(x) p_u(x) + \sum_{\{u, v\} \in E} \tilde{r}_{uv}(x) \tilde{q}_{uv}(x) = 1.$$

Then, it is not hard to see that λ is characterized by the system

$$\lambda_1 = \lambda_{x_u^2} \quad \forall u \in V, \quad (5.1.16)$$

$$\lambda_{x_w x_u} = -\lambda_{x_w x_v} \quad \forall w \in V, \forall \{u, w\} \in E, \quad (5.1.17)$$

$$\lambda_{x_u} = \lambda_{x_u x_v^2} \quad \forall u, v \in V, \quad (5.1.18)$$

$$\lambda_{x_u} = -\lambda_{x_v} \quad \forall w \in V, \forall \{u, w\} \in E. \quad (5.1.19)$$

Since G is not bipartite, it has an odd cycle. Suppose that u_0, u_1, \dots, u_{2m} are the vertices of such cycle and $\{u_0, u_{2m}\}, \{u_i, u_{i+1}\} \in E$ for every $i \in \{0, 1, \dots, 2m-1\}$. Thus, using the equations (5.1.16) and (5.1.17) we see that

$$\lambda_1 = \lambda_{x_{u_0}^2} = -\lambda_{x_{u_0} x_{u_1}} = \lambda_{x_{u_0} x_{u_2}} = \dots = \lambda_{x_{u_0} x_{u_{2m}}} = -\lambda_{x_{u_{2m}}^2} = -\lambda_1. \quad (5.1.20)$$

A minimal certificate is

$$-\frac{1}{2}(x_{u_0}^2 - 1) - \frac{1}{2}(x_{u_{2m}}^2 - 1) + \frac{1}{2}x_{u_0} \sum_{i=0}^{2m-1} (-1)^i (x_{u_i} + x_{u_{i+1}}) + \frac{1}{2}x_{u_{2m}} (x_{u_0} + x_{u_{2m}}) = 1.$$

□

We get a similar result for (FCOL) as follows.

Corollary 5.1.8. *Let G be a non-bipartite graph. Then, (FCOL) has a minimal Nullstellensatz Certificate of degree two for the non-2-colorability of G .*

Proof. By Proposition 5.1.5 and Theorem 5.1.7, we know that (FCOL) has a Nullstellensatz Certificate of degree two. Let us show that this certificate is minimal by proving the existence of a Nullstellensatz Dual Certificate of degree one for (FCOL). Once again, let us define the polynomials

$$r_{uv}(x) := b_1^{q_{uv}} + \sum_{w \in V} b_{x_w}^{q_{uv}} x_w \quad \forall \{u, v\} \in E,$$

$$s_u(x) := a_1^{p_u} + \sum_{v \in V} a_{x_v}^{p_u} x_v \quad \forall u \in V.$$

Let $\lambda = (\lambda_{x^\alpha})_{|\alpha| \leq d}$ be orthogonal to the columns of the system defined by the equation

$$\sum_{u \in V} \tilde{s}_u(x) p_u(x) + \sum_{\{u, v\} \in E} r_{uv}(x) q_{uv}(x) = 1.$$

Then, it is not hard to see that λ is characterized by the system

$$\lambda_1 = \lambda_{x_u^2} \quad \forall u \in V, \quad (5.1.21)$$

$$\lambda_1 = -\lambda_{x_u x_v} \quad \forall \{u, w\} \in E, \quad (5.1.22)$$

$$\lambda_{x_u} = \lambda_{x_u x_v^2} \quad \forall u, v \in V, \quad (5.1.23)$$

$$\lambda_{x_w} = -\lambda_{x_w x_u x_v} \quad \forall w \in V, \forall \{u, w\} \in E. \quad (5.1.24)$$

Let us define the vector $\bar{\lambda}$ with coordinates

$$\bar{\lambda}_{x^\alpha} := \begin{cases} 1 & \text{if } x^\alpha \in \{x_u^2 : u \in V\} \cup \{1\}, \\ -1 & \text{if } x^\alpha \in \{x_u x_v : \{u, v\} \in E\}, \\ 0 & \text{otherwise.} \end{cases}$$

We clearly see that $\bar{\lambda}$ gives a Nullstellensatz Dual Certificate of degree one and the proof follows. \square

The above results show that NulLA always detects 2-colorability after two iterations if we use the system (BCOL). A natural question to ask is whether for every k there exists a degree $d(k)$, independent from $|V|$ and $|E|$, such that every non- k -colorable graph has a Nullstellensatz Certificate of degree $d(k)$. As one might expect from the results of Karp concerning the hardness of k -colorability, this may be too much to ask for:

Theorem 5.1.9 (De Loera et al. [20]). *Let $k \geq 3$ be an integer. Suppose that there exists a number $d(k)$ such that every non- k -colorable graph has a Nullstellensatz Certificate of degree $d \leq d(k)$, then $P = NP$.*

Proof. We will prove that the existence of such $d(k)$ implies the existence of a polynomial-time algorithm for detecting k -colorability. Since this latter problem is in the class NP – complete ([33]) the result will follow. But this is easy. Indeed, if such $d(k)$ exists, then NulLA would detect the k -colorability of a graph $G = (V, E)$ after solving a system of linear equations of size $\binom{|V|+d(k)+k}{|V|} \times \binom{|V|+d(k)}{|V|} (|E| + |V|)$, which is a polynomial in $|V|$ and $|E|$. Since the entries of such system are only zeros, ones and minus ones, the encoding size of such system is polynomial in the size of $|V|$ and $|E|$. The result follows as every system of linear equations over the rationals can be solved in a number of elementary arithmetic operations that is polynomial in the encoding size of the system ([53]). \square

Therefore, for any $k \geq 3$ there should exist an infinite family of graphs $\{G_i\}_{i \in \mathbb{N}}$ with minimal degree certificates $\{d_i\}_{i \in \mathbb{N}}$ being unbounded. It is still an open problem to find

such family for any $k \geq 3$. Moreover, it is still an open problem to construct a graph with Nullstellensatz Certificate bigger than 4 for (BCOL), even if we consider such system over any field \mathbb{K} . We will come back to this question later on (see Section 5.3).

5.2 Nullstellensatz Dual Certificates and k -colorability

In this section we will study the annihilator of the polynomials defined by (FCOL) and (BCOL). Let $G = (V, E)$ be a non- k -colorable graph and let $d, \tilde{d} \geq 1$ be a pair of non-negative integers. Let us define the sets of polynomials

$$\begin{aligned}\mathcal{P}^F &:= \{p_w, q_{uv} : w \in V, \{u, v\} \in E\}, \\ \mathcal{P}^B &:= \{p_w, \tilde{q}_{uv} : w \in V, \{u, v\} \in E\}.\end{aligned}\tag{5.2.1}$$

As in Chapter 4, for integers $d, \tilde{d} \geq 1$ consider the sets,

$$\begin{aligned}\mathcal{P}_d^F &:= \{x^\alpha p : |\alpha| \leq d, p \in \mathcal{P}^F\}, \\ \mathcal{P}_{\tilde{d}}^B &:= \{x^\alpha p : |\alpha| \leq \tilde{d}, p \in \mathcal{P}^B\}.\end{aligned}\tag{5.2.2}$$

Thus, a vector $\lambda = (\lambda_{x^\alpha})_{|\alpha| \leq d+k}$ is in the annihilator of \mathcal{P}_d^F if and only if λ is a solution to the system

$$\begin{aligned}\lambda_{x^\alpha} - \lambda_{x^\alpha x_w^k} &= 0 \quad \forall |\alpha| \leq d, \forall w \in V \\ \lambda_{x^\alpha} + \lambda_{x^\alpha x_u^{k-1} x_v} + \cdots + \lambda_{x^\alpha x_u x_v^{k-1}} &= 0 \quad \forall |\alpha| \leq d, \forall \{u, v\} \in E.\end{aligned}\tag{5.2.3}$$

Similarly, a vector $\tilde{\lambda} = (\tilde{\lambda}_{x^\alpha})_{|\alpha| \leq \tilde{d}+k}$ is in the annihilator of $\mathcal{P}_{\tilde{d}}^B$ if and only if $\tilde{\lambda}$ is a solution to the system

$$\begin{aligned}\tilde{\lambda}_{x^\alpha} - \tilde{\lambda}_{x^\alpha x_w^k} &= 0 \quad \forall |\alpha| \leq \tilde{d}, \forall w \in V \\ \tilde{\lambda}_{x^\alpha x_u^{k-1}} + \tilde{\lambda}_{x^\alpha x_u^{k-2} x_v} + \cdots + \tilde{\lambda}_{x^\alpha x_v^{k-1}} &= 0 \quad \forall |\alpha| \leq \tilde{d}, \forall \{u, v\} \in E.\end{aligned}\tag{5.2.4}$$

Notice that we can reduce the size of the systems (5.2.3) and (5.2.4) using the equations $\lambda_{x^\alpha} = \lambda_{x^\alpha x_w^k}$ and $\tilde{\lambda}_{x^\alpha} = \tilde{\lambda}_{x^\alpha x_w^k}$. More concretely, we have the following result.

Theorem 5.2.1. *Let $G = (V, E)$ be a non- k -colorable graph. Then,*

1. (FCOL) has a Nullstellensatz Certificate of degree d if and only if the system

$$\sum_{r \in \mathbb{Z}_k} \lambda_{\alpha+r(e_u-e_v)} = 0 \quad \forall \alpha \in \mathbb{Z}_k^V, |\alpha| \leq d, \forall \{u, v\} \in E, \tag{DFCOL}$$

has no solution with $\lambda_0 \neq 0$.

2. (BCOL) has a Nullstellensatz Certificate of degree \tilde{d} if and only if the system

$$\sum_{r \in \mathbb{Z}_k} \tilde{\lambda}_{\alpha+r(e_u-e_v)-e_v} = 0 \quad \forall \alpha \in \mathbb{Z}_k^V, |\alpha| \leq \tilde{d}, \forall \{u, v\} \in E, \quad (\text{DBCOL})$$

has no solution with $\tilde{\lambda}_0 \neq 0$.

Proof. We will prove the theorem for (FCOL), the proof for (BCOL) is similar. Thus, suppose that (FCOL) has a Nullstellensatz Certificate of degree d . By Proposition 4.2.6, every vector λ in the annihilator of \mathcal{P}_d^F satisfies $\lambda_1 = 0$. Let $f := (f_\alpha)_{\alpha \in \mathbb{Z}_k^V}$ be a solution to (DFCOL), we shall prove that $f_0 = 0$.

Define the vector $\lambda = (\lambda_{x^\alpha})_{|\alpha| \leq d+k}$ given by

$$\lambda_{x^\alpha} := f_\beta \quad \text{provided that } \beta \in \mathbb{Z}_k^V \text{ and } \alpha \cong \beta \pmod{\mathbb{Z}_k^V}. \quad (5.2.5)$$

We claim that $\lambda \in (\mathcal{P}_d^F)^\circ$. Indeed, let α be any given multi-index such that $|\alpha| \leq d$ and let $\beta \in \mathbb{Z}_k^V$ be such that $\beta \cong \alpha \pmod{\mathbb{Z}_k^V}$. Then, we see that $|\beta| \leq d$. Moreover, for every vertex $w \in V$, β is also congruent with $\alpha + ke_w$ modulo \mathbb{Z}_k^V and as a consequence

$$\lambda_{x^\alpha x_w^k} - \lambda_{x^\alpha} = f_\beta - f_\beta = 0, \quad \forall |\alpha| \leq d, \forall w \in V.$$

Similarly, for every edge $\{u, v\} \in E$ and every $r \in \mathbb{Z}_k$ we have that $\beta + r(e_u - e_v)$ is congruent with $\alpha + re_u + (k-r)e_v$. Hence,

$$\lambda_{x^\alpha} + \lambda_{x^\alpha x_u^{k-1} x_v} + \cdots + \lambda_{x^\alpha x_u x_v^{k-1}} = \sum_{r \in \mathbb{Z}_k} f_{\beta+r(e_u-e_v)} = 0. \quad (5.2.6)$$

This implies that λ is in the annihilator of \mathcal{P}_d^F and $f_0 = \lambda_1 = 0$.

Now, suppose that (FCOL) has no degree d certificate. Then, by Proposition 4.2.6, (FCOL) has a Nullstellensatz Dual Certificate $\lambda \in (\mathcal{P}_d^F)^\circ$ such that $\lambda_1 \neq 0$. We claim that $\lambda_{x^\alpha} = \lambda_{x^{\alpha'}}$ provided that $\alpha \cong \alpha' \pmod{\mathbb{Z}_k^V}$ and the size of each α and α' is at most $d+k$. Indeed, let β be the unique multi-index in \mathbb{Z}_k^V congruent to both α and α' . Then, $|\beta| \leq d+k$ and there exist two sequences of multi-indexes $\beta_0, \beta_1, \dots, \beta_s$ and $\beta'_0, \beta'_1, \dots, \beta'_t$ such that

$$\begin{aligned} \beta_0 &= \beta, \beta_s = \alpha, \\ \beta'_0 &= \beta, \beta'_t = \alpha', \\ \beta_{i+1} &= \beta_i + ke_{w_i}, \quad \text{for some } w_i \in V, \forall i \in \{0, 1, \dots, s-1\}, \\ \beta'_{j+1} &= \beta'_j + ke_{w'_j}, \quad \text{for some } w'_j \in V, \forall j \in \{0, 1, \dots, t-1\}. \end{aligned} \quad (5.2.7)$$

Since λ is in the annihilator of \mathcal{P}_d^F , we conclude that $\lambda_{x^{\beta_{i+1}}} = \lambda_{x^{\beta_i}}$ and $\lambda_{x^{\beta'_{j+1}}} = \lambda_{x^{\beta'_j}}$ for every $i \in \{0, \dots, s-1\}$ and every $j \in \{0, \dots, t-1\}$. In particular, $\lambda_{x^\beta} = \lambda_{x^\alpha} = \lambda_{x^{\alpha'}}$ and our claim follows.

Define the vector f given by $f_\alpha := \lambda_{x^\alpha}$ for each $\alpha \in \mathbb{Z}_k^V \setminus \{0\}$ with $|\alpha| \leq d+k$, and $f_\alpha := 0$ otherwise. Then, by our previous claim, we see that

$$\sum_{r \in \mathbb{Z}_k} f_{\alpha+r(e_u-e_v)} = \lambda_{x^\alpha} + \lambda_{x^\alpha x_u^{k-1} x_v} + \dots + \lambda_{x^\alpha x_u x_v^{k-1}} = 0. \quad (5.2.8)$$

Hence, f is a solution to (DFCOL) with $f_0 = \lambda_1 \neq 0$ and the theorem follows. \square

We have the following corollaries:

Corollary 5.2.2. *Let G be a non- k -colorable graph. Let \mathcal{I}_V be the ideal generated by the polynomials $p_w(x) = x_w^k - 1$ with $w \in V$. Then, (FCOL) has a Nullstellensatz certificate of degree d if and only if the system*

$$q_{uv}(x) = 0, \quad \forall \{u, v\} \in E, \quad x \in \mathcal{V}_{\mathbb{C}}(\mathcal{I}_V), \quad (5.2.9)$$

has a Nullstellensatz certificate of degree d over the ring $\mathbb{C}[x_1, \dots, x_{|V|}]/\mathcal{I}_V$.

Proof. Consider the set

$$\mathcal{P}_d := \{x^\alpha q_{uv} + \mathcal{I}_V : \{u, v\} \in E, \alpha \in \mathbb{Z}_k^V, |\alpha| \leq d\} \subseteq \mathbb{C}[x_1, \dots, x_{|V|}]/\mathcal{I}_V$$

and the vector space $\mathbf{V}_d = \text{span}_{\mathbb{C}}\{\mathcal{P}_d\} \subseteq \mathbb{C}[x_1, \dots, x_{|V|}]/\mathcal{I}_V$. Then, the system (5.2.9) has a Nullstellensatz certificate of degree d if and only if $1 + \mathcal{I}_V \in \mathbf{V}_d$.

Notice that \mathbf{V}_d can be seen as a subspace of the finite dimensional space \mathbf{W}_d spanned by the monomials $x^\alpha + \mathcal{I}_V$ with $\alpha \in \mathbb{Z}_k^V$ and $|\alpha| \leq d+k$. We can identify the dual space \mathbf{W}_d^* with the set of all vectors $(\lambda_\alpha)_{\alpha \in \mathbb{Z}_k^V, |\alpha| \leq d+k}$ via the mapping

$$\lambda \in \mathbf{W}_d^* \mapsto (\lambda(x_\alpha + \mathcal{I}_V))_{\alpha \in \mathbb{Z}_k^V, |\alpha| \leq d+k}.$$

Thus, a linear functional $\lambda \in \mathbf{W}_d^*$ satisfies $\lambda(p(x) + \mathcal{I}_V)$ for every $p(x) + \mathcal{I}_V \in \mathbf{V}_d$ if and only if its corresponding vector $(\lambda_\alpha)_{\alpha \in \mathbb{Z}_k^V, |\alpha| \leq d+k}$ given by $\lambda_\alpha := \lambda(x^\alpha + \mathcal{I}_V)$ is a solution to (DFCOL).

In particular, $1 + \mathcal{I}_V \in \mathbf{V}_d$ if and only if every solution $(\lambda_\alpha)_{\alpha \in \mathbb{Z}_k^V, |\alpha| \leq d+k}$ to (DFCOL) satisfies $\lambda_0 = 0$. The claim follows by the preceding theorem. \square

Corollary 5.2.3. *Let $G = (V, E)$ be a non- k -colorable graph and suppose that (FCOL) has minimal Nullstellensatz Certificate of degree d^* . Then,*

$$d^* \cong 0 \pmod{k}. \quad (5.2.10)$$

Moreover, $d^* \geq k$.

Proof. Notice that the size of α is congruent with the size of $\alpha + r(e_u - e_v)$ modulo \mathbb{Z}_k for every $r \in \mathbb{Z}_k$ and every $\{u, v\} \in E$. In particular, the equation

$$\sum_{r \in \mathbb{Z}_k} \lambda_{\alpha + r(e_u - e_v)} = 0$$

in (DFCOL) will always involve multi-indexes of size congruent with $|\alpha|$ modulo \mathbb{Z}_k . Since the existence of a certificate only depends on the value λ_0 for every solution λ to (DFCOL), the existence of a certificate depends only on the solutions to the subsystem

$$\sum_{r \in \mathbb{Z}_k} \lambda_{\alpha + r(e_u - e_v)} = 0, \quad |\alpha| \cong 0 \pmod{k}, \quad |\alpha| \leq d, \quad \forall \{u, v\} \in E. \quad (5.2.11)$$

This implies that $d^* \cong 0 \pmod{\mathbb{Z}_k}$.

Let us show the existence of a Dual Nullstellensatz Certificate of degree zero. Thus, consider the vector $(\lambda_\alpha)_{|\alpha| \leq 3}$ defined as

$$\begin{aligned} \lambda_0 &= 1, \\ \lambda_{r(e_u - e_v)} &= -\frac{1}{k-1}, \quad \forall \{u, v\} \in E, \forall r \in \mathbb{Z}_k \setminus \{0\} \\ \lambda_\alpha &= 0, \quad \text{for any other } |\alpha| \leq 3. \end{aligned}$$

Then, λ clearly satisfies the equations

$$\sum_{r \in \mathbb{Z}_k} \lambda_{\alpha + r(e_u - e_v)} = 0, \quad \forall |\alpha| \leq 0, \forall \{u, v\} \in E.$$

Since $\lambda_0 = 1$, it follows that $d^* \geq k$. □

Corollary 5.2.4 (De Loera et al. [18]). *Let $G = (V, E)$ be a non- k -colorable graph with $k \geq 3$ and suppose that (BCOL) has minimal Nullstellensatz Certificate of degree d^* . Then,*

$$d^* \cong 1 \pmod{k}. \quad (5.2.12)$$

Moreover, $d^* \geq k + 1$.

Proof. Suppose that G has a minimal Nullstellensatz Certificate of degree d^* . By the same arguments used in Corollary 5.2.3, it is clear that

$$d^* \cong 1 \pmod{k}.$$

Let us show the existence of a Dual Nullstellensatz Certificate $(\tilde{\lambda}_\alpha)_{|\alpha| \leq k+1}$ of degree one. We will consider the cases $k \geq 4$ and $k = 3$ separately.

First, suppose that $k \geq 4$ and let $\zeta \neq 1$ be a k -th root of the unity (if $k = 4$ choose $\zeta := -1$). Let us identify the set of vertices of G with the set of integers $[n]$ where $|V| = n$. Define $\tilde{\lambda} := (\tilde{\lambda}_\alpha)_{|\alpha| \leq k+1}$ as follows,

$$\begin{aligned} \tilde{\lambda}_{r(e_u - e_v)} &:= \zeta^r, \quad \forall r \in \mathbb{Z}_k, \forall \{u, v\} \in E, u < v, \\ \tilde{\lambda}_{e_w + 2e_u - 3e_v} &:= -\tilde{\lambda}_{e_w - e_v}, \quad \forall \{u, v\}, \{v, w\} \in E, \\ \tilde{\lambda}_\alpha &:= 0 \quad \text{for any other multi-index } |\alpha| \leq k+1. \end{aligned} \tag{5.2.13}$$

Notice that $\tilde{\lambda}$ is well defined. The only possible inconsistency might come up for the case $k = 4$, as the multi-indexes $e_w + 2e_u - 3e_v$ and $-3e_w + 2e_u + e_v$ are the same. However, since we set $\zeta = -1$ for this case, the equalities

$$\tilde{\lambda}_{e_w - e_v} = \tilde{\lambda}_{e_v - e_w} = \zeta = \zeta^3,$$

hold and $\tilde{\lambda}$ is well defined.

We claim that $\tilde{\lambda}$ is a Nullstellensatz Dual Certificate of degree one. Indeed, since $\tilde{\lambda}_0 = 1$, we only need to prove that $\tilde{\lambda}$ satisfies the equalities

$$\sum_{r \in \mathbb{Z}_k} \tilde{\lambda}_{e_w + r(e_u - e_v) - e_v} = 0$$

for every $w \in V$ and every $\{u, v\} \in E$. On the one hand, if $w \in \{u, v\}$ then

$$\sum_{r \in \mathbb{Z}_k} \tilde{\lambda}_{e_w + r(e_u - e_v) - e_v} = \sum_{r \in \mathbb{Z}_k} \tilde{\lambda}_{r(e_u - e_v)} = \sum_{r \in \mathbb{Z}_k} \zeta^r = 0.$$

On the other hand, if $w \notin \{u, v\}$, then by the way we defined $\tilde{\lambda}$, we see that

$$\tilde{\lambda}_{e_w + r(e_u - e_v) - e_v} = 0, \quad \forall r \notin \{0, 2, k-3, k-1\}.$$

In particular,

$$\sum_{r \in \mathbb{Z}_k} \tilde{\lambda}_{e_w + r(e_u - e_v) - e_v} = \tilde{\lambda}_{e_w - e_v} + \tilde{\lambda}_{e_w + 2e_u - 3e_v} + \tilde{\lambda}_{e_w - 3e_u + 2e_v} + \tilde{\lambda}_{e_w - e_u}. \tag{5.2.14}$$

Now, if the edges $\{u, w\}$ and $\{v, w\}$ are not in E , then (5.2.14) is zero as

$$\tilde{\lambda}_{e_w - e_v} = \tilde{\lambda}_{e_w + 2e_u - 3e_v} = \tilde{\lambda}_{e_w - 3e_u + 2e_v} = \tilde{\lambda}_{e_w - e_u} = 0,$$

by the definition of $\tilde{\lambda}$. If any of $\{u, w\}$ or $\{v, w\}$ is in E , then

$$\tilde{\lambda}_{e_w - e_v} + \tilde{\lambda}_{e_w + 2e_u - 3e_v} = 0 \quad \text{or} \quad \tilde{\lambda}_{e_w - 3e_u + 2e_v} + \tilde{\lambda}_{e_w - e_u} = 0.$$

Thus, (5.2.14) is zero and $\tilde{\lambda}$ is a Dual Nullstellensatz Certificate of degree one. Now, let us consider the case $k = 3$. This time, define $\tilde{\lambda} := (\tilde{\lambda}_\alpha)_{|\alpha| \leq k+1}$ as

$$\begin{aligned} \tilde{\lambda}_0 &:= 1, \\ \tilde{\lambda}_{e_u - e_v} = \tilde{\lambda}_{e_v - e_u} &:= -\frac{1}{2}, \quad \forall \{u, v\} \in E, \\ \tilde{\lambda}_{e_w + e_u + e_v} &:= \frac{1}{2}, \quad \forall \{u, v\}, \{v, w\} \in E, \{u, w\} \notin E, \\ \tilde{\lambda}_{e_w + e_v + e_u} &:= 1, \quad \forall \{u, v\}, \{v, w\}, \{u, w\} \in E, \\ \tilde{\lambda}_\alpha &:= 0 \quad \text{for any other multi-index } |\alpha| \leq k+1, \end{aligned} \tag{5.2.15}$$

We will show that for every $w \in V$ and every $\{u, v\} \in E$ the equation

$$\tilde{\lambda}_{e_w + 2e_u} + \tilde{\lambda}_{e_w + e_u + e_v} + \tilde{\lambda}_{e_w + 2e_v} = 0 \tag{5.2.16}$$

holds. Since $\tilde{\lambda}_0 \neq 0$, the statement follows. Again, if $w \in \{u, v\}$, then

$$\tilde{\lambda}_{e_w + 2e_u} + \tilde{\lambda}_{e_w + e_u + e_v} + \tilde{\lambda}_{e_w + 2e_v} = \tilde{\lambda}_0 + \tilde{\lambda}_{e_u + 2e_v} + \tilde{\lambda}_{2e_u + e_v} = 1 - \frac{1}{2} - \frac{1}{2}.$$

If $w \notin \{u, v\}$ and the edges $\{u, w\}$ and $\{v, w\}$ are not in E , then

$$\tilde{\lambda}_{e_w + 2e_u} + \tilde{\lambda}_{e_w + e_u + e_v} + \tilde{\lambda}_{e_w + 2e_v} = 0 + 0 + 0 = 0.$$

If $w \notin \{u, v\}$ and $\{v, w\} \in E$, but $\{u, w\} \notin E$, then

$$\tilde{\lambda}_{e_w + 2e_u} + \tilde{\lambda}_{e_w + e_u + e_v} + \tilde{\lambda}_{e_w + 2e_v} = 0 + \frac{1}{2} - \frac{1}{2} = 0.$$

Finally, if $w \notin \{u, v\}$ and $\{v, w\}, \{u, w\} \in E$, then

$$\tilde{\lambda}_{e_w + 2e_u} + \tilde{\lambda}_{e_w + e_u + e_v} + \tilde{\lambda}_{e_w + 2e_v} = -\frac{1}{2} + 1 - \frac{1}{2} = 0.$$

This concludes the proof. □

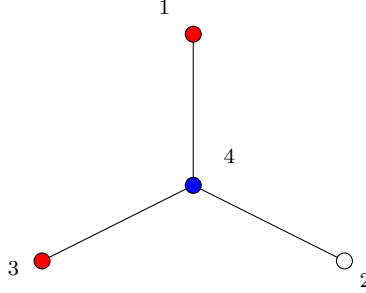


Figure 5.2: A 3-star

Remark 5.2.5. *We must point out that the proof of the case $k > 3$ is independent from the underlying field. Thus, it can be seen as an alternative proof to that of [18]. For the case $k = 3$, there exist graphs with minimal Nullstellensatz Certificates of degree one over \mathbb{F}_2 . Such graphs have been already characterized ([39], [19]).*

Example 5.2.6. *Consider the graph of Figure 5.2. Clearly, this graph is 3-colorable (it is 2-colorable) and hence (FCOL) has Nullstellensatz Dual Certificates of any degree for $k = 3$. We can find such certificates using proper three colorings of the graph. For instance, let $\beta := (0, 1, 0, 2)$ and set*

$$\lambda_\alpha := \kappa_\beta(\alpha), \quad \forall \alpha \in \mathbb{Z}_3^3.$$

Notice that β is a proper three coloring of the graph. Thus, for every multi-index $\alpha \in \mathbb{Z}_3^3$ and every edge $\{u, v\} \in E$ we have

$$\begin{aligned} \lambda_\alpha + \lambda_{\alpha+(e_u-e_v)} + \lambda_{\alpha+2(e_u-e_v)} &= \kappa_\beta(\alpha) (1 + \kappa_\beta(e_u - e_v) + \kappa_\beta(2e_u - 2e_v)), \\ &= \kappa_\beta(\alpha) \left(1 + e^{(\beta_u-\beta_v)\frac{2\pi i}{3}} + e^{2(\beta_u-\beta_v)\frac{2\pi i}{3}} \right), \\ &= 0 \end{aligned}$$

Since $\lambda_0 = 1$, the vector λ is a Dual Nullstellensatz Certificate (of any degree).

5.2.1 Using symmetries to find Nullstellensatz Certificates

It is possible to reduce the size of (DFCOL) using the symmetries of the graph G . Indeed, let $\phi : V \rightarrow V$ be a *graph automorphism*, i.e., ϕ is a bijection such that $\{\phi(u), \phi(v)\} \in E$ for every $\{u, v\} \in E$. Then, ϕ naturally defines a mapping $\bar{\phi} : \mathbb{Z}_k^V \rightarrow \mathbb{Z}_k^V$ given by

$$\bar{\phi}(\alpha) = (\alpha_{\phi^{-1}(u)})_{u \in V}.$$

The set of all group automorphisms of a graph G forms a group under composition of functions. Such group is called the *automorphism group* of G and it is denoted by $Aut(G)$.

Lemma 5.2.7 (See [20] Theorem 3.5 for a similar result). *Let $G = (V, E)$ be a non- k -colorable graph and let $Aut(G)$ be the automorphism group of G . Then, G has a Nullstellensatz Certificate of degree d if and only if every solution to the system*

$$\begin{aligned} \sum_{r \in \mathbb{Z}_k} \lambda_{\alpha+r(e_u-e_v)} &= 0, & |\alpha| \leq d, \quad \forall \{u, v\} \in E, \\ \lambda_\alpha - \lambda_{\bar{\phi}(\alpha)} &= 0, & |\alpha| \leq d+k, \quad \forall \phi \in Aut(G). \end{aligned} \tag{Aut-DFCOL}$$

satisfies $\lambda_0 = 0$.

Proof. Let λ be a solution to (DFCOL) and define the vector $\bar{\lambda}$ given by

$$\bar{\lambda}_\alpha := \frac{1}{|Aut(G)|} \sum_{\phi \in Aut(G)} \lambda_{\bar{\phi}(\alpha)}, \quad |\alpha| \leq d+k.$$

We claim that $\bar{\lambda}$ is a solution to (Aut-DFCOL). Indeed, for every multi-index α of size at most d and every edge $\{u, v\} \in E$, we have

$$\begin{aligned} \sum_{r \in \mathbb{Z}_k} \bar{\lambda}_{\alpha+r(e_u-e_v)} &= \sum_{r \in \mathbb{Z}_k} \left(\frac{1}{|Aut(G)|} \sum_{\phi \in Aut(G)} \lambda_{\bar{\phi}(\alpha+r(e_u-e_v))} \right), \\ &= \frac{1}{|Aut(G)|} \sum_{\phi \in Aut(G)} \underbrace{\left(\sum_{r \in \mathbb{Z}_k} \lambda_{\bar{\phi}(\alpha)+r(e_{\phi(u)}-e_{\phi(v)})} \right)}_{=0}, \\ &= 0. \end{aligned}$$

The last equality follows from the fact that λ is a solution to (DFCOL), the size of $\bar{\phi}(\alpha)$ is at most d for every $\phi \in Aut(G)$ and that $\{\phi(u), \phi(v)\} \in E$.

Now, for every $\phi' \in Aut(G)$ and every multi-index α of size at most $d+k$ we have

$$\begin{aligned} \bar{\lambda}_{\phi'(\alpha)} &= \frac{1}{|Aut(G)|} \sum_{\phi \in Aut(G)} \lambda_{\bar{\phi} \circ \phi'(\alpha)}, \\ &= \frac{1}{|Aut(G)|} \sum_{\phi \in Aut(G)} \lambda_{\bar{\phi}(\alpha)}, \\ &= \bar{\lambda}_\alpha. \end{aligned}$$

This proves our claim. Now, since $\lambda_0 = \bar{\lambda}_0$, the above shows that the existence of a Nullstellensatz Dual Certificate of degree d implies the existence of a solution $\bar{\lambda}$ to (Aut-DFCOL) with $\bar{\lambda}_0 \neq 0$. As every solution to (Aut-DFCOL) is a solution to (DFCOL), the result follows. \square

Example 5.2.8. *Let $G = K_4$ be the complete graph with four vertices and let $k = 3$. Using the above results we can easily prove that K_4 has a Nullstellensatz Certificate of degree 3 for (FCOL). Indeed, the automorphism group of G is the symmetric group S_4 . Thus, every solution λ to (Aut-DFCOL) satisfies*

$$\begin{aligned}\lambda_{(0,0,0,0)} + \lambda_{(1,2,0,0)} + \lambda_{(2,1,0,0)} &= \lambda_{(0,0,0,0)} + 2\lambda_{(1,2,0,0)} = 0, \\ \lambda_{(1,2,0,0)} + \lambda_{(1,2,1,2)} + \lambda_{(1,2,2,1)} &= \lambda_{(1,2,0,0)} + 2\lambda_{(1,1,2,2)} = 0, \\ \lambda_{(1,2,0,0)} + \lambda_{(1,0,2,0)} + \lambda_{(1,1,1,0)} &= \lambda_{(1,1,1,0)} + 2\lambda_{(1,2,0,0)} = 0, \\ \lambda_{(1,1,1,0)} + \lambda_{(1,1,0,1)} + \lambda_{(1,1,2,2)} &= 2\lambda_{(1,1,1,0)} + \lambda_{(1,1,2,2)} = 0.\end{aligned}$$

Therefore,

$$\lambda_{(0,0,0,0)} = -2\lambda_{(1,2,0,0)} = 4\lambda_{(1,1,2,2)} = -8\lambda_{(1,1,1,0)} = 16\lambda_{(1,2,0,0)} = -8\lambda_{(0,0,0,0)}.$$

This proves that $\lambda_{(0,0,0,0)} = 0$ and the result follows.

Example 5.2.9. *The next case to consider is $G = K_5$ and $k = 4$. First, let us try to determine the existence of a Nullstellensatz Certificate of degree $d = 4$ for (FCOL). Up to permutation, there are only five multi-indexes in \mathbb{Z}_4^V of size at most four and congruent with zero modulo 4. These are*

$$\begin{aligned}\alpha_0 &:= (0, 0, 0, 0, 0), \\ \alpha_1 &:= (1, 3, 0, 0, 0), \\ \alpha_2 &:= (2, 2, 0, 0, 0), \\ \alpha_3 &:= (1, 1, 2, 0, 0), \\ \alpha_4 &:= (1, 1, 1, 1, 0).\end{aligned}$$

Now, the only equation of (Aut-DFCOL) generated by α_0 is

$$\lambda_{(0,0,0,0,0)} + 2\lambda_{(1,3,0,0,0)} + \lambda_{(2,2,0,0,0)} = 0.$$

The equations generated by α_1 are

$$\begin{aligned} 2\lambda_{(1,3,0,0,0)} + 2\lambda_{(2,3,3,0,0)} &= 0, \\ 2\lambda_{(1,3,0,0,0)} + 2\lambda_{(1,1,2,0,0)} &= 0, \\ \lambda_{(1,3,0,0,0)} + 2\lambda_{(1,1,3,3,0)} + \lambda_{(1,2,2,3,0)} &= 0. \end{aligned}$$

The equations generated by α_2 are

$$\begin{aligned} 2\lambda_{(2,2,0,0,0)} + \lambda_{(1,1,2,0,0)} + \lambda_{(2,3,3,0,0)} &= 0, \\ \lambda_{(2,2,0,0,0)} + 2\lambda_{(1,2,2,3,0)} + \lambda_{(2,2,2,2,0)} &= 0. \end{aligned}$$

The equations generated by α_3 are

$$\begin{aligned} 2\lambda_{(1,1,2,0,0)} + 2\lambda_{(1,2,2,3,0)} &= 0, \\ 2\lambda_{(1,1,2,0,0)} + \lambda_{(1,1,1,1,0)} + \lambda_{(1,1,3,3,0)} &= 0, \\ \lambda_{(1,1,2,0,0)} + 2\lambda_{(1,1,1,2,3)} + \lambda_{(1,1,2,2,2)} &= 0. \end{aligned}$$

And the only equation generated by α_4 is

$$2\lambda_{(1,1,1,1,0)} + 2\lambda_{(1,1,1,2,3)} = 0.$$

From the above equations we can see that the system (**Aut-DFCOL**) for $d = 4$ is equivalent to the system

$$\begin{aligned} \lambda_{(1,3,0,0,0)} = -\lambda_{(2,3,3,0,0)} = -\lambda_{(1,1,2,0,0)} = \lambda_{(2,2,0,0,0)} = \lambda_{(1,2,2,3,0)} = -\lambda_{(1,1,3,3,0)}, \\ \lambda_{(0,0,0,0,0)} = \lambda_{(1,1,1,1,0)} = \lambda_{(2,2,2,2,0)} = -\lambda_{(1,1,1,2,3)}, \\ \lambda_{(0,0,0,0,0)} + 3\lambda_{(1,3,0,0,0)} = 0, \\ -\lambda_{(1,3,0,0,0)} - 2\lambda_{(0,0,0,0,0)} + \lambda_{(1,1,2,2,2)} = 0. \end{aligned} \tag{5.2.17}$$

Hence, we can just set $\lambda_{(0,0,0,0,0)} = 1$ and generate a Nullstellensatz Dual Certificate of degree 4 for (**FCOL**) using the above equations.

It is not hard to see that K_5 has a degree $d = 8$ certificate. Indeed, we can add to the system (5.2.17) the equations

$$\begin{aligned} 2\lambda_{(2,2,2,2,0)} + \lambda_{(1,1,2,2,2)} + \lambda_{(2,2,2,3,3)} &= 0, \\ 2\lambda_{(1,2,2,3,0)} + 2\lambda_{(2,2,2,3,3)} &= 0, \\ 2\lambda_{(1,2,2,3,0)} + 2\lambda_{(1,1,2,2,2)} &= 0. \end{aligned} \tag{5.2.18}$$

Using the equalities $\lambda_{(2,2,2,2,0)} = \lambda_{(0,0,0,0,0)}$ and $\lambda_{(1,3,0,0,0)} = \lambda_{(1,2,2,3,0)}$, we conclude that $\lambda_{(0,0,0,0,0)} = \lambda_{(1,3,0,0,0)}$. However, the equation

$$\lambda_{(0,0,0,0,0)} + 3\lambda_{(1,3,0,0,0)} = 0,$$

implies that $\lambda_{(0,0,0,0,0)} = 0$ and our claim follows.

Remark 5.2.10. Using computing software, we found that K_6 has a minimal Nullstellensatz Certificate for (FCOL) of degree 10 and K_7 has a minimal Nullstellensatz Certificate for (FCOL) of degree 14. However, we could not find any short proof of this statement. As far as we are aware of, the above example shows the first proof (without the aid of computing software) that K_5 has a Nullstellensatz Certificate of degree 9 for (BCOL).

5.2.2 Fourier Analysis and Nullstellensatz Certificates

Recall from the last section that a graph $G = (V, E)$ is not k -colorable if and only if the system

$$g_{uv}(\alpha) = 0, \quad \forall \{u, v\} \in E, \quad (\text{COL})$$

has no solution $\alpha \in \mathbb{Z}_k^V$. By the Group Nullstellensatz, (COL) has no solution if and only if there exist functions $f_{uv} \in L^2(\mathbb{Z}_k^V)$ such that

$$\sum_{\{u,v\} \in E} f_{uv} g_{uv} = 1. \quad (\text{FNCERT})$$

From the way we derived the system (FCOL) and (BCOL), the following theorem should be no surprise at all.

Theorem 5.2.11. Let $d \geq 1$ and let \mathcal{T}_d be the set of multi-indices of size at most d . Then, G has a Nullstellensatz Certificate of degree d for (FCOL) if and only if there exist functions $f_{uv} \in L^2(\mathbb{Z}_k^V)$ with Fourier support contained in \mathcal{T}_d such that (FNCERT) holds.

Proof. By Corollary 5.2.2, G has a Nullstellensatz Certificate for (FCOL) of degree d if and only if there exist polynomials r_{uv} with $\{u, v\} \in E$ of degree at most d such that

$$\sum_{\{u,v\} \in E} r_{uv}(x) q_{uv}(x) \equiv 1 \quad \text{mod } \mathcal{I}_{G,k}.$$

Now, suppose that

$$r_{uv}(x) =: \sum_{|\beta| \leq d} r_{\beta}^{uv} x^{\beta}, \quad \forall \{u, v\} \in E,$$

and define the functions

$$f_{uv}(\alpha) := \sum_{|\beta| \leq d} r_{\beta}^{uv} \kappa_{\beta}(\alpha).$$

Then, for every $\alpha \in \mathbb{Z}_k^V$ and $\{u, v\} \in E$ we have

$$\begin{aligned} f_{uv}(\alpha)g_{uv}(\alpha) &= \left(\sum_{|\beta| \leq d} r_{\beta}^{uv} \kappa_{\beta}(\alpha) \right) \left(\sum_{\beta} \widehat{g}_{uv}(\beta) \kappa_{\beta}(\alpha) \right), \\ &= \left(\sum_{|\beta| \leq d} r_{\beta}^{uv} e^{\frac{2\pi i}{k} \sum_{u \in V} \beta_u \alpha_u} \right) \left(\sum_{r \in \mathbb{Z}_k} e^{r \alpha_u \frac{2\pi i}{k}} e^{(k-r) \alpha_v \frac{2\pi i}{k}} \right) \\ &= r_{uv}(x)q_{uv}(x), \end{aligned}$$

where $x_u := e^{\alpha_u \frac{2\pi i}{k}}$ for every $u \in V$. In particular,

$$\sum_{\{u,v\} \in E} f_{uv}g_{uv} = 1.$$

The converse is similar. □

Example 5.2.12. *It is possible to use (COL) and an a simple inclusion-exclusion argument to find (large) Nullstellensatz Certificates as follows. Let $\{u_1, v_1\}, \{u_2, v_2\}, \dots, \{u_m, v_m\} \in E$ be any enumeration of the edges of a non- k -colorable graph G . Let $f_{u_1 v_1} := 1$ and for every $2 \leq s \leq m$ define the functions*

$$f_{u_s v_s} := 1 - \left(\sum_{r=1}^{s-1} g_{u_r v_r} f_{u_r v_r} \right).$$

Then,

$$\sum_{s=1}^m g_{u_s v_s} f_{u_s v_s} = 1.$$

Indeed, for each $\{u, v\} \in E$, let \mathcal{S}_{uv} be the support of the function g_{uv} . Let us define the sets

$$\mathcal{R}_s := \mathcal{S}_{u_s v_s} \setminus \left(\bigcup_{r < s} \mathcal{S}_{u_r v_r} \right)$$

for every $s \in [m]$. Then, since G is not k -colorable, the sets $\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_m$ form a partition of the set \mathbb{Z}_k^n . We claim that

$$g_{u_s v_s} f_{u_s v_s}(\alpha) = \begin{cases} 1 & \text{if } \alpha \in \mathcal{R}_s, \\ 0 & \text{otherwise.} \end{cases} \quad (5.2.19)$$

hence, proving our initial claim. We use induction on s with the cases $s = 1$ being trivial. Suppose that for every $r < s$, the function $g_{u_r v_r} f_{u_r v_r}$ satisfies (5.2.19). Now, notice that

$$g_{u_s v_s} f_{u_s v_s} = g_{u_s v_s} - g_{u_s v_s} \left(\sum_{r=1}^{s-1} g_{u_r v_r} f_{u_r v_r} \right).$$

But then, our induction hypothesis implies that the support of $g_{u_s v_s} f_{u_s v_s}$ is equal to

$$\mathcal{S}_{i_s j_s} \setminus \left(\bigcup_{r < s} (\mathcal{S}_{i_s j_s} \cap \mathcal{R}_r) \right) = \mathcal{R}_s,$$

and the statement follows.

From the convolution theorem, we see that (FNCERT) is equivalent to

$$\sum_{\{u,v\} \in E} \widehat{g}_{uv} * \widehat{f}_{uv}(\alpha) = \delta_0(\alpha). \quad (5.2.20)$$

We can rewrite the above equation as follows. For each $\{u, v\} \in E$, consider the matrices

$$A_{uv}(\alpha, \beta) := \begin{cases} 1 & \alpha - \beta = r(e_u - e_v), \quad \text{for some } r \in \mathbb{Z}_k, \\ 0 & \text{else.} \end{cases}$$

Then, we see that A_{uv} is the adjacency matrix of the Cayley graph $\text{Cay}(\mathbb{Z}_k^V, \mathcal{S}_{uv})$ where $\mathcal{S}_{uv} = \{r(e_u - e_v) : r \in \mathbb{Z}_k\}$. Moreover, (5.2.20) is equivalent (up to some constant factor) to the system of linear equations.

$$\sum_{\{u,v\} \in E} \frac{1}{k} A_{uv} \widehat{f}_{uv} = \delta_0. \quad (5.2.21)$$

Using the results from Chapter 3 and the properties of the functions g_{uv} , we can summarize the properties of the matrices A_{uv} in the following proposition.

Proposition 5.2.13. *Let $G = (V, E)$ be a graph. For each $\{u, v\} \in E$ let A_{uv} be as above. Then,*

1. *For every $\alpha \in \mathbb{Z}_k^V$, the character $\kappa_\alpha \in \widehat{\mathbb{Z}_k^V}$ is an eigenvector of A_{uv} with associated eigenvalue equal to $kg_{uv}(\alpha)$.*
2. *The matrix $\frac{1}{k}A_{uv}$ defines a projection of $L^2(\mathbb{Z}_k^V)$ onto the space of all functions spanned by the characters of the form κ_α with $\alpha_u = \alpha_v$. In particular, the equation $\frac{1}{k^2}A_{uv}^2 = \frac{1}{k}A_{uv}$ holds.*
3. *For every pair of edges $\{u_1, v_1\}, \{u_2, v_2\} \in E$ the matrices $A_{u_1v_1}$ and $A_{u_2v_2}$ commute.*
4. *Let $F \subseteq E$ be any subset of edges and let $T \subseteq F$ be a spanning forest of F . Then,*

$$\frac{1}{k^{|F|}} \prod_{uv \in F} A_{uv} = \frac{1}{k^{|T|}} \prod_{uv \in T} A_{uv}. \quad (5.2.22)$$

We also have an interpretation of Dual Nullstellensatz Certificates as follows. First, notice that if we want to obtain Nullstellensatz Certificates of degree d , then the system (5.2.21) should be

$$\sum_{\{u,v\} \in E} \frac{1}{k} A_{uv} \widehat{f}_{uv} = \delta_0, \quad \text{supp}(\widehat{f}) \subseteq \mathcal{T}_d. \quad (5.2.23)$$

By Fredholm's Theorem of the Alternative, (5.2.23) has no solution if and only if there exists some function $h \in L^2(\mathbb{Z}_k^V)$ such that

$$\begin{aligned} A_{uv} \widehat{h}(\alpha) &= 0, \quad \forall |\alpha| \leq d, \quad \forall \{u, v\} \in E, \\ \widehat{h}(0) &= 1. \end{aligned} \quad (5.2.24)$$

Equivalently, $h \in L^2(\mathbb{Z}_k^V)$ will be a Dual Nullstellensatz Certificate if and only if

$$\begin{aligned} \text{supp}(\widehat{hg_{uv}}) \cap \mathcal{T}_d &= \emptyset, \quad \forall \{u, v\} \in E, \\ \sum_{\alpha \in \mathbb{Z}_k} h(\alpha) &= 1. \end{aligned} \quad (5.2.25)$$

5.3 Girth and Nullstellensatz Certificates

In this section we will take a closer look at the *structure* of the system (DFCOL). In particular, we will see that it is possible to exploit the sparsity of a graph to construct Dual Nullstellensatz Certificates and hence, obtain lower bounds for the degrees of Nullstellensatz Certificates. Throughout this section we will always assume that $G = (V, E)$ is a simple, connected graph with at least two vertices. We start with a very simple observation.

Lemma 5.3.1. *Let \mathcal{Z}_0 be the set of all multi-indexes in \mathbb{Z}_k^V of size congruent with zero modulo \mathbb{Z}_k . Let $T \subseteq E$ be a spanning tree of G , then*

$$\mathcal{Z}_0 = \left\{ \alpha \in \mathbb{Z}_k^V : \alpha = \sum_{\{u,v\} \in T} r_{uv}(e_u - e_v), r_{uv} \in \mathbb{Z}_k \right\}. \quad (5.3.1)$$

Proof. The proof is by induction on $|V|$. Clearly, if $|V| = 2$ then G has a single edge and the result follows. Suppose that the result holds for every connected graph with at most $n - 1$ vertices.

Let G be a connected graph with n vertices and let $T \subseteq E$ be a spanning tree of G . Let $u \in V$ be a leaf of T with $\{u, v\} \in T$. For every $\alpha \in \mathcal{Z}_0$ consider the multi-index $\hat{\alpha} \in \mathbb{Z}_k^{V \setminus \{v\}}$ defined by

$$\hat{\alpha}_w = \begin{cases} \alpha_w & \text{if } w \neq u, \\ \alpha_u + \alpha_v & \text{if } w = u. \end{cases}$$

By our induction hypothesis, as the graph $G \setminus \{u, v\}$ is connected, we can write $\hat{\alpha}$ as

$$\hat{\alpha} = \sum_{\{u',v'\} \in T \setminus \{u,v\}} r_{u'v'}(e_{u'} - e_{v'}).$$

Hence,

$$\alpha = \sum_{\{u',v'\} \in T \setminus \{u,v\}} r_{u'v'}(e_{u'} - e_{v'}) + \alpha_v(e_v - e_u),$$

thus \mathcal{Z}_0 is contained in the right hand side of 5.3.1. The reverse inclusion is immediate. \square

The above lemma naturally motivates the following definitions. For each $0 \leq \ell \leq |E|$ let us denote by \mathcal{M}_ℓ the set of all multi-indexes that can be written as a combination of

exactly ℓ different multi-indexes of the form $e_u - e_v$ with $\{u, v\} \in E$. In other words, \mathcal{M}_ℓ is the set of all multi-indexes $\alpha \in \mathbb{Z}_k^V$ such that

$$\alpha = \sum_{\{u,v\} \in F} r_{uv}(e_u - e_v),$$

for some set of edges $F \subseteq E$ with $|F| = \ell$ and $r_{uv} \in \mathbb{Z}_k \setminus \{0\}$ for each $\{u, v\} \in F$. Notice that for two different ℓ and ℓ' the sets \mathcal{M}_ℓ and $\mathcal{M}_{\ell'}$ might intersect. In fact, the way these sets intersect is characterized by all the \mathbb{Z}_k -circulations of the graph G (see [7] for basic results on \mathbb{Z}_k -circulations). Instead, we can study the partition of \mathcal{Z}_0 given by the sets

$$\mathcal{N}_\ell := \mathcal{M}_\ell \setminus \left(\bigcup_{j \leq \ell-1} \mathcal{M}_j \right).$$

The following lemma relates the structure of the system (DFCOL) with the sets \mathcal{N}_ℓ .

Lemma 5.3.2. *Let $\ell \geq 1$ be a positive integer and let $\alpha \in \mathcal{N}_\ell$. Then, for every edge $\{u, v\} \in E$ and every $r \in \mathbb{Z}_k$ we have that*

$$\alpha + r(e_u - e_v) \in \mathcal{N}_{\ell-1} \cup \mathcal{N}_\ell \cup \mathcal{N}_{\ell+1}.$$

Moreover, if $\alpha + r'(e_u - e_v) \in \mathcal{N}_{\ell-1}$ for some $r' \in \mathbb{Z}_k$, then

$$\alpha + r(e_u - e_v) \in \mathcal{N}_{\ell-1} \cup \mathcal{N}_\ell \quad \forall r \in \mathbb{Z}_k.$$

Proof. Let $\alpha \in \mathcal{N}_\ell$, $\{u, v\} \in E$ and $r \in \mathbb{Z}_k$ be as in the statement. Suppose that $\alpha + r(e_u - e_v) \in \mathcal{N}_j$ for some $j < \ell - 1$. Hence, there exist some $F \subseteq E$ such that $|F| = j$ and

$$\alpha + r(e_u - e_v) = \sum_{\{u',v'\} \in F} r_{u'v'}(e_{u'} - e_{v'}).$$

for some $r_{u'v'} \in \mathbb{Z}_k$. Hence, if we let $F' = F \cup \{u, v\}$ then

$$\alpha = \sum_{\{u',v'\} \in F'} r_{u'v'}(e_{u'} - e_{v'}),$$

for some $r_{u'v'} \in \mathbb{Z}_k$. In particular, $\alpha \in \mathcal{M}_{j+1}$ with $j+1 < \ell$. This contradicts the definition of \mathcal{N}_ℓ and the claim follows.

Now, suppose that $\alpha + r'(e_u - e_v) \in \mathcal{N}_{\ell-1}$ and let $F \subseteq E$ be such that $|F| = \ell - 1$ and

$$\alpha + r'(e_u - e_v) = \sum_{\{u',v'\} \in F} r_{u'v'}(e_{u'} - e_{v'}).$$

Then, for every $r \in \mathbb{Z}_k$ we have

$$\alpha + r(e_u - e_v) = \sum_{\{u',v'\} \in F} r_{u'v'}(e_{u'} - e_{v'}) + (r - r')(e_u - e_v) \in \mathcal{M}_\ell \cup \mathcal{M}_{\ell-1}.$$

The claim follows. \square

Lemma 5.3.3. *Let $\alpha \in \mathcal{N}_\ell$ be such that*

$$\alpha = \sum_{\{u,v\} \in F} r_{uv}(e_u - e_v), \quad (5.3.2)$$

for some set of edges $F \subseteq E$ with $|F| = \ell$ and some $r_{uv} \in \mathbb{Z}_k \setminus \{0\}$ with $\{u, v\} \in F$. Then,

1. F is a forest of G .
2. Let $T \subseteq F$ be a connected component of F . Then,

$$\alpha_T := \sum_{v \in V(T)} \alpha_v e_v \in \mathcal{N}_{|T|}.$$

In particular, α_T has size congruent with zero modulo \mathbb{Z}_k .

Proof. 1. Suppose that F has a cycle and let F' be a spanning forest of F . Since α is supported on $V(F)$ by our previous lemma, we can write α as

$$\alpha = \sum_{\{u,v\} \in F'} r'_{uv}(e_u - e_v).$$

Hence, $\alpha \in \mathcal{M}_{|F'|}$ with $|F'| < |F| = \ell$ which is a contradiction.

2. Let $T \subseteq F$ be a connected component of F . Then,

$$\alpha = \sum_{\{u,v\} \in T} r_{uv}(e_u - e_v) + \sum_{\{u,v\} \in F \setminus T} r_{uv}(e_u - e_v).$$

As T is a connected component, we see that

$$\alpha_T = \sum_{v \in V(T)} \alpha_v e_v = \sum_{\{u,v\} \in T} r_{uv}(e_u - e_v) \in \mathcal{M}_{|T|}.$$

Now, suppose that $\alpha_T \in \mathcal{N}_j$ for some $j < |T|$ and let F' be a forest of G such that $|F'| = j$ and

$$\alpha_T = \sum_{\{u,v\} \in F'} r'_{uv}(e_u - e_v).$$

In particular,

$$\alpha = \sum_{\{u,v\} \in F'} r'_{uv}(e_u - e_v) + \sum_{\{u,v\} \in F \setminus T} r_{uv}(e_u - e_v),$$

with $|F' \cup (F \setminus T)| < \ell$ which is a contradiction. □

By the above lemma, a multi-index $\alpha \in \mathcal{N}_\ell$ can always be described by a labeled forest having exactly ℓ edges. For instance, if F is a forest with ℓ edges satisfying (5.3.2), then we can view α as the forest F where each vertex $u \in V$ has been given the label α_u . Of course, such description is not always unique as we may find different ways of writing the multi-index α using ℓ edges of the graph. Nevertheless, as the following lemma shows, if ℓ is small and α has two different descriptions, then the graph must have a small cycle.

Lemma 5.3.4. *Let $\alpha \in \mathcal{N}_\ell$ for some $\ell \geq 1$. Suppose that F and F' are two different forests of G such that $|F| = |F'| = \ell$ and*

$$\alpha = \sum_{\{u,v\} \in F} r_{uv}(e_u - e_v) = \sum_{\{u,v\} \in F'} r'_{uv}(e_u - e_v), \quad (5.3.3)$$

for some $r_{uv}, r'_{uv} \in \mathbb{Z}_k \setminus \{0\}$. Then, $F \cup F'$ has a cycle of length less than or equal to 2ℓ .

Proof. Without loss of generality, let us assume that $V = [n]$ for some integer $n \geq 1$ and

$$\alpha = \sum_{\{u,v\} \in F, u < v} r_{uv}(e_u - e_v) = \sum_{\{u,v\} \in F', u < v} r'_{uv}(e_u - e_v), \quad (5.3.4)$$

for some forests F and F' as in the statement of the lemma. Then,

$$\begin{aligned}
0 &= \sum_{\substack{\{u,v\} \in F, \\ u < v}} r_{uv}(e_u - e_v) - \sum_{\substack{\{u,v\} \in F', \\ u < v}} r'_{uv}(e_u - e_v), \\
&= \sum_{\substack{\{u,v\} \in F \cap F', \\ u < v}} \underbrace{(r_{uv} - r'_{uv})}_{:=r''_{uv}}(e_u - e_v) + \sum_{\substack{\{u,v\} \in F \setminus F', \\ u < v}} \underbrace{(r_{uv})}_{:=r''_{uv}}(e_u - e_v) + \sum_{\substack{\{u,v\} \in F' \setminus F, \\ u < v}} \underbrace{(-r'_{uv})}_{:=r''_{uv}}(e_u - e_v), \\
&= \sum_{\substack{\{u,v\} \in F \cup F', \\ u < v}} r''_{uv}(e_u - e_v).
\end{aligned}$$

Thus,

$$0 = \sum_{u \in V} \left(\sum_{\substack{\{u,v\} \in F \cup F', \\ u < v}} r''_{uv} - \sum_{\substack{\{u,v\} \in F \cup F', \\ v < u}} r''_{uv} \right) e_u. \quad (5.3.5)$$

Let $F'' \subseteq F \cup F'$ be the set of edges $\{u, v\} \in F \cup F'$ with $u < v$ such that $r''_{uv} \neq 0$. Since F and F' are different, we have that $r'' \neq 0$ and hence $F'' \neq \emptyset$. Moreover, by (5.3.5), the graph $G'' := (V, F'')$ has no vertices of degree one. Thus, G'' contains a cycle of size less than or equal to $|F''| \leq |F \cup F'| \leq 2\ell$. \square

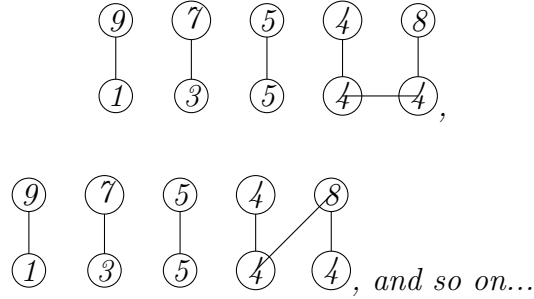
Remark 5.3.5. *The above lemma can be strengthened a little more. Indeed, suppose that F and F' are forests as in the statement where each has at least three leaves, then it is not hard to see that $F \cup F'$ actually has a cycle of length strictly less than 2ℓ .*

If the graph G has no cycles of length less than or equal to 2ℓ , i.e. G has *girth* at least $2\ell + 1$, then for every $\alpha \in \mathcal{N}_\ell$ there will be a unique forest $F(\alpha)$ with ℓ edges satisfying (5.3.2). In particular, we can represent α using the labeled forest $F(\alpha)$.

Example 5.3.6. *Let $G = K_{11}$ and consider the multi-index $\alpha = (1, 4, 7, 8, 3, 4, 4, 5, 5, 9, 0) \in \mathbb{Z}_{10}^{11}$. Let us find $\ell \in [10]$ such that $\alpha \in \mathcal{N}_\ell$. We can use a simple greedy algorithm to find this. First, we start by finding pairs of coordinates whose sum is equal to zero modulo 10. Such pairs are $(\alpha_1 = 1, \alpha_9 = 9)$, $(\alpha_3 = 7, \alpha_5 = 3)$ and $(\alpha_8 = \alpha_9 = 5)$. Now, we seek triples of numbers whose sum is congruent to zero in the remaining values $\alpha_2 = 4, \alpha_4 = 8, \alpha_6 = 4$ and $\alpha_7 = 4$. No such triple exists, thus we obtain a partition of the support of α given by the sets $U_1 := \{1, 9\}, U_2 := \{3, 5\}, U_3 := \{8, 9\}$ and $U_4 = \{2, 4, 6, 7\}$. Since $G = K_{11}$, we see that*

$$\alpha = (e_1 - e_9) + 3(e_5 - e_3) + 5(e_8 - e_9) + 2(e_2 - e_4) + 2(e_2 - e_6) + 4(e_7 - e_6) \in \mathcal{M}_5.$$

But $\alpha \notin \mathcal{M}_4$, otherwise the size of the support of α would be at most 8, however the size of the support of α is 10. Hence, $\alpha \in \mathcal{N}_5$. Notice that we can represent α with the forests:



We now state the main result of this section.

Theorem 5.3.7. *Let $G = (V, E)$ be non-3-colorable graph with minimal Nullstellensatz Certificate for (FCOL) of degree d^* . If G has girth at least six, then*

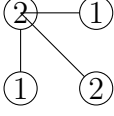
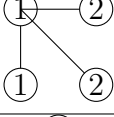
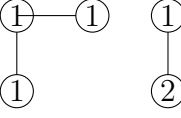
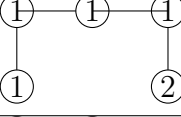
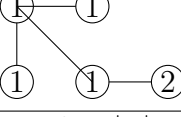
$$d^* \geq 6.$$

Proof. Suppose that G has girth at least six. We will prove that G has a Dual Nullstellensatz Certificate of degree three for (FCOL). By Theorem 5.2.1 and Corollary 5.2.3 this implies that a minimal Nullstellensatz Certificate for (FCOL) must have degree at least six.

First, notice that if $\alpha \in \mathbb{Z}_k^V$ has size $|\alpha| \in \{0, 3\}$, then the support of α has at most three vertices. In particular, the support of the multi-indexes of the form $\alpha + r(e_u - e_v)$ for some $\{u, v\} \in E$ and some $r \in \mathbb{Z}_k$ has at most five vertices. Since G has girth at least six, then the subgraph induced by the vertices in the support of $\alpha + r(e_u - e_v)$ is necessarily a forest.

Consider the vector $\lambda := (\lambda_\alpha)_{|\alpha| \leq 6}$ defined by the following table.

Type	α	λ_α	Induced Graph
(i)	0	1	—
(ii)	$e_u - e_v$	$-\frac{1}{2}$	$\textcircled{1} - \textcircled{2}$
(iii)	$e_u + e_v + e_w$	$\frac{1}{2}$	$\textcircled{1} - \textcircled{1}$
			$\textcircled{1}$
(iv)	$2e_u + 2e_v + 2e_w$	$\frac{1}{2}$	$\textcircled{2} - \textcircled{2}$
			$\textcircled{2}$
(v)	$e_u - e_v + e_{u'} - e_{v'}$	$\frac{1}{4}$	$\textcircled{2} \quad \textcircled{2}$
			$\textcircled{1} \quad \textcircled{1}$
(vi)	$e_u - e_v + e_{u'} - e_{v'}$	$\frac{1}{2}$	$\textcircled{2} - \textcircled{1}$
			$\textcircled{1} \quad \textcircled{2}$
(vii)	$e_u - e_v + e_{u'} - e_{v'}$	$-\frac{1}{2}$	$\textcircled{2} - \textcircled{1}$ $\textcircled{2} \quad \textcircled{1}$

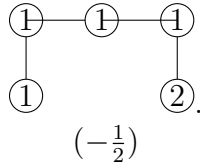
Type	α	λ_α	Induced Graph
(viii)	$e_u - e_v + e_{u'} - e_{v'}$	$-\frac{1}{2}$	
(ix)	$e_u - e_v + e_{u'} - e_{v'}$	$\frac{1}{2}$	
(x)	$e_u + e_v + e_w + e_{u'} - e_{v'}$	$-\frac{1}{4}$	
(xi)	$e_u + e_v + e_w + e_{u'} - e_{v'}$	$-\frac{1}{2}$	
(xii)	$e_u + e_v + e_w + e_{u'} - e_{v'}$	$-\frac{1}{2}$	
	α	0	Any other $ \alpha \leq 6$

We claim that λ is a Dual Nullstellensatz Certificate of degree 3. Clearly, since $\lambda_0 = 1 \neq 0$, we only need to prove the λ is a solution to (DFCOL), i.e. we need to verify that the equation

$$\lambda_\alpha + \lambda_{\alpha+e_{u'}-e_{v'}} + \lambda_{\alpha+e_v-e_{u'}} = 0 \quad (\star)$$

holds for every multi-index $\alpha \in \{0, 3\}$ and every $\{u', v'\} \in E$. Notice that this reduces to prove that if α is of any of the types (i), ..., (xi) and there exists some edge $\{u', v'\} \in E$ such that $|\alpha + r(e_{u'} - e_{v'})| \in \{0, 3\}$ for some $r \in \mathbb{Z}_3$, then the equation (\star) holds.

In order to ease notation, we will identify each of the variables λ_α with the labeled graph induced by the vertices in the support of α . For instance, say we have a multi-index $\tilde{\alpha} := e_u + e_v + e_w$ and an edge $\{u', v'\} \in E$ such that the graph induced by the vertices u, v, w, u' and v' only contains the edges $\{u, v\}, \{v, w\}, \{u', v'\}$ and $\{u', w\}$ (i.e. $\tilde{\alpha} + e_{u'} - e_{v'}$ is of type (xi) in the table). Then, the variable $\lambda_{\tilde{\alpha}+e_{u'}-e_{v'}}$ (whose value equals $-\frac{1}{2}$) will be represented by the figure



We will also write equations using these graphs. For instance, the multi-index $\tilde{\alpha}$ has size three and hence the equation

$$\lambda_{\tilde{\alpha}} + \lambda_{\tilde{\alpha}+e_{u'}-e_{v'}} + \lambda_{\tilde{\alpha}-e_{u'}+e_{v'}} = 0$$

appears in (DFCOL) (of degree 3). Thus, the above equation can be written as

$$\begin{array}{c} \textcircled{1} \\ | \\ \textcircled{1} \end{array} - \textcircled{1} - \textcircled{} + \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{1} \end{array} - \textcircled{1} - \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{2} \end{array} + \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{1} \end{array} - \textcircled{1} - \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \end{array} = 0. \quad (5.3.6)$$

$(\frac{1}{2}) \qquad \qquad (-\frac{1}{2}) \qquad \qquad (0)$

Notice that the multi-index $\tilde{\alpha} - e_{u'} + e_{v'}$ does not appear on the table so $\lambda_{\tilde{\alpha}-e_{u'}+e_{v'}} = 0$. We continue the proof of the theorem by considering the following cases.

1. **Type (i).** Suppose that α is of type (i). Then, $\alpha = 0$ and for every edge $\{u, v\} \in E$ the equation

$$\lambda_0 + \lambda_{e_u-e_v} + \lambda_{e_v-e_u} = 1 - \frac{1}{2} - \frac{1}{2} = 0, \quad (5.3.7)$$

shows that (★) holds for any multi-index of type (i). Notice that we can write the above equation using the graph representation of the multi-indexes:

$$\begin{array}{c} \textcircled{} \\ | \\ \textcircled{} \end{array} + \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \end{array} + \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{2} \end{array} = 0 \quad (5.3.8)$$

$(1) \qquad (-\frac{1}{2}) \qquad (-\frac{1}{2})$

2. **Type (ii).** Suppose that $\alpha := e_u - e_v$ is of type (ii). Then, α has size three and hence, for every $\{u'v'\} \in E$ the equation (★) holds. There are three cases we consider:

1. Suppose that $\{u, v\} = \{u', v'\}$, then (★) is the same as equation (5.3.8).
2. Suppose the graph induced by u, v, u' and v' has two disjoint edges. Thus, (★) is the equation:

$$\begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \end{array} - \textcircled{} + \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \end{array} - \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \end{array} + \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \end{array} - \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{2} \end{array} = 0 \quad (5.3.9)$$

$(-\frac{1}{2}) \qquad \qquad (\frac{1}{4}) \qquad \qquad (\frac{1}{4})$

3. Suppose the graph induced by u, v, u' and v' has only two meeting edges. Then (★) can be either

$$\begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \\ (-\frac{1}{2}) \end{array} \text{---} \circ + \begin{array}{c} \textcircled{1} \text{---} \textcircled{1} \\ | \\ \textcircled{1} \\ (\frac{1}{2}) \end{array} + \begin{array}{c} \circ \text{---} \textcircled{2} \\ | \\ \textcircled{1} \\ (0) \end{array} = 0 \quad (5.3.10)$$

or,

$$\begin{array}{c} \textcircled{1} \\ | \\ \textcircled{2} \\ (-\frac{1}{2}) \end{array} \text{---} \circ + \begin{array}{c} \textcircled{2} \text{---} \textcircled{2} \\ | \\ \textcircled{2} \\ (\frac{1}{2}) \end{array} + \begin{array}{c} \circ \text{---} \textcircled{1} \\ | \\ \textcircled{2} \\ (0) \end{array} = 0 \quad (5.3.11)$$

4. Suppose the graph induced by u, v, u' and v' has only three edges. Since G has girth six, such graph cannot have a three cycle. Thus, the equation (★) can be either

$$\begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \\ (-\frac{1}{2}) \end{array} \text{---} \circ \text{---} \circ + \begin{array}{c} \textcircled{2} \text{---} \textcircled{2} \\ | \quad | \\ \textcircled{1} \quad \textcircled{1} \\ (0) \end{array} + \begin{array}{c} \textcircled{2} \text{---} \textcircled{1} \\ | \quad | \\ \textcircled{1} \quad \textcircled{2} \\ (\frac{1}{2}) \end{array} = 0 \quad (5.3.12)$$

or,

$$\begin{array}{c} \textcircled{1} \\ | \\ \textcircled{2} \\ (-\frac{1}{2}) \end{array} \text{---} \circ \text{---} \circ + \begin{array}{c} \textcircled{1} \text{---} \textcircled{2} \\ | \quad | \\ \textcircled{2} \quad \textcircled{1} \\ (\frac{1}{2}) \end{array} + \begin{array}{c} \textcircled{1} \text{---} \textcircled{1} \\ | \quad | \\ \textcircled{2} \quad \textcircled{2} \\ (0) \end{array} = 0. \quad (5.3.13)$$

3. **Type (iii).** Suppose that $\alpha := e_u + e_v + e_w$ is of type (iii) with $\{u, v\}, \{v, w\} \in E$. Then, for every $\{u', v'\} \in E$ the equation (★) appears in (DFCOL).

1. If $\{u', v'\}$ is equal to either $\{u, v\}$ or $\{v, w\}$, then (★) equals the equation (5.3.10).
2. If $\{u', v'\}$ meets one of $\{u, v\}$ or $\{v, w\}$, then (★) equals to either

$$\begin{array}{c} \textcircled{1} \text{---} \textcircled{1} \\ | \quad | \\ \textcircled{1} \quad \circ \\ (\frac{1}{2}) \end{array} + \begin{array}{c} \textcircled{1} \text{---} \textcircled{2} \\ | \quad | \\ \textcircled{1} \quad \textcircled{2} \\ (-\frac{1}{2}) \end{array} + \begin{array}{c} \textcircled{1} \text{---} \circ \\ | \quad | \\ \textcircled{1} \quad \textcircled{1} \\ (0) \end{array} = 0, \quad (5.3.14)$$

or,

$$\begin{array}{c} \textcircled{1} - \textcircled{1} \\ | \quad \diagdown \\ \textcircled{1} \quad \circ \end{array} + \begin{array}{c} \textcircled{2} - \textcircled{1} \\ | \quad \diagdown \\ \textcircled{1} \quad \textcircled{2} \end{array} + \begin{array}{c} \circ - \textcircled{1} \\ | \quad \diagdown \\ \textcircled{1} \quad \textcircled{1} \end{array} = 0. \quad (5.3.15)$$

$\left(\frac{1}{2}\right) \quad \quad \quad \left(-\frac{1}{2}\right) \quad \quad \quad (0)$

3. If $\{u', v'\}$ is disjoint from the edges $\{u, v\}$ or $\{v, w\}$ and no other edge is in the graph induced by the vertices u, v, w, u' and v' , then (\star) equals to

$$\begin{array}{c} \textcircled{1} - \textcircled{1} \\ | \\ \textcircled{1} \end{array} \quad \circ + \begin{array}{c} \textcircled{1} - \textcircled{1} \\ | \\ \textcircled{1} \end{array} \quad \textcircled{2} \\ | \\ \textcircled{1} \end{array} + \begin{array}{c} \textcircled{1} - \textcircled{1} \\ | \\ \textcircled{1} \end{array} \quad \textcircled{1} \\ | \\ \textcircled{2} \end{array} = 0. \quad (5.3.16)$$

$\left(\frac{1}{2}\right) \quad \quad \quad \left(-\frac{1}{4}\right) \quad \quad \quad \left(-\frac{1}{4}\right)$

4. If $\{u', v'\}$ is disjoint from the edges $\{u, v\}$ or $\{v, w\}$ and the graph induced by the vertices u, v, w, u' and v' contains another edge, then (\star) is equal to either

$$\begin{array}{c} \textcircled{1} - \textcircled{1} - \circ \\ | \quad \quad | \\ \textcircled{1} \quad \quad \circ \end{array} + \begin{array}{c} \textcircled{1} - \textcircled{1} - \textcircled{1} \\ | \quad \quad | \\ \textcircled{1} \quad \quad \textcircled{2} \end{array} + \begin{array}{c} \textcircled{1} - \textcircled{1} - \textcircled{2} \\ | \quad \quad | \\ \textcircled{1} \quad \quad \textcircled{1} \end{array} = 0, \quad (5.3.17)$$

$\left(\frac{1}{2}\right) \quad \quad \quad \left(-\frac{1}{2}\right) \quad \quad \quad (0)$

or,

$$\begin{array}{c} \textcircled{1} - \textcircled{1} \\ | \quad \quad \diagdown \\ \textcircled{1} \quad \quad \circ - \circ \end{array} + \begin{array}{c} \textcircled{1} - \textcircled{1} \\ | \quad \quad \diagdown \\ \textcircled{1} \quad \quad \textcircled{1} - \textcircled{2} \end{array} + \begin{array}{c} \textcircled{1} - \textcircled{1} \\ | \quad \quad \diagdown \\ \textcircled{1} \quad \quad \textcircled{2} - \textcircled{1} \end{array} = 0. \quad (5.3.18)$$

$\left(\frac{1}{2}\right) \quad \quad \quad \left(\frac{1}{2}\right) \quad \quad \quad (0)$

Notice that the graph induced by the vertices u, v, w, u' and v' cannot have five edges as this would imply the existence of a cycle of length less than or equal to five.

Type (iv). Suppose that $\alpha := 2e_u + 2e_v + 2e_w$ is of type (iv) with $\{u, v\}, \{v, w\} \in E$. Since α has size six and G has no cycles of length three, the only edges $\{u', v'\} \in E$ for which $|\alpha + e_{u'} - e_{v'}| \in \{0, 3\}$ are precisely the edges in the graph induced by the vertices u, v and w . Thus, the only equation on which λ_α appears is (5.3.11).

Type (v). Suppose that $\alpha = e_u - e_v + e_{u'} - e_{v'}$ is of type (v) with $\{u, v\}, \{u', v'\} \in E$. Since α has size six and there is no edges between the vertices u, v and u', v' , by the girth constraints of the graph, the variable λ_α only appears on equations of the form (5.3.9).

Type (vi). Suppose that $\alpha = e_u - e_v + e_{u'} - e_{v'}$ is of type (vi) with $\{u, v\}, \{u', v\}, \{v', v\} \in E$. Then, λ_α appears in the following equations:

1. The equations of the form (5.3.12).
2. The equations of the form

$$\begin{array}{ccc}
 \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \\ (\frac{1}{2}) \end{array} & \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{2} \\ (-\frac{1}{2}) \end{array} & + & \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{1} \\ (-\frac{1}{2}) \end{array} & \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{2} \\ (-\frac{1}{2}) \end{array} & + & \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{1} \\ (0) \end{array} & \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{2} \\ (0) \end{array} & = 0, & (5.3.19)
 \end{array}$$

Type (vii). Suppose that $\alpha = e_u - e_v + e_{u'} - e_{v'}$ is of type (vii) with $\{u, u'\}, \{u', v'\}, \{v, v'\} \in E$. Then, λ_α only appears on the equations of the form (5.3.14) and (5.3.19).

Type (viii). Suppose that $\alpha = e_u - e_v + e_{u'} - e_{v'}$ is of type (viii) with $\{u, u'\}, \{u', v'\}, \{v, v'\} \in E$. Then, λ_α only appears on the equations of the form

- (a) 1. Equations of the form (5.3.15).
- (b) 2. Equations of the form

$$\begin{array}{ccc}
 \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{1} \\ (-\frac{1}{2}) \end{array} & \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{2} \\ (\frac{1}{2}) \end{array} & + & \begin{array}{c} \textcircled{1} \\ | \\ \textcircled{1} \\ (0) \end{array} & \begin{array}{c} \textcircled{2} \\ | \\ \textcircled{2} \\ (0) \end{array} & = 0, & (5.3.20)
 \end{array}$$

Type (ix). Suppose that $\alpha := e_u - e_v + e_{u'} - e_{v'}$ is of type (ix) with $\{u, u'\}, \{u', v'\}, \{u', v\} \in E$. Then, λ_α only appears on the equations of the form (5.3.20).

Type (x). Suppose that $\alpha := e_u + e_v + e_w + e_{u'} - e_{v'}$ is of type (x) with $\{u, v\}, \{v, w\}, \{u', v'\} \in E$. Since there are no edges between the vertices u, v, w and u', v' , λ_α appears only on the equations of the form (5.3.16).

Type (xi). Suppose that $\alpha := e_u + e_v + e_w + e_{u'} - e_{v'}$ is of type (xi) with $\{u, v\}, \{v, w\}, \{w, u'\}, \{u', v'\} \in E$. Then, λ_α only appears on the equations of the form (5.3.17).

Type (xii). Suppose that $\alpha := e_u + e_v + e_w + e_{u'} - e_{v'}$ is of type (xi) with $\{u, v\}, \{v, w\}, \{v, u'\}, \{u', v'\} \in E$. Then, λ_α only appears on the equations of the form (5.3.18).

□

We should point out that the vector λ of the above theorem is not a Dual Nullstellensatz Certificate of degree 6. Indeed, if G is not 3-colorable, then it has vertex $v \in V$ of degree at least three. Now, suppose that $\alpha := 2e_u + 2e_v + 2e_w$ is of type (iv), with $\{u, v\}, \{v, w\} \in E$ and let $v' \in V$ some other neighbor of v . Then, the system (DFCOL) (of degree six) has the equation

$$\lambda_\alpha + \lambda_{\alpha+e_{v'}-e_v} + \lambda_{\alpha-e_{v'}+e_v} = 0.$$

However, we see that $\alpha + e_{v'} - e_v$ is of type (ix) and hence

$$\begin{array}{c} \textcircled{2} \text{---} \textcircled{2} \\ | \quad \diagdown \\ \textcircled{2} \quad \circ \\ (\frac{1}{2}) \end{array} + \begin{array}{c} \textcircled{1} \text{---} \textcircled{2} \\ | \quad \diagdown \\ \textcircled{2} \quad \textcircled{1} \\ (\frac{1}{2}) \end{array} + \begin{array}{c} \circ \text{---} \textcircled{2} \\ | \quad \diagdown \\ \textcircled{2} \quad \textcircled{2} \\ (0) \end{array} \neq 0. \tag{5.3.21}$$

We believe that it is possible to find Dual Nullstellensatz Certificates of higher degree for graphs with large girth and chromatic number. In general, suppose that $d := 3r$ for some $r \geq 2$ and $G = (V, E)$ is a non-3-colorable graph with girth at least $6r + 4$. Then, for every multi-index α of size less than or equal to d and every edge $\{u, v\} \in E$, the multi-index $\alpha + e_u - e_v$ is supported in at most $3r + 2$ vertices and its induced graph is necessarily a forest. We might be able to use such local property to construct a Dual Nullstellensatz Certificate of degree d from a previously constructed Dual Nullstellensatz Certificate of degree $d - 3$.

The existence of graphs with large girth and chromatic number is due to Paul Erdős [24], who introduced the *probabilistic method* to the field of combinatorics. However, László Lovász [40] was the first to give an explicit construction of such graphs. An important family of *regular* graphs with large girth and chromatic number are the non-bipartite *Ramanujan Graphs* introduced by Lubotzky, Phillips and Sarnak [43].

Theorem 5.3.8 ([43]). *Let $p, q \in \mathbb{Z}$ be prime numbers congruent with one modulo 4. If q is a quadratic residue modulo p , then there exists a $(p + 1)$ -regular graph $X^{p,q}$ with the following properties:*

1. $X^{p,q}$ has $\frac{q(q^2-1)}{2}$ vertices.
2. $X^{p,q}$ has girth greater than or equal to $2 \log_p(q)$
3. $\chi(X^{p,q}) \geq \frac{p+1}{2\sqrt{p}}$.

Their proof is constructive. In fact $X^{p,q}$ is the Cayley Graph $Cay(PSL(\mathbb{F}_q^2), \mathcal{S}_p)$ where $PSL(\mathbb{F}_q^2)$ is the *projective special linear group* of \mathbb{F}_q^2 and \mathcal{S}_p is a set of $p + 1$ matrices determined by some particular solutions (a_0, a_1, a_2, a_3) of the equation

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p.$$

Example 5.3.9. *Let us find out the number of vertices and edges of a non-3-colorable graph $X^{p,q}$ of girth at least six. First of all, the chromatic number of $X^{p,q}$ should be at least four, thus*

$$\frac{p^2 + 1}{2\sqrt{p}} \geq 4 \quad \Leftrightarrow \quad p \geq 62.$$

The smallest prime number $p \geq 62$ congruent with one modulo four is $p := 73$. Now, the girth of $X^{p,q}$ should be greater than or equal to six. Thus,

$$2 \log_p(q) \geq 6 \quad \Leftrightarrow \quad q \geq 73^3 = 389017.$$

The smallest prime $q \geq 73^3$ congruent with one modulo four and being a quadratic residue modulo 73 is $q := 389297$. In conclusion, there exists a non-3-colorable graph of girth at least six with

$$n := 29499399488355888 \approx 2.9 \times 10^{16}$$

number of vertices and $m \approx 1.09 \times 10^{18}$ number of edges.

5.4 Using Degree-Cutter Equations

We can reduce the size of the certificates by carefully appending redundant polynomial equations to the systems (FCOL) and (BCOL) as follows. Let us denote by $\mathcal{I}_{G,k}$ the ideal generated by the polynomials in (FCOL). By the proof of Proposition 5.1.5, the ideal $\mathcal{I}_{G,k}$ and the ideal generated the polynomials in (BCOL) are equal. For any polynomial $p \in \mathcal{I}_{G,k}$ and any solution $x \in \mathbb{K}^n$ to (FCOL) we have that $p(x) = 0$, hence we can append such equation into the polynomial system and hope to obtain lower degree certificates. Moreover, we have the following lemma.

Lemma 5.4.1. *Let $p \in \mathbb{C}[x_1, \dots, x_{|V|}]$ be a polynomial that vanishes on every solution to (FCOL), then $p \in \mathcal{I}_{G,k}$. In other words, the ideal $\mathcal{I}_{G,k}$ is radical.*

Proof. By Proposition 2.7 of [15] (page 41), every zero dimensional ideal \mathcal{I} (i.e. $\mathcal{V}(\mathcal{I})$ is finite) is radical if and only if it contains a square free univariate polynomial. Now, $\mathcal{I}_{G,k}$ is clearly zero dimensional and for any $u \in V$ the polynomial $x_u^k - 1$ is a square free polynomial in $\mathcal{I}_{G,k}$. The statement follows. \square

Now, one way to obtain polynomials p as in the above lemma is to translate basic ‘graph theoretic’ statements into polynomial equations and add them to (FCOL). For instance, if a graph G has a K_k as a subgraph, then we know that every proper k -coloring of G must use all the k colors in such subgraph. We can translate this basic idea into a polynomial equation as follows.

Lemma 5.4.2. *Let $G = (V, E)$ be a non- k -colorable graph. Suppose that G contains a K_k as a subgraph and let u_1, u_2, \dots, u_k be the vertices of such subgraph. Then, the polynomial*

$$s(x) := (x_{u_1}x_{u_2} \dots x_{u_k}) + (-1)^k,$$

is in the ideal $\mathcal{I}_{G,k}$.

Proof. By Lemma 5.4.1 we only need to prove that every solution $\bar{x} \in \mathbb{C}^V$ to (FCOL) is a zero of the polynomial s . Since all the vertices u_1, \dots, u_k have an edge in common, for every solution \bar{x} to (FCOL) the values \bar{x}_{u_j} with $j \in [k]$ are different, in particular they are all the possible k -th roots of the unity. Hence,

$$\bar{x}_{u_1}\bar{x}_{u_2} \dots \bar{x}_{u_k} = e^{\frac{2\pi i}{k}} e^{2\frac{2\pi i}{k}} \dots e^{(k-1)\frac{2\pi i}{k}} = (-1)^{k+1}.$$

The statement follows. □

We obtain the following interesting result.

Theorem 5.4.3. *Let $G = (V, E)$ be a graph and let $k \geq 2$ be an odd integer. Consider the subgroup*

$$\Gamma_k := \langle e_{u_1} + \dots + e_{u_k} : u_1, \dots, u_n \in V \text{ form a } k\text{-clique} \rangle \subseteq \mathbb{Z}_k^V,$$

i.e. Γ_k is the group generated by all the multi-indices of the form $e_{u_1} + \dots + e_{u_k}$ where u_1, u_2, \dots, u_k form a K_k . If there exists an edge $\{u, v\} \in E$ such that $e_u - e_v \in \Gamma_k$, then G is not k -colorable.

Proof. Once again, consider the sets

$$\begin{aligned} \mathcal{P}^F &:= \{p_w, q_{uv} : w \in V, \{u, v\} \in E\}, \text{ and} \\ \mathcal{P}_d^F &:= \{x^\alpha p : |\alpha| \leq d, p \in \mathcal{P}^F\}, \end{aligned} \tag{5.4.1}$$

for integers $d \geq 1$. Let $\mathbf{V}_d := \text{span}_{\mathbb{C}}\{\mathcal{P}_d^F\}$ be the complex vector space spanned by the polynomials in \mathcal{P}_d^F . By Lemma 5.4.2, there exists some d^* such that for every set of vertices u_1, u_2, \dots, u_k of a k -clique in G , we have

$$(x_{u_1}x_{u_2} \dots x_{u_k}) - 1 \in \mathbf{V}_{d^*}.$$

Hence, if $\lambda \in (\mathcal{P}_{d^*}^F)^\circ$ is in the annihilator of $\mathcal{P}_{d^*}^F$, then

$$\lambda_{x_{u_1}x_{u_2}\dots x_{u_k}} = \lambda_1.$$

In particular, every solution λ to (DFCOL) (of degree d^*) satisfies

$$\lambda_{e_{u_1}+\dots+e_{u_k}} = \lambda_0.$$

Moreover, for any given $\alpha \in \mathbb{Z}_k^V$, we have that

$$x^\alpha (x_{u_1}x_{u_2}\dots x_{u_k} - 1) \in \mathbf{V}_{d^*+|\alpha|}.$$

Thus, every solution λ to (DFCOL) (of degree $d^* + |\alpha|$) satisfies the equation

$$\lambda_{e_{u_1}+\dots+e_{u_k}+\alpha} = \lambda_\alpha.$$

Now, suppose that there exists some edge $\{u, v\} \in E$ such that $e_u - e_v \in \Gamma_k$. Then, by the above discussion, for a sufficiently large degree d , every solution λ to (DFCOL) (of degree d) satisfies

$$\lambda_0 = \lambda_{e_u - e_v} = \lambda_{2(e_u - e_v)} = \dots = \lambda_{(k-1)(e_u - e_v)}.$$

Thus, the equation

$$\lambda_0 + \lambda_{e_u - e_v} + \lambda_{2(e_u - e_v)} + \dots + \lambda_{(k-1)(e_u - e_v)} = 0$$

implies that $\lambda_0 = 0$ and G has a Nullstellensatz Certificate of degree d for its non- k -colorability. \square

Example 5.4.4. Consider the graph H discussed at the beginning of the chapter. We can use Theorem 5.4.3 to prove that H is not 3-colorable (see Figure 5.3 below). Indeed, notice that

$$\begin{aligned} e_9 - e_{10} &= 2(e_{10} + e_1 + e_5) + (e_1 + e_2 + e_3) + 2(e_2 + e_3 + e_4) + \dots \\ &\quad \dots + (e_5 + e_6 + e_7) + 2(e_6 + e_7 + e_8) + (e_9 + e_4 + e_8). \end{aligned}$$

Thus, $e_9 - e_{10} \in \Gamma_3$ and H is not 3-colorable.

Notice that the proof of Theorem 5.4.3 states that if $e_u - e_v \in \Gamma_k$ for some edge $\{u, v\} \in E$, then there exists some degree d such that every solution λ to (DFCOL) (of degree d) satisfies

$$\lambda_0 = \lambda_{e_u - e_v} = \lambda_{2(e_u - e_v)} = \dots = \lambda_{(k-1)(e_u - e_v)}.$$

In such case, we would guarantee the existence of a Nullstellensatz certificate of degree d for (FCOL). For the case of 3-colorability we can find such d using the following lemma:

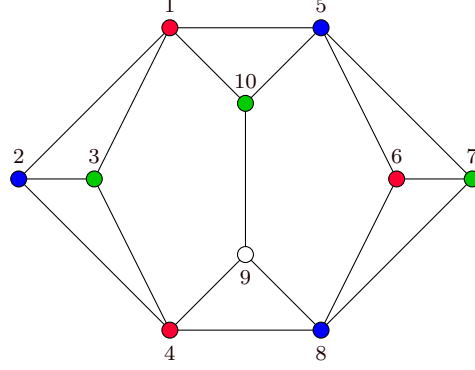


Figure 5.3: The graph H .

Lemma 5.4.5. *Let $G = (V, E)$ be a graph, let $k = 3$ and let λ be a solution to (DFCOL) (of degree d) for some integer $d \geq k$. Suppose that u, v and w are the vertices of a 3-cycle in G and let $\beta \in \{e_u + e_v + e_w, 2e_u + 2e_v + 2e_w\} \subseteq \mathbb{Z}_k^V$. Then,*

$$\lambda_\alpha = \lambda_{\alpha+\beta}$$

for every $\alpha \in \mathbb{Z}_k^V$ such that

1. $|\alpha| \leq d - k$, or
2. $|\alpha| = d$ and $\alpha_u + \alpha_v + \alpha_w \geq 3$, or
3. $|\alpha| = d$, $\{\alpha_u, \alpha_v, \alpha_w\} = \{2, 0, 0\}$ and $\beta = e_u + e_v + e_w$.

Proof. Let α and β be as in the statement, by Corollary 5.2.3 we may assume that d and $|\alpha|$ are congruent with zero modulo $k = 3$. We will prove that system (DFCOL) (of degree d) contains the equations

$$\begin{aligned} \lambda_\alpha &= -\lambda_{\alpha+e_u+2e_v} - \lambda_{\alpha+2e_u+e_v}, \\ &= -\lambda_{\alpha+e_u+2e_w} - \lambda_{\alpha+2e_u+e_w}, \\ &= -\lambda_{\alpha+e_v+2e_w} - \lambda_{\alpha+2e_v+e_w}, \end{aligned} \tag{5.4.2}$$

and

$$\begin{aligned} \lambda_{\alpha+\beta} &= -\lambda_{\alpha+\beta+e_u+2e_v} - \lambda_{\alpha+\beta+2e_u+e_v}, \\ &= -\lambda_{\alpha+\beta+e_u+2e_w} - \lambda_{\alpha+\beta+2e_u+e_w}, \\ &= -\lambda_{\alpha+\beta+e_v+2e_w} - \lambda_{\alpha+\beta+2e_v+e_w}. \end{aligned} \tag{5.4.3}$$

By the way we have chosen β , it is not hard to see that if we sum up the equations in (5.4.2) and (5.4.3), the equation

$$3\lambda_\alpha = 3\lambda_{\alpha+\beta}$$

follows. We consider the three cases separately.

1. Suppose that $|\alpha| \leq d - k$ and $\beta = e_u + e_v + e_w$. Since $|\beta| \leq k$, we have that $|\alpha + \beta| \leq d$. Thus, the equations (5.4.2) and (5.4.3) will appear on (DFCOL) as the edges $\{u, v\}$, $\{u, w\}$ and $\{v, w\}$ are in G .
Now, suppose that $|\alpha| \leq d - k$ and $\beta = 2e_u + 2e_v + 2e_w$. It is not hard to see that for every edge $\{u', v'\} \in \{\{u, v\}, \{u, w\}, \{v, w\}\}$ we have

$$|\alpha + \beta + (e'_u - e'_v)| \leq d.$$

Indeed, this readily follows from the equation $(2, 2, 2) + (1, 2, 0) \equiv (0, 1, 2) \pmod{\mathbb{Z}_3^3}$. In particular, the equation

$$\lambda_{\alpha+\beta+(e'_u-e'_v)} + \lambda_{\alpha+\beta+2(e'_u-e'_v)} + \lambda_{\alpha+\beta} = 0 \quad (5.4.4)$$

appears in (DFCOL) for every such edge $\{u', v'\}$. However, these equations are equivalent to the equations in (5.4.3). Since $|\alpha| \leq d - k$, the equations (5.4.2) appear in (DFCOL) as well and the statement follows.

2. Suppose that $|\alpha| = d$, $\alpha_u + \alpha_v + \alpha_w \geq 3$ and $\beta = e_u + e_v + e_w$. Then,

$$\{\alpha_u, \alpha_v, \alpha_w\} \in \{\{0, 1, 2\}, \{1, 1, 1\}, \{1, 1, 2\}, \{0, 2, 2\}, \{1, 2, 2\}, \{2, 2, 2\}\},$$

and

$$\{\alpha_u + 1, \alpha_v + 1, \alpha_w + 1\} \in \{\{1, 2, 0\}, \{2, 2, 2\}, \{2, 2, 0\}, \{1, 0, 0\}, \{2, 0, 0\}, \{0, 0, 0\}\}.$$

Hence, if $\{\alpha_u, \alpha_v, \alpha_w\} \neq \{1, 1, 1\}$ then $|\alpha + \beta| \leq d$ and the equations (5.4.2) and (5.4.3) will appear on (DFCOL).

Now, suppose that $\{\alpha_u, \alpha_v, \alpha_w\} = \{1, 1, 1\}$. Let $\alpha' := \alpha - \beta$, so that $|\alpha'| \leq d - k$ and by the above case, the equations

$$\lambda_{\alpha'} = \lambda_{\alpha'+\beta} = \lambda_{\alpha'+2\beta}.$$

hold for every solution λ to (DFCOL) (of degree d). In particular, $\lambda_\alpha = \lambda_{\alpha+\beta}$ and this case follows as well.

Finally, suppose that $|\alpha| = d$, $\alpha_u + \alpha_v + \alpha_w \geq 3$ and $\beta = 2e_u + 2e_v + 2e_w$. Then,

$$\{\alpha_u + 2, \alpha_v + 2, \alpha_w + 2\} \in \{\{2, 0, 1\}, \{0, 0, 0\}, \{0, 0, 1\}, \{2, 1, 1\}, \{0, 1, 1\}, \{1, 1, 1\}\}.$$

In particular, $|\alpha + \beta| \leq d$ for every such α . Hence, the equations (5.4.2) and (5.4.3) appear in (DFCOL) (of degree d) and the statement follows.

3. Suppose that $|\alpha| = d$, $\{\alpha_u, \alpha_v, \alpha_w\} = \{2, 0, 0\}$ and $\beta = e_u + e_v + e_w$. Then,

$$\{\alpha_u + 1, \alpha_v + 1, \alpha_w + 1\} = \{1, 1, 0\}.$$

Hence, $|\alpha + \beta| \leq d$ and the equations (5.4.2) and (5.4.3) appear in (DFCOL) (of degree d). Notice that the above is equivalent to case $|\alpha| = d$, $\{\alpha_u, \alpha_v, \alpha_w\} = \{1, 1, 0\}$ and $\beta = 2e_u + 2e_v + 2e_w$.

□

Example 5.4.6. *We can use the above lemma to show that the graph H has a Nullstellensatz Certificate of degree $d := 6$ for (FCOL) with $k = 3$ (see Figure 5.4 for a graphic interpretation of this proof). Thus, let λ be a solution to (DFCOL) of degree 6. Now, the multi-index $e_9 - e_{10}$ has size $d - k$, hence*

$$\lambda_{e_9 - e_{10}} = \lambda_{e_9 - e_{10} + (e_{10} + e_4 + e_8)} = \lambda_{e_9 + e_4 + e_8}.$$

The size of $e_9 + e_4 + e_8$ is $d - k$, hence

$$\lambda_{e_9 + e_4 + e_8} = \lambda_{e_9 + e_4 + e_8 + (2e_2 + 2e_3 + 2e_4)} = \lambda_{e_9 + e_8 + 2e_2 + 2e_3}.$$

The size of $\alpha := e_9 + e_8 + 2e_2 + 2e_3$ is d , however $\alpha_1 + \alpha_2 + \alpha_3 = 4 \geq 3$. Thus,

$$\lambda_{e_9 + e_8 + 2e_2 + 2e_3} = \lambda_{e_9 + e_8 + 2e_2 + 2e_3 + (e_1 + e_2 + e_3)} = \lambda_{e_9 + e_8 + e_1}.$$

The size of $e_9 + e_8 + e_1$ is $d - k$, hence

$$\lambda_{e_9 + e_8 + e_1} = \lambda_{e_9 + e_8 + e_1 + (2e_6 + 2e_7 + 2e_8)} = \lambda_{e_9 + e_1 + 2e_6 + 2e_7}.$$

Once again, the size of $\alpha := e_9 + e_1 + 2e_6 + 2e_7$ with $\alpha_5 + \alpha_6 + \alpha_7 = 4 \geq 3$. Thus,

$$\lambda_{e_9 + e_1 + 2e_6 + 2e_7} = \lambda_{e_9 + e_1 + 2e_6 + 2e_7 + (e_5 + e_6 + e_7)} = \lambda_{e_1 + e_5 + e_9}.$$

Finally, the multi-index $e_1 + e_5 + e_9$ has size $d - k$ and as a consequence

$$\lambda_{e_1 + e_5 + e_9} = \lambda_{e_1 + e_5 + e_9 + 2(e_1 + e_5 + e_9)} = \lambda_0.$$

The above proves that $\lambda_{e_9 - e_{10}} = \lambda_0$. Similarly, one can prove that $\lambda_{-e_9 + e_{10}} = \lambda_0$ and the proof follows.

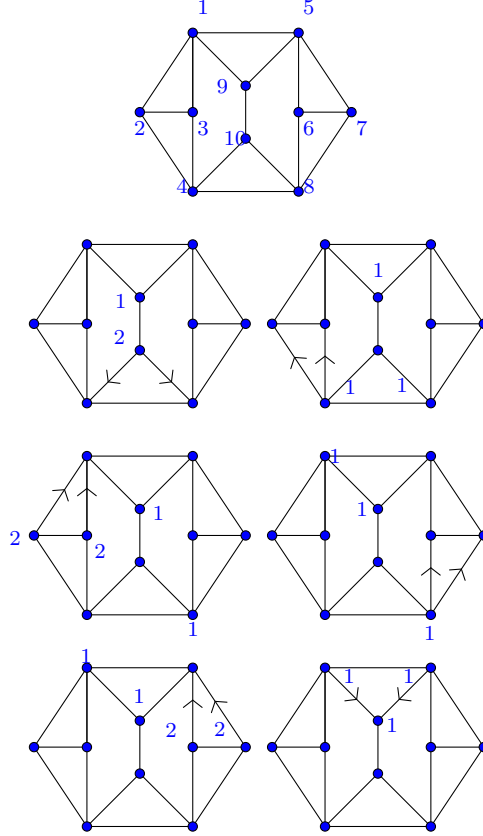


Figure 5.4: H has a degree six Nullstellensatz Certificate for (FCOL). Each labelled graph represents a multi-index (except for the first one).

Proposition 5.4.7 (Odd Wheels). *Let $n \geq 3$ be an odd integer and let W_n be the wheel on $n + 1$ vertices i.e., the graph with vertex set $V(W_n) = \{0, 1, \dots, n - 1, v\}$ and edge set $E(W_n) = \{\{i, i + 1\} : i \in \mathbb{Z}_n\} \cup \{\{i, v\} : i \in \mathbb{Z}_n\}$. Then, W_n has a Nullstellensatz Certificate of degree $d := 3$ for (FCOL) with $k = 3$.*

Proof. Let λ be a solution to (DFCOL) (of degree 3). We will prove by induction that the equations

$$\lambda_0 = \lambda_{e_0 - e_i} = \lambda_{e_{n-1} - e_{n-1-i}}$$

hold for every $i \in \{0, 2, 4, \dots, n - 1\}$. In particular, since the edge $\{0, n - 1\}$ is in $E(W_n)$ and the equations

$$\lambda_0 = \lambda_{e_0 - e_{n-1}} = \lambda_{e_{n-1} - e_0}$$

hold, the statement follows.

The base case $i = 0$ is trivial. Thus, assume that the statement holds for $i - 2 \leq n - 3$ and let us prove it for i even. Notice that the sets of vertices $\{i - 2, i - 1, v\}$, $\{i - 1, i, v\}$ and $\{n - i + 1, n - i, v\}$, $\{n - i, n - 1 - i, v\}$ form 3-cycles in G . Thus, by Lemma 5.4.5, we have that

$$\begin{aligned}\lambda_{e_0 - e_i} &= \lambda_{e_0 - e_i + (e_{i-1} + e_i + e_v)} = \lambda_{e_0 + e_{i-1} + e_v}, \\ &= \lambda_{e_0 + e_{i-1} + e_v + 2(e_{i-1} + e_{i-2} + e_v)} = \lambda_{e_0 - e_{i-2}} \\ &= \lambda_0.\end{aligned}$$

Similarly,

$$\begin{aligned}\lambda_{e_{n-1} - e_{n-1-i}} &= \lambda_{e_{n-1} - e_{n-1-i} + (e_{n-1-i} + e_{n-i} + e_v)}, \\ &= \lambda_{e_{n-1} + e_{n-i} + e_v} = \lambda_{e_{n-1} + e_{n-i} + e_v + 2(e_{n-i} + e_{n-i+1} + e_v)}, \\ &= \lambda_{e_{n-1} - e_{n-1-(i-2)}} = \lambda_0.\end{aligned}$$

The claim follows. □

The following corollary follows immediately.

Corollary 5.4.8 (De Loera et al. [17]). *Let $n \geq 3$ be an odd integer and let W_n be the wheel on $n + 1$ vertices. Then, W_n has a Nullstellensatz Certificate of degree $d = 4$ for (BCOL) with $k = 3$.*

Remark 5.4.9. *We must point out that the proof in [17] of the above corollary uses different techniques. De Loera et al. [19] also proved that W_n has a Nullstellensatz Certificate of degree one for (BCOL) over the field \mathbb{F}_2 .*

Chapter 6

Final Remarks and Future Work

In this dissertation we gave a concrete study of the applications of Hilbert's Nullstellensatz to some combinatorial problems such as the *Maximum Stable Set Problem* and *Graph Colorability Problems*. We have seen that, through the lenses of *duality*, it is possible to obtain a much better understanding of the Nullstellensatz Certificates and the theory behind them. In particular, when a system of polynomial equations is *sparse*, the *annihilators* of the system are useful if one wants to determine both upper and lower bounds for the degrees of Nullstellensatz Certificates.

We have introduced new techniques and given new proofs to most of the results known in the literature. In particular, the results in Section 5.3 shine a new light to the *Nullstellensatz Paradigm* for Graph Colorability: we have stated a possible structural property a graph must satisfy in order to have no small degree Nullstellensatz certificates. Although our results seem to be far from being optimal, we believe that this is the right path to obtain the so desired family of non- k -colorable graphs with minimal Nullstellensatz Certificates of large degree.

There are several questions that remain open.

1. Probably the most important open problem is the following:

Problem 6.0.1. *For given integers $k \geq 3$ and $d \geq k$, characterize all non- k -colorable graphs with minimal Nullstellensatz Certificates for (BCOL) (or (FCOL)) of degree d .*

Moreover, we would like to solve the following problem.

Problem 6.0.2. Find a non-3-colorable graph whose minimal Nullstellensatz Certificate for (BCOL) has degree greater than four.

We believe that any non-3-colorable graph of girth at least eight should suffice.

2. In Section 5.2.1 we used basic group theory to determine the degree of a minimal Nullstellensatz Certificate for (FCOL) to prove the non-3-colorability and non-4-colorability of the complete graphs K_4 and K_5 respectively. Using computing software, we could determine the degree of a minimal Nullstellensatz Certificate for the non-5-colorability of K_6 . However, we could not find a short proof of such finding. We would like to solve the following problem.

Problem 6.0.3. For every integer $k \geq 6$, find the degree of a minimal Nullstellensatz Certificate for (FCOL) to prove the non- k -colorability of K_{k+1} .

We believe that such degree should be $2k$ (for (FCOL)).

3. Let $G = (V, E)$ be a graph and an let $k \geq 2$ be an integer. Consider the functions $g_{uv} \in L^2(\mathbb{Z}_k^V)$ with $\{u, v\} \in E$ defined as in Section 5, i.e.

$$g_{uv}(\alpha) := \begin{cases} 1, & \text{if } \alpha_u = \alpha_v, \\ 0, & \text{otherwise.} \end{cases}$$

Then, G is not- k -colorable if and only if the function

$$h_{G,k} := \sum_{\{u,v\} \in E} g_{uv} - 1$$

is non-negative. In particular, if G is not k -colorable, then there exist functions $r_1, r_2, \dots, r_m \in L^2(\mathbb{Z}_k^V)$ such that

$$h_{G,k} = r_1^2 + r_2^2 + \dots + r_m^2. \tag{6.0.1}$$

Thus the functions r_1, \dots, r_m provide a *Sums of Squares (SOS) Certificate* for the non- k -colorability of G .

Problem 6.0.4. Given a non- k -colorable graph G , find SOS certificates r_1, \dots, r_m with the sparsest Fourier support.

The above problem is closely related to the recent work of Hamza Fawzi, Pablo Parrilo and James Saunderson ([25]). We believe this problem can be attacked using their techniques. It would be interesting to see if these certificates share some relation with the Nullstellensatz Certificates (e.g. Theorem 5.2.11).

4. Let $G = (V, E)$ be a non- k -colorable graph and let $A_d \mathbf{z}_d = b_d$ be the *Nullstellensatz Linear System* (NLS) of degree $d \geq 0$ for (FCOL). That is, the linear system derived from the equation

$$\sum_{u \in V} s_u(x) p_u(x) + \sum_{\{u,v\} \in E} r_{uv}(x) q_{uv}(x) = 1,$$

where the polynomials s_u and r_{uv} have degree at most d and the polynomials p_u and q_{uv} are as in the definition of (FCOL). If G has a minimal Nullstellensatz Certificate of degree d^* for (FCOL), then the support of a (sparse) solution $\mathbf{z}_{d^*}^*$ to the (NLS) of degree d^* defines a (small) sub-matrix B_{d^*} of A_{d^*} which encodes the non- k -colorability of G . For instance, in Example 5.1.6 and Theorem 5.1.7 we saw that for the 2-colorability of non-bipartite graphs, the (NLS) contained a much smaller sub-system encoding an odd cycle in the graph. In particular, this sub-matrix encoded a well known structural theorem for the 2-colorability of graphs.

Conversely, given a structural theorem characterizing the non- k -colorability of G , there should exist a corresponding sub-matrix B_d or sub-system derived from A_d for some $d \geq d^*$ exposing such structure (e.g. Lemma 5.4.1). However, we do not have concrete results linking structures that certify the non- k -colorability of G and the sub-matrices or sub-systems derived from A_d . Such results should be helpful as one might use well known theorems in graph theory to deduce properties of the (NLS). For instance, Maria Chudnovsky, Alex Scott and Paul Seymour recently proved a series of beautiful results relating the chromatic number of a graph and the existence of *holes* (i.e. an induced cycle of length at least four) of prescribed length.

Theorem 6.0.1 (Scott, Seymour [54]). *Let G be a graph with no odd holes. Then,*

$$\chi(G) \leq 2^{2^{\omega(G)}},$$

where $\omega(G)$ is the size of the maximum clique of G .

Theorem 6.0.2 (Chudnovsky, Scott, Seymour [11]). *Let G be a graph with no holes of length $\geq \ell$. Then,*

$$\chi(G) \leq \phi(\ell, \omega(G)),$$

for some constant $\phi(\ell, \omega(G))$.

In particular, if a graph G is not $\phi(\ell, \omega(G))$ -colorable, then G must have a hole of length at least ℓ . Such a hole should be implicit in some sub-system derived from A_d and hence, it is important to study the structure of matrices A_d in the presence (or absence) of even and odd holes.

References

- [1] Noga Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8(1-2):7–29, 1999. Recent trends in combinatorics (Mátraháza, 1995).
- [2] K. Appel and W. Haken. Every planar map is four colorable. I. Discharging. *Illinois J. Math.*, 21(3):429–490, 1977.
- [3] K. Appel, W. Haken, and J. Koch. Every planar map is four colorable. II. Reducibility. *Illinois J. Math.*, 21(3):491–567, 1977.
- [4] Enrique Arrondo. Another elementary proof of the Nullstellensatz. *Amer. Math. Monthly*, 113(2):169–171, 2006.
- [5] David Allen Bayer. *The Division Algorithm and the Hilbert Scheme*. ProQuest LLC, Ann Arbor, MI, 1982. Thesis (Ph.D.)—Harvard University.
- [6] Paul Beame, Stephen Cook, Jeff Edmonds, Russell Impagliazzo, and Toniann Pitassi. The relative complexity of NP search problems. *J. Comput. System Sci.*, 57(1):3–19, 1998. 27th Annual ACM Symposium on the Theory of Computing (STOC’95) (Las Vegas, NV).
- [7] J. A. Bondy and U. S. R. Murty. *Graph theory*, volume 244 of *Graduate Texts in Mathematics*. Springer, New York, 2008.
- [8] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Ann. of Math. (2)*, 126(3):577–591, 1987.
- [9] Samuel R. Buss. Lower bounds on Nullstellensatz proofs via designs. In *Proof complexity and feasible arithmetics (Rutgers, NJ, 1996)*, volume 39 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 59–71. Amer. Math. Soc., Providence, RI, 1998.

- [10] Samuel R. Buss and Toniann Pitassi. Good degree bounds on Nullstellensatz refutations of the induction principle. *J. Comput. System Sci.*, 57(2):162–171, 1998. Complexity 96—The Eleventh Annual IEEE Conference on Computational Complexity (Philadelphia, PA).
- [11] M. Chudnovsky, A. Scott, and P. Seymour. Induced subgraphs of graphs with large chromatic number. III. Long holes. *ArXiv e-prints*, June 2015.
- [12] Maria Chudnovsky, Alex Scott, and Paul Seymour. Induced subgraphs of graphs with large chromatic number. II. Three steps towards Gyárfás’ conjectures. *J. Combin. Theory Ser. B*, 118:109–128, 2016.
- [13] V. Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Math.*, 4:305–337, 1973.
- [14] David Cox, John Little, and Donal O’Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.
- [15] David A. Cox, John Little, and Donal O’Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.
- [16] J. A. De Loera, J. Lee, S. Margulies, and J. Miller. Weak orientability of matroids and polynomial equations. *European J. Combin.*, 50:56–71, 2015.
- [17] J. A. De Loera, J. Lee, S. Margulies, and S. Onn. Expressing combinatorial problems by systems of polynomial equations and Hilbert’s Nullstellensatz. *Combin. Probab. Comput.*, 18(4):551–582, 2009.
- [18] J. A. De Loera, S. Margulies, M. Pernpeintner, E. Riedl, D. Rolnick, G. Spencer, D. Stasi, and J. Swenson. Grobner Bases and Nullstellensätze for Graph-Coloring Ideals. *ArXiv e-prints*, October 2014.
- [19] Jesús A. De Loera, Christopher J. Hillar, Peter N. Malkin, and Mohamed Omar. Recognizing graph theoretic properties with polynomial ideals. *Electron. J. Combin.*, 17(1):Research Paper 114, 26, 2010.
- [20] Jesús A. De Loera, Jon Lee, Peter N. Malkin, and Susan Margulies. Hilbert’s Nullstellensatz and an algorithm for proving combinatorial infeasibility. In *ISSAC 2008*, pages 197–206. ACM, New York, 2008.

- [21] Jesús A. De Loera, Jon Lee, Peter N. Malkin, and Susan Margulies. Computing infeasibility certificates for combinatorial problems through Hilbert’s Nullstellensatz. *J. Symbolic Comput.*, 46(11):1260–1283, 2011.
- [22] Jesus A De Loera, Peter N Malkin, and Pablo A Parrilo. Computation with polynomial equations and inequalities arising in combinatorial optimization. In *Mixed Integer Nonlinear Programming*, pages 447–481. Springer, 2012.
- [23] Jack Edmonds. Minimum partition of a matroid into independent subsets. *J. Res. Nat. Bur. Standards Sect. B*, 69B:67–72, 1965.
- [24] P. Erdős. Graph theory and probability. *Canad. J. Math.*, 11:34–38, 1959.
- [25] H. Fawzi, J. Saunderson, and P. A. Parrilo. Sparse sum-of-squares certificates on finite abelian groups. *ArXiv e-prints*, March 2015.
- [26] M. R. Garey, D. S. Johnson, and L. Stockmeyer. Some simplified NP-complete graph problems. *Theoret. Comput. Sci.*, 1(3):237–267, 1976.
- [27] Edinah K Gngang. Computational aspects of the combinatorial nullstellensatz method. *arXiv preprint arXiv:1402.6920*, 2014.
- [28] Chris Godsil and Gordon Royle. *Algebraic Graph Theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.
- [29] Bruno Grenet, Pascal Koiran, and Natacha Portier. The multivariate resultant is NP-hard in any characteristic. In *Mathematical foundations of computer science 2010*, volume 6281 of *Lecture Notes in Comput. Sci.*, pages 477–488. Springer, Berlin, 2010.
- [30] Peter Heinig. Proof of the combinatorial Nullstellensatz over integral domains, in the spirit of Kouba. *Electron. J. Combin.*, 17(1):Note 14, 5, 2010.
- [31] David Hilbert. Ueber die vollen Invariantensysteme. *Math. Ann.*, 42(3):313–373, 1893.
- [32] David Hilbert. *Hilbert’s invariant theory papers*. Lie Groups: History, Frontiers and Applications, VIII. Math Sci Press, Brookline, Mass., 1978. Translated from the German by Michael Ackerman, With comments by Robert Hermann.
- [33] Richard M. Karp. Reducibility among combinatorial problems. In *Complexity of computer computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y., 1972)*, pages 85–103. Plenum, New York, 1972.

- [34] János Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.
- [35] Omran Kouba. A duality based proof of the combinatorial Nullstellensatz. *Electron. J. Combin.*, 16(1):Note 9, 3, 2009.
- [36] Michał Lasoń. A generalization of combinatorial Nullstellensatz. *Electron. J. Combin.*, 17(1):Note 32, 6, 2010.
- [37] Daniel Lazard. Algèbre linéaire sur $K[X_1, \dots, X_n]$, et élimination. *Bull. Soc. Math. France*, 105(2):165–190, 1977.
- [38] David W. Lewis. David Hilbert and the theory of algebraic invariants. *Irish Math. Soc. Bull.*, (33):42–54, 1994.
- [39] B. Li, B. Lowenstein, and M. Omar. Low degree Nullstellensatz certificates for 3-colorability. *ArXiv e-prints*, March 2015.
- [40] L. Lovász. On chromatic number of finite set-systems. *Acta Math. Acad. Sci. Hungar.*, 19:59–67, 1968.
- [41] L. Lovász. Kneser’s conjecture, chromatic number, and homotopy. *J. Combin. Theory Ser. A*, 25(3):319–324, 1978.
- [42] L. Lovász. Stable sets and polynomials. *Discrete Math.*, 124(1-3):137–153, 1994. Graphs and combinatorics (Qawra, 1990).
- [43] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.
- [44] S. Margulies and I. V. Hicks. An algebraic exploration of dominating sets and Vizing’s conjecture. *Electron. J. Combin.*, 19(2):Paper 1, 30, 2012.
- [45] S. Margulies, S. Onn, and D. V. Pasechnik. On the complexity of Hilbert refutations for partition. *J. Symbolic Comput.*, 66:70–83, 2015.
- [46] J. Mycielski. Sur le coloriage des graphs. *Colloq. Math.*, 3:161–162, 1955.
- [47] Jorge Nocedal and Stephen J. Wright. *Numerical Optimization*. Springer Series in Operations Research. Springer-Verlag, New York, 1999.

- [48] Stephen Prajna, Antonis Papachristodoulou, Peter Seiler, and Pablo A Parrilo. New developments in sum of squares optimization and sostools. In *Proceedings of the American Control Conference*, pages 5606–5611, 2004.
- [49] Bruce Reznick. Extremal PSD forms with few terms. *Duke Math. J.*, 45(2):363–374, 1978.
- [50] Neil Robertson, Daniel Sanders, Paul Seymour, and Robin Thomas. The four-colour theorem. *J. Combin. Theory Ser. B*, 70(1):2–44, 1997.
- [51] Neil Robertson, Daniel P. Sanders, Paul Seymour, and Robin Thomas. Efficiently four-coloring planar graphs. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 571–575. ACM, New York, 1996.
- [52] Neil Robertson, Daniel P. Sanders, Paul Seymour, and Robin Thomas. A new proof of the four-colour theorem. *Electron. Res. Announc. Amer. Math. Soc.*, 2(1):17–25, 1996.
- [53] Alexander Schrijver. *Theory of Linear and Integer Programming*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons, Ltd., Chichester, 1986. A Wiley-Interscience Publication.
- [54] Alex Scott and Paul Seymour. Induced subgraphs of graphs with large chromatic number. i. odd holes. *Journal of Combinatorial Theory, Series B*, pages –, 2015.
- [55] Terence Tao. Hilbert’s nullstellensatz. <https://terrytao.wordpress.com/2007/11/26/hilberts-nullstellensatz/>, 2007.
- [56] Audrey Terras. *Fourier Analysis on Finite Groups and Applications*, volume 43 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.