Combinatorial Nullstellensatz: Various Proofs, Extensions and Applications

by

Yulia Alexandr
Class of 2019

A thesis submitted to the
faculty of Wesleyan University
in partial fulfillment of the requirements for the
Degree of Bachelor of Arts
with Departmental Honors in Mathematics

"Нельзя быть математиком, не будучи в то же время и поэтом в душе."

– Софья Ковалевская

"It is impossible to be a mathematician without being a poet in soul."

– Sophia Kovalevskaya [1]

[1] Russian mathematician; the first woman to obtain a doctorate degree in mathematics.

Abstract

The Combinatorial Nullstellensatz is an algebraic technique first introduced by Noga Alon [2] in 1999. Being closely related to the famous Hilbert's Nullstellensatz, it has extensive applications in combinatorics and number theory where various results are obtained by analyzing roots of well-chosen polynomials. In this thesis, we present the two main theorems associated with the Combinatorial Nullstellensatz along with their original proofs. Moreover, we give attention to alternative proofs and extensions of these theorems that were introduced in later papers by other researchers as well as discuss several existing applications, focusing our attention on those in graph theory. Using the Combinatorial Nullstellensatz, we give a necessary and sufficient condition for an m-uniform hypergraph to be k-colorable, thus generalizing one of Alon's results. We also introduce a fun application of the Combinatorial Nullstellensatz in determining the existence of solutions to the well-known Sudoku Puzzle.

Acknowledgments

First and foremost, I would like to thank my amazing mentor, Professor Karen Collins, for her extensive guidance and support throughout my time at Wesleyan. I am thankful to her for suggesting this thesis topic and always being extremely helpful when I had questions. Working under her supervision has strengthened my interest in graph theory and algebraic combinatorics and convinced me to pursue a research career in these areas. I am also thankful to Professors David Constantine and Daniel Krizanc for the many helpful comments on the manuscript.

I also want to express my sincere gratitude to Professor Cameron Donnay Hill for always being so supportive, caring, and confident in my mathematical abilities. He has sparked my interest in algebra, without which this thesis wouldn't be possible. I am also grateful to Professor Han Li for teaching me to appreciate the power of mathematical analysis, pushing me to succeed and always do my best. I would also like to thank Professors David Constantine, Constance Leidy, and James Lipton for the wonderful classes I took with them during my time at Wesleyan.

I would like to thank Professor Ayalur Krishnan for encouraging me to explore the beauty of mathematics as a college freshman, helping me along my path and being a wonderful friend and mentor. I would have never transferred to Wesleyan and devoted myself to mathematics if it weren't for him. Finally, I would like to thank my friends and colleagues π, Maksim, Joomy, Joe, Alex, and Rocco for their emotional support. Most importantly, I wish to thank my family for making all my achievements possible.

Contents

1 Introduction

The Hilbert's Nullstellensatz is an important theorem in algebraic geometry which asserts the following:

(Hilbert's Nullstellenstaz, [9]) *Let $\mathbb{F}$ be an algebraically closed field and I be an ideal in the polynomial ring $\mathbb{F}[x_1, \cdots, x_n]$. If $f \in \mathbb{F}[x_1, \cdots, x_n]$ is a polynomial that vanishes over all common roots of the elements in I, then $f^k \in I$ for some positive integer k.*

The proof of the above theorem can be found in [3]. It is clear that if the ideal I above is radical, we get that $f \in I$. (Refer to Section 3.1 for the definition of a radical ideal). The Combinatorial Nullstellensatz I is the theorem that is obtained by taking I to be the ideal finitely generated by some special univariate polynomials $g_1(x_1), \cdots, g_n(x_n)$ in the ring $\mathbb{F}[x_1, \cdots, x_n]$, in which case the requirement that $\mathbb{F}$ is algebraically closed may be relaxed to obtain the same conclusion. Moreover, the alternative proof given by Vishnoi [14], which we present in Section 3.1, demonstrates that in that special case, $I = \langle g_1(x_1), \cdots, g_n(x_n) \rangle$ is a radical ideal, and by the remark above we are able to conclude that $f \in I$. The Combinatorial Nullstellensatz I finds many application in graph theory, especially in graph coloring where f is often taken to be the graph polynomial (Section 4.2). Furthermore, the theorem is applicable in hypergraph coloring. One of the interesting applications of the Combinatorial Nullstellensatz I given by Alon is that it gives a necessary and sufficient condition for a 3-uniform hypergraph to be 2-colorable. We generalize his result to arbitrary m-uniform hypergraphs and arbitrary k colors in Section 4.2. The theorem may also be used in determining

the existence of solutions to a given Sudoku Puzzle, when we view the puzzle as a partially colored graph. We introduce this application in Section 4.3.

The Combinatorial Nullstellensatz II is the theorem that was originally proven to be a consequence of the Combinatorial Nullstellensatz I which asserts that for any field $\mathbb{F}$ and a polynomial $f \in \mathbb{F}[x_1, \cdots, x_n]$ satisfying certain conditions, there is a tuple $(a_1, \cdots, a_n)$ in a subset of $\mathbb{F}^n$ on which f doesn't vanish. This theorem has numerous applications in number theory, linear algebra, graph theory and other areas, and we discuss some of them here.

A shorter proof of the Combinatorial Nullstellensatz II that is independent of the Combinatorial Nullstellensatz I was given by Michałek [13] in 2010, which we present in Section 3.2. It has led to a discovery of a more general version of the theorem by Łason [12], in which the requirement that the polynomial f must be of a particular degree may be relaxed (Section 3.3). We present an application of this generalized theorem in Section 4.6.

Throughout this work, let $[n]$ denote the set $\{1, \cdots, n\}$ for every natural number n. We presuppose the reader is familiar with basic concepts in commutative algebra and graph theory. We also follow the terminology of [3] and [15] for the concepts not explicitly defined in this paper.

2 Combinatorial Nullstellensatz: Main Theorems

In this section, we will state and present the original proofs of the two main theorems associated with the Combinatorial Nullstellensatz. Before we do so, we

need the following lemma.

Lemma 1. [2] Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x_1, \cdots, x_n]$ be a polynomial of degree at most t_i in the variable x_i for each $i \in [n]$. Also, for each such i, let $A_i \subseteq \mathbb{F}$ be a set of distinct members of $\mathbb{F}$ such that $|A_i| \geq t_i + 1$. If $f(a_1, \cdots, a_n) = 0$ for all $(a_1, \cdots, a_n) \in A_1 \times \cdots \times A_n$, then f is the zero polynomial.

Proof. We prove the claim by induction. For the base case, let $n = 1$. Then f is a polynomial in one variable x of degree at most t. Let $A \subseteq \mathbb{F}$ such that $|A| \geq t + 1$. If f is not the zero polynomial, it has at most t roots. But we know that f vanishes at all elements of A, so it has to be the zero polynomial.

Now assume that the lemma holds for the polynomials in $n - 1$ variables. Let $f = f(x_1, \cdots, x_n)$ and let $A_i \subseteq \mathbb{F}$ be a set of distinct members of $\mathbb{F}$ such that $|A_i| \geq t_i + 1$ for all $i \in [n]$. Note that we can re-write f as follows:

$$f = \sum_{i=0}^{t_n} g_i(x_1, \cdots, x_{n-1}) x_n^i$$

where each g_i is a polynomial with degree at most t_i in each variable x_i, by the hypothesis. Let $(a_1, \cdots, a_{n-1}) \in A_1 \times \cdots \times A_{n-1}$ be arbitrary. Consider the polynomial $f(a_1, \cdots, a_{n-1}, x_n)$, which is a polynomial in one variable x_n. We know that f vanishes for all specified n-tuples, so $f(a_1, \cdots, a_{n-1}, a_n) = 0$ for all $a_n \in A_n$. Since $|A_n| \geq t_n + 1$ and $\deg_{x_n}(f) = t_n$, we have that $f(a_1, \cdots, a_{n-1}, x_n) \equiv 0$, just as in the base case. From the way, we re-wrote f above, it follows that $g_i(a_1, \cdots, a_{n-1}) = 0$ for all $i \in \{0\} \cup [t_n]$. Since $(a_1, \cdots, a_{n-1})$ was arbitrary, each g_i vanishes at all elements of $A_1 \times \cdots \times A_{n-1}$. By the inductive hypothesis, g_i is the zero polynomial for all i. It immediately follows that f is the zero polynomial. $\square$

2.1 Combinatorial Nullstellensatz I

Theorem 1 (Combinatorial Nullstellensatz I)**.** [2] Let $\mathbb{F}$ be a field and let $f = f(x_1, \cdots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \cdots, x_n]$. Let $A_1, \cdots, A_n$ be finite non-empty subsets of $\mathbb{F}$ and define $g_i(x_i) = \prod_{a \in A_i}(x_i - a)$ (note g_i is a polynomial in one variable). If $f(a_1, \cdots, a_n) = 0$ for all $a_i \in A_i$ (i.e. if f vanishes at all common zeros of $g_1, \cdots, g_n$), then there are polynomials $h_1, \cdots, h_n \in \mathbb{F}[x_1, \cdots, x_n]$ satisfying $\deg(h_i) \leq \deg(f) - \deg(g_i)$ such that:

$$f = \sum_{i=1}^{n} h_i g_i.$$

Proof. Let $t_i = |A_i| - 1$ for each $i \in [n]$. Note that each g_i can be re-written as:

$$g_i(x_i) = \prod_{a \in A_i}(x_i - a) = x_i^{|A_i|} - \sum_{j=0}^{t_i} g_{i,j} x_i^j = x_i^{t_i+1} - \sum_{j=0}^{t_i} g_{i,j} x_i^j \tag{1}$$

where $g_{i,j}$ are the appropriate coefficients. Consider the following relation:

$$x_i^{t_i+1} = \sum_{j=0}^{t_i} g_{i,j} x_i^j. \tag{2}$$

We can see that the relation holds when evaluated at any $a_i \in A_i$ by noting that $g_i(a_i) = 0$ and applying (1). Now, we will construct the polynomial $\hat{f}$ as follows: we start with the polynomial f and for all $i \in [n]$ repeatedly replace each term of the form $x_i^{d_i}$ where $d_i > t_i$ by a linear combination of smaller powers in x_i using the relation in (2). Below we demonstrate how to do it for the first 3 terms. The terms in dark red are the terms that are in f but are left out when constructing $\hat{f}$. The terms in black on the right-hand side are the terms that are in $\hat{f}$.

$$
\begin{aligned}
x_i^{t_i+1} &= g_i(x_i) + \sum_{j=0}^{t_i} g_{i,j} x_i^j \\
x_i^{t_i+2} &= g_i(x_i)x_i + \sum_{j=0}^{t_i} g_{i,j} x_i^{j+1} \\
&= g_i(x_i)x_i + g_{i,t_i} x_i^{t_i+1} + \sum_{j=0}^{t_i-1} g_{i,j} x_i^{j+1} \\
&= g_i(x_i)x_i + g_{i,t_i} g_i(x_i) + g_{i,t_i} \sum_{j=0}^{t_i} g_{i,j} x_i^j + \sum_{j=1}^{t_i} g_{i,j-1} x_i^j \\
&= g_i(x_i)\big(x_i + g_{i,t_i}\big) + g_{i,t_i} \sum_{j=0}^{t_i} g_{i,j} x_i^j + \sum_{j=0}^{t_i} h_{i,j} x_i^j && (*) \\
&= g_i(x_i)\big(\underbrace{x_i + g_{i,t_i}}_{h_i}\big) + \sum_{j=0}^{t_i} q_{i,j} x_i^j && (**)
\end{aligned}
$$

where in (*) we define $h_{i,0} = 0$ and for all $j > 0$ we define $h_{i,j} = g_{i,j-1}$. In (**) we define $q_{i,j} = g_{i,t_i} g_{i,j} + h_{i,j}$. Similarly, observe:

$$
\begin{aligned}
x_i^{t_i+3} &= g_i(x_i)\big(x_i + g_{i,t_i}\big)x_i + \sum_{j=0}^{t_i} q_{i,j} x_i^{j+1} \\
&= g_i(x_i)\big(x_i^2 + g_{i,t_i+1} x_i\big) + q_{i,t_i} x_i^{t_i+1} + \sum_{j=0}^{t_i-1} q_{i,j} x_i^{j+1} \\
&= g_i(x_i)\big(x_i^2 + g_{i,t_i+1} x_i\big) + q_{i,t_i} g_i(x_i) + q_{i,t_i} \sum_{j=0}^{t_i} g_{i,j} x_i^j + \sum_{j=0}^{t_i} p_{i,j} x_i^j && (*) \\
&= g_i(x_i)\big(\underbrace{x_i^2 + g_{i,t_i} x_i + q_{i,t_i}}_{h_i}\big) + \sum_{j=0}^{t_i} r_{i,j} x_i^j && (**)
\end{aligned}
$$

where we let where in (*) we define $p_{i,0} = 0$ and for all $j > 0$ we define $p_{i,j} = q_{i,j-1}$. In (**) we define $r_{i,j} = q_{i,t_i} g_{i,j} + p_{i,j}$. The above computation may be generalized to an arbitrary $d_i > t_i$ by induction by combining sums in this manner. We

can see that each of the dark red terms will always have a multiple of $g_i(x_i)$ by construction. So, we can now see that the polynomial $\hat{f}$ is obtained from f by subtracting terms of the form $h_i g_i$ for each $i \in [n]$, where h_i is a polynomial in $\mathbb{F}[x_1, \cdots, x_n]$. Stated differently, we have that:

$$f = \hat{f} + \sum_{i=1}^{n} h_i g_i.$$

By a previous remark, the relation (2) holds true for all elements in $A_1 \times \cdots \times A_n$, so $\hat{f}(a_1, \cdots, a_n) = f(a_1, \cdots, a_n)$ for all $(a_1, \cdots, a_n) \in A_1 \times \cdots \times A_n$. Since f vanishes at all these tuples by assumption, so does $\hat{f}$. But since we also have that $\hat{f}$ is of degree at most t_i in each variable x_i for all $i \in [n]$, applying Lemma 1, we conclude that $\hat{f}$ is the zero polynomial. So,

$$f = \sum_{i=1}^{n} h_i g_i$$

as desired. Moreover, it is also clear that for each $i \in [n]$:

$$\deg(f) \geq \deg(h_i g_i) = \deg(h_i) + \deg(g_i)$$

since $\mathbb{F}$ is a field, and thus an integral domain. So we also get that $\deg(h_i) \leq \deg(f) - \deg(g_i)$, and this concludes the proof. □

2.2 Combinatorial Nullstellensatz II

Theorem 2 (Combinatorial Nullstellensatz II)**.** [2] Let $\mathbb{F}$ be a field and $f = f(x_1, \cdots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \cdots, x_n]$. For each $i \in [n]$, let t_i be a non-negative integer, and suppose $\deg(f) = \sum_{i=1}^{n} t_i$. Also, suppose that the coefficient

of $\prod_{i=1}^{n} x_i^{t_i}$ in f is non-zero. Then, for all subsets $A_i \subseteq F$ such that $|A_i| > t_i$, $i \in [n]$, there are $a_1 \in A_1, \cdots, a_n \in A_n$ such that $f(a_1, \cdots, a_n) \neq 0$.

Proof. Note that we may assume that $|A_i| = t_i + 1$ for all $i \in [n]$, since if the cardinality of A_i is greater, the result will follow as well. Suppose, toward a contradiction, that the theorem is false, so f vanishes at all elements of $A_1 \times \cdots \times A_n$. Define $g_i(x_i) = \prod_{a \in A_i}(x_i - a)$. By Theorem 1, since f vanishes at all common zeros of $g_1, \cdots, g_n$, by assumption, we get polynimoals $h_1, \cdots, h_n \in F[x_1, \cdots, x_n]$ satisfying $\deg(h_j) \leq \deg(f) - \deg(g_j) = \sum_{i=1}^{n} t_i - \deg(g_j)$, such that

$$f = \sum_{i=1}^{n} h_i g_i. \tag{3}$$

Now note that, by the hypothesis, the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is non-zero, so it has to be non-zero in $\sum_{i=1}^{n} h_i g_i$. However,

$$\deg(h_i g_i) = \deg\left(h_i \prod_{a \in A_i}(x_i - a)\right) = \deg(h_i) + \deg(g_i) \leq \deg(f).$$

This means that $\deg(f)$ is a maximum degree of each of the terms in the sum on the right-hand side of (3). Each term of degree $\deg(f)$ in the sum in (3) looks like $y \cdot x_i^{t_i+1}$ for some y that is a highest-power term in h_i for some i. Hence each term of degree $\deg(f)$ is divisible by $x_i^{t_i+1}$ for some $i \in [n]$. But $\prod_{i=1}^{n} x_i^{t_i}$ is of degree $\deg(f)$ and has a non-zero coefficient in f, by assumption. It is, however, not divisible by $x_i^{t_i+1}$ for any i. This is a contradiction to the equality in (3). $\square$

3 Alternative Proofs and Extensions

The proofs presented in the previous section are the original proofs suggested by Alon [2]. Because of the usefulness of the Combinatorial Nullstellensatz, alternative proofs of the above theorems were soon introduced by other researchers. We present these proofs in this section.

3.1 Algebraic Proof of the Combinatorial Nullstellensatz I

The purely algebraic proof of Theorem 1, which uses basic facts from commutative algebra, was first introduced by N. Vishnoi [14]. We present his proof here filling in all the details left to the reader in the original paper. Before proceeding with the proof, let us state several preliminary algebraic definitions.

Let R be a commutative ring with identity. An *ideal* I of R is a subset of R satisfying two properties:

1. I is a subgroup of R under the operation of addition;
2. for all $x \in I$ and $r \in R$, $xr \in I$.

We say that an ideal M or R is *maximal* if $M \neq R$ and there are no proper ideals of R properly containing M. For any two ideals I and J of R, we define their addition as follows:

$$I + J = \{a + b : a \in I, b \in J\}.$$

The multiplication is defined as follows:

$$IJ = \left\{ \sum_{i=1}^{m} a_i b_i : a_i \in I, b_i \in J, m \in \mathbb{N} \right\}.$$

It is easy to verify that the sets defined above are ideals. We say that I and J are *coprime* if $I + J = R$. Note that if I and J are distinct maximal ideals of R, then they are coprime, since $I \subsetneq I + J$, so $I + J = R$.
Define:

$$\sqrt{I} = \{a : a^k \in I,\ k \in \mathbb{N}^+\}.$$

An ideal I is a *radical ideal* if $\sqrt{I} = I$.

For any field $\mathbb{F}$ and polynomials $f_1, \cdots f_m$ in the ring $\mathbb{F}[x_1, \cdots, x_n]$ where $m, n \in \mathbb{N}$, we define the *variety* of $f_1, \cdots f_m$ to be the set of all their common roots, denoted by $V(f_1, \cdots, f_m)$. We will also write $\langle f_1, \cdots, f_m \rangle$ to denote the ideal generated by the polynomials $f_1, \cdots f_m$.

The next proposition can be found in most algebra textbooks. For completeness, we present the proof of it outlined in [3].

Proposition 1. [3] Let R be a commutative ring with identity and let $m \in \mathbb{N}$. If $I_1, \cdots, I_m$ are pairwise coprime ideals of R, then:

$$I_1 \cdots I_m = I_1 \cap \cdots \cap I_m$$

Proof. Let $m \in \mathbb{N}$ be given and let $I_1, \cdots, I_m$ be pairwise coprime ideals of R. Let $J = \prod_{k=1}^{m-1} I_k$. We claim that J and I_m are coprime. To prove the claim, observe that since for all $k \in [m-1]$, I_k and I_m are coprime, then $I_k + I_m = R = \langle 1 \rangle$. Therefore, there is some $x_k \in I_k$ and $y_k \in I_m$ such that $x_k + y_k = 1$. Then we

have the following equality:

$$\prod_{k=1}^{m-1} x_k = \prod_{k=1}^{m-1} (1 - y_k) = 1 \mod I_m$$

where the last equality follows from the fact that $y_k \in I_m$ for all $k \in [m-1]$, and so are their products. But then we have that $J + I_n = \langle 1 \rangle$, so indeed J and I_n are coprime.

Due to the above claim, it now suffices to prove the proposition for the case when $m = 2$, as it can then be easily generalized to arbitrary m by induction. Hence, we may assume $m = 2$, so the claim becomes:

$$I_1 I_2 = I_1 \cap I_2.$$

We proceed to prove this by double containment. First, observe that $I_1 I_2$, by definition, is the sum of the products of the form ab where $a \in I_1$ and $b \in I_2$. Hence, it suffices to show that $ab \in I_1 \cap I_2$ for all such a and b. But this follows directly from the definition of an ideal: since $a \in I_1$, then $ab \in I_1$, and similarly since $b \in I_2$, then $ab \in I_2$. Hence $ab \in I_1 \cap I_2$ and we conclude that $I_1 I_2 \subseteq I_1 \cap I_2$. For the reverse direction, let $x \in I_1 \cap I_2$. Since I_1 and I_2 are coprime, there exist some $a \in I_1$ and $b \in I_2$ such that $a + b = 1$. Multiplying both sides by x, we obtain:

$$ax + bx = x$$

Now note that since $a \in I_1$ and $x \in I_2$ and since $x \in I_1$ and $b \in I_2$, we have that $ax + bx \in I_1 I_2$, so $x \in I_1 I_2$, as desired. Hence, the reverse containment holds, and we conclude $I_1 I_2 = I_1 \cap I_2$. □

We are now ready to prove Theorem 1 using the concepts described above. Recall the statement of the theorem:

Theorem 1. Let $\mathbb{F}$ be a field and let $f = f(x_1, \cdots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \cdots, x_n]$. Let $A_1, \cdots, A_n$ be non-empty finite subsets of $\mathbb{F}$ and define $g_i(x_i) = \prod_{a \in A_i}(x_i - a)$. If $f(a_1, \cdots, a_n) = 0$ for all $a_i \in A_i$, then there are polynomials $h_1, \cdots, h_n \in \mathbb{F}[x_1, \cdots, x_n]$ satisfying $\deg(h_i) \leq \deg(f) - \deg(g_i)$ such that:

$$f = \sum_{i=1}^{n} h_i g_i.$$

The below proof was first introduced by [14], and we add some left out details with the help of [8] for completeness.

Proof. Let $\Omega = V(g_1, \cdots, g_n)$. Note that the common zeros of $g_1, \cdots, g_n$ are exactly the set $A_1 \times \cdots \times A_n$, so $\Omega = A_1 \times \cdots \times A_n$. Since, by assumption, the polynomial f vanishes at all common roots of $g_1, \cdots, g_n$, we also have that $\Omega \subseteq V(f)$. Let $\bar{a} = (a_1, \cdots, a_n) \in \Omega$ be arbitrary. Consider the ideal

$$M_{\bar{a}} = \langle x_1 - a_1, \cdots, x_n - a_n \rangle.$$

We claim that $M_{\bar{a}}$ is maximal. Define

$$h : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F} : p \mapsto p(a_1, \cdots, a_n).$$

It is routine to verify that h is a surjective homomorphism. Moreover, the kernel of h is precisely all the polynomials that vanish at the tuple $\bar{a}$. Since $a_1, \cdots, a_n \in \mathbb{F}$, every such polynomial has a factor $x_i - a_i$ for some $i \in [n]$. Hence, the kernel

of h is exactly the ideal $\langle x_1 - a_1, \cdots, x_n - a_n \rangle$. Thus, by the First Isomorphism Theorem, we get:

$$\mathbb{F}[x_1, \cdots, x_n]/M_{\bar{a}} \cong \mathbb{F}.$$

Since $\mathbb{F}$ is a field, so is $\mathbb{F}[x_1, \cdots, x_n]/M_{\bar{a}}$. It follows that $M_{\bar{a}}$ is maximal.

Now note that if $f \notin M_{\bar{a}}$, then, since $M_{\bar{a}}$ is maximal, $\langle M_{\bar{a}} \cup f \rangle = \langle 1 \rangle$. Equivalently, there exist some polynomials $P \in \mathbb{F}[x_1, \cdots, x_n]$ and $q \in M_{\bar{a}}$ such that $Pf + q \equiv 1$. But also note that:

$$P(\bar{a}) \cdot f(\bar{a}) + q(\bar{a}) = 0 + 0 = 0$$

which is a contradiction. Hence, $f \in M_{\bar{a}}$. Since $\bar{a}$ was arbitrary, this holds for each $\bar{a} \in \Omega$, so $f \in \bigcap_{\bar{a} \in \Omega} M_{\bar{a}}$. Since all the ideals in the intersection are maximal (and hence pairwise coprime), by Proposition 1, we get that $\bigcap_{\bar{a} \in \Omega} M_{\bar{a}} = \prod_{\bar{a} \in \Omega} M_{\bar{a}}$. Therefore, $f \in \prod_{\bar{a} \in \Omega} M_{\bar{a}}$.

We now claim that $\prod_{\bar{a} \in \Omega} M_{\bar{a}} \subseteq \langle g_1(x_1), \cdots, g_n(x_n) \rangle$. Let $q \in \prod_{\bar{a} \in \Omega} M_{\bar{a}}$. Note that, by definition,

$$\prod_{\bar{a} \in \Omega} M_{\bar{a}} = \left\{ \sum_{j=1}^{m} \prod_{\bar{a} \in \Omega} h_{\bar{a}}^j : h_{\bar{a}}^j \in M_{\bar{a}}, m \in \mathbb{N} \right\}.$$

Then, $q = \sum_{j=1}^{m} \prod_{\bar{a} \in \Omega} h_{\bar{a}}^j$ for some $m \in \mathbb{N}$. It then suffices to show that $\prod_{\bar{a} \in \Omega} h_{\bar{a}}^j \in \langle g_1(x_1), \cdots, g_n(x_n) \rangle$ for all $j \leq m$, since ideals are closed under addition. Let $j \in [m]$ be fixed. Then, for simplicity of notation, we shall omit j in the superscript when writing polynomials. Note that for each $\bar{a} = (a_1, \cdots, a_n) \in \Omega$, since $h_{\bar{a}} \in$

$M_{\bar{a}}$, it must be of the form:

$$h_{\bar{a}} = p_1^{\bar{a}} \cdot (x_1 - a_1) + \cdots + p_n^{\bar{a}} \cdot (x_n - a_n)$$

where $p_i^{\bar{a}} \in F[x_1, \cdots, x_n]$ for all $i \in [n]$. Then observe that the product of these polynomials over all tuples can be represented as follows:

$$\prod_{\bar{a} \in \Omega} h_{\bar{a}}^j = \prod_{\bar{a} \in \Omega} \Big(p_1^{\bar{a}} \cdot (x_1 - a_1) + \cdots + p_n^{\bar{a}} \cdot (x_n - a_n) \Big) \tag{4}$$

$$= \sum_{f : \Omega \to [n]} \prod_{\bar{a} \in \Omega} \Big(p_{f(\bar{a})}^{\bar{a}} \cdot (x_{f(\bar{a})} - a_{f(\bar{a})}) \Big). \tag{5}$$

Hence, it suffices to show that each of the terms in the sum above is in the specified ideal.

Let $f : \Omega \to [n]$ be arbitrary. We now claim that $\prod_{\bar{a} \in \Omega} \Big(p_{f(\bar{a})}^{\bar{a}} \cdot (x_{f(\bar{a})} - a_{f(\bar{a})}) \Big)$ is divisible by $g_i(x_i)$ for some $i \in [n]$, which will then conclude the proof. For a given $i \in [n]$ and $a \in A_i$, we will say that a satisfies property Π_i if there exists no tuple $\bar{a} = (a_1, \cdots, a_n) \in \Omega$ such that $f(\bar{a}) = i$ and $a_i = a$. We claim that there exists some $i \in [n]$ such that no $a \in A_i$ satisfies Π_i. To prove this, suppose, toward a contradiction, that for all $i \in [n]$, there is some $a_i^* \in A_i$ that satisfies Π_i. For each i, fix such a_i^*. Let $\bar{b} = (b_1, \cdots, b_n) = (a_1^*, \cdots, a_n^*) \in A_1 \times \cdots \times A_n = \Omega$. Let $k = f(\bar{b})$. Then, observe that $b_k = a_k^*$. However, by assumption, a_k^* satisfies Π_k, which is a contradiction. Thus, there exists some $i \in [n]$ such that no $a \in A_i$ satisfies Π_i. Fix such an i.

Then, since none of the elements in A_i satisfy Π_i, for all $a \in A_i$, there is a tuple $\bar{c} = (c_1, \cdots, c_n) \in \Omega$ such that $f(\bar{c}) = i$ and $c_i = a$. For each $a \in A_i$, fix and

denote such a tuple by $\bar{c}_a$. Then, for all $a \in A_i$, the product $\prod_{\bar{a}\in\Omega}(x_{f(\bar{a})} - a_{f(\bar{a})})$ will have a factor

$$x_{f(\bar{c}_a)} - c_{f(\bar{c}_a)} = x_i - c_i = x_i - a.$$

Since the above is true for all $a \in A_i$, the product $\prod_{\bar{a}\in\Omega}(x_{f(\bar{a})} - a_{f(\bar{a})})$ will have a factor $g_i(x_i) = \prod_{\bar{a}\in\Omega}(x_i - a)$, and so will lie in the specified ideal. Hence, indeed, $\prod_{\bar{a}\in\Omega}\left(p^{\bar{a}}_{f(\bar{a})} \cdot (x_{f(\bar{a})} - a_{f(\bar{a})})\right)$ is divisible by $g_i(x_i)$ for the fixed i. Since $f : \Omega \to [n]$ was arbitrary, this concludes the proof.

□

3.2 Short Proof of the Combinatorial Nullstellensatz II

As shown in Section 2, the proof of the Combinatorial Nullstellensatz II originally used the Combinatorial Nullstellensatz I. The next proof due to Michałek [13] is independent of the Combinatorial Nullstellensatz I and is shorter than the original one. Recall the statement of the theorem:

Theorem 2: Let $\mathbb{F}$ be a field and let $f = f(x_1, \cdots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \cdots, x_n]$. For each $i \in [n]$, let t_i be a non-negative integer, and suppose $\deg(f) = \sum_{i=1}^n t_i$. Also, suppose that the coefficient of $\prod_{i=1}^n x_i^{t_i}$ in f is non-zero. Then, for all subsets $A_i \subseteq F$ such that $|A_i| > t_i$, $i \in [n]$, there are $a_1 \in A_1, \cdots, a_n \in A_n$ such that $f(a_1, \cdots, a_n) \neq 0$.

Proof. [13] We proceed by induction on $\deg(f) = \sum_{i=1}^n t_i$. Note that if $\sum_{i=1}^n t_i = 0$, then $t_i = 0$ for all $i \in [n]$. Since the highest degree of f is 0 and the coefficient of the highest term is non-zero, $f \equiv c \neq 0$, so the assertion is clearly true. Now, suppose $\sum_{i=1}^n t_i > 0$ and let the sets $A_1, \cdots, A_n$ satisfy the hypotheses of the theorem. Without loss of generality, we may assume that $t_1 > 0$. Then, let $a \in A_1$ (note $|A_1| > 1$). By the division algorithm for polynomials, we get polynomials

$p, q \in \mathbb{F}[x_1, \cdots, x_n]$ such that

$$f = p \cdot (x_1 - a) + q$$

where

$$\deg_{x_1}(q) < \deg_{x_1}(x_1 - a).$$

Therefore, $\deg_{x_1}(q) = 0$, so q is independent of x_1. Since $t_1 > 0$, there are no monomials of the form $x_1^{t_1} \cdots x_n^{t_n}$ in q. Hence, $x_1^{t_1 - 1} \cdots x_n^{t_n}$ has a non-zero coefficient in p, and moreover, $\deg(p) = \left(\sum_{i=1}^{n} t_i\right) - 1 < \sum_{i=1}^{n} t_i = \deg(f)$.

If there exists some $(a_2, \cdots, a_n) \in A_2 \times \cdots \times A_n$ such that $q(a_2, \cdots, a_n) \neq 0$, then $f(a, a_2, \cdots, a_n) = q(a_2, \cdots, a_n) \neq 0$ and the theorem holds. So, suppose q vanishes for tuples in $A_2 \times \cdots \times A_n$. Applying the inductive hypothesis to p and the sets $A' = A_1 \setminus \{a\}, A_2, \cdots, A_n$, we get a tuple $(a_1, a_2, \cdots, a_n) \in A' \times A_2 \times \cdots \times A_n$ such that $p(a_1, a_2, \cdots, a_n) \neq 0$, Hence, we obtain

$$\begin{aligned} f(a_1, \cdots, a_n) &= (a_1 - a) \cdot p(a_1, \cdots, a_n) + q(a_2, \cdots, a_n) \\ &= (a_1 - a) \cdot p(a_1, \cdots, a_n) \neq 0 \end{aligned}$$

and this concludes the proof. □

3.3 Generalized Combinatorial Nullstellensatz II

The Generalized Combinatorial Nullstellensatz is a theorem due to Łason [12], which relaxes the assumption on the degree of the polynomial. The proof is very similar to the one in the previous section.

Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, \cdots, x_n]$ where $n \in \mathbb{N}^+$. We define the support of f, denoted by $S(f)$, to be the set of all $(t_1, \cdots, t_n) \in \mathbb{N}^n$ such that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is non-zero in f. We can define a natural partial order on the set $S(f)$ by letting $(t_1, \cdots, t_n) \leq (s_1, \cdots, s_n)$ if and only if $t_i \leq s_i$ for all $i \in [n]$.

Theorem 3. [12] Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x_1, \cdots, x_n]$. Let $(t_1, \cdots, t_n) \in S(f)$ be a maximal element in $S(f)$. Then, for any subsets $A_i \subseteq F$ such that $|A_i| \geq t_i+1$ for all $i \in [n]$, there are $a_1 \in A_1, \cdots, a_n \in A_n$ such that $f(a_1, \cdots, a_n) \neq 0$.

Note that this theorem is a generalization of the Combinatorial Nullstellensatz, since now the degree of f is not required to be $\sum_{i=1}^n t_i$; we only require $(t_1, \cdots, t_n)$ to be maximal in the support.

Proof. Note that since $(t_1, \cdots, t_n)$ is in the support of f, we get that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ in f is non-zero. We proceed by induction on $\sum_{i=1}^n t_i$. For the base case, suppose $\sum_{i=1}^n t_i = 0$. Then, as degrees are always non-negative in polynomials, we get that $t_i = 0$ for all $i \in [n]$. Then, as the monomial $x_1^{t_1} \cdots x_n^{t_n}$ has a non-zero coefficient, it becomes a non-zero constant c. Moreover, as $(t_1, t_2, \cdots, t_n) = (0, 0, \cdots, 0)$ is assumed to be maximal in $S(f)$, it is clearly also maximum, so $f \equiv c \neq 0$. Hence, $f \neq 0$ for any input, and the claim holds.

Now let $\sum_{i=1}^n t_i > 0$ and assume that it also holds for all natural numbers $k < \sum_{i=1}^n t_i$. Let the sets $A_1, \cdots, A_n$ satisfy the hypotheses of the theorem. Without loss of generality, we may assume that $t_1 > 0$. Let some $a \in A_1$ be given. Then, by the division algorithm, there exist some polynomials $p, q \in \mathbb{F}[x_1, \cdots, x_n]$ such

that:

$$f = p \cdot (x_1 - a) + q$$

where $\deg_{x_1}(q) < \deg_{x_1}(x_1 - a)$. This means $\deg_{x_1}(q) = 0$, i.e. q is a polynomial in variables $x_2, \cdots, x_n$ only. If there exists a tuple $(a_2, \cdots, a_n) \in A_2 \times \cdots \times A_n$ such that $q(a_2, \cdots, a_n) \neq 0$, then we obtain $f(a, a_2, \cdots, a_n) = q(a_2, \cdots, a_n)$ and the claim holds. So assume that q vanishes for all elements in $A_2 \times \cdots \times A_n$.

Note that if some $(r_1, \cdots, r_n) \in S(p)$, then $x_1^{r_1} \cdots x_n^{r_n}$ has a non-zero coefficient in p. Then $x_1^{r_1+1} \cdots x_n^{r_n}$ has a non-zero coefficient in $p \cdot (x_1 - a)$. It also then has a non-zero coefficient in $f = p \cdot (x_1 - a) + q$, as q is a polynomial in $x_2, \cdots, x_n$ only. Hence, $(r_1 + 1, \cdots, r_n) \in S(f)$. Therefore,

$$S(p) \subseteq \{(a_1 - 1, a_2, \cdots, a_n) : (a_1, a_2, \cdots, a_n) \in S(f)\} \tag{6}$$

Now consider $(t_1 - 1, t_2, \cdots, t_n)$. If the coefficient of $x_1^{t_1-1} x_2^{t_2} \cdots x_n^{t_n}$ is zero in p, then the coefficient of the monomial $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ is zero in $p \cdot (x_1 - a)$. But then its coefficient is also zero in f, which contradicts the fact $(t_1, \cdots, t_n) \in S(f)$. Hence, the coefficient of $x_1^{t_1-1} x_2^{t_2} \cdots x_n^{t_n}$ is non-zero in p, and since $(t_1, \cdots, t_n)$ was maximal in $S(f)$, then $(t_1 - 1, \cdots, t_n)$ has to be maximal in the support of p, by (6).

Let $A' = A_1 \setminus \{a\}$. Applying the inductive hypothesis to the polynomial p, the tuple $(t_1 - 1, t_2, \cdots, t_n)$ and the sets $A', A_2, \cdots, A_n$, we get that there is some $a_1 \in A', a_2 \in A_2, \cdots, a_n \in A_n$ such that $p(a_1, \cdots, a_n) \neq 0$. But then, as q

vanishes at all $(a_2, \cdots, a_n)$, we get:

$$\begin{aligned} f(a_1, \cdots, a_n) &= (a_1 - a) \cdot p(a_1, \cdots, a_n) + q(a_2, \cdots, a_n) \\ &= (a_1 - a) \cdot p(a_1, \cdots, a_n) \neq 0 \end{aligned}$$

Hence we obtained the desired tuple and this concludes the proof. □

Note that the above expression uses the fact that $\mathbb{F}$ has no zero divisors, since it is a field. In fact, the assumption that $\mathbb{F}$ is a field is too strong and can be relaxed to just requiring that $\mathbb{F}$ is an integral domain for the two theorems above to hold.

4 Applications

We devote this section to numerous applications of the Combinatorial Nullstellensatz in various areas of mathematics.

4.1 Cauchy-Davenport Theorem: Two Proofs

The first application, which Alon [2] referred to as a "classical" one is the Cauchy-Davenport Theorem, a famous theorem in number theory and combinatorics. The Combinatorial Nullstellensatz provides an alternative proof of the theorem. In this section, we contrast two different proofs, one of which uses the Combinatorial Nullstellensatz and one of which doesn't.

For any two sets A and B, we define their sum $A + B$ as follows:

$$A + B = \{a + b : a \in A, b \in B\}.$$

Theorem 4 (Cauchy-Davenport)**.** Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

4.1.1 Proof 1

Proof 1. [11] We proceed by induction on $|A|$. For the base case, let $|A| = 1$. Then, $|A+B| = |B| = |A|+|B|-1$, which concludes the base case. Now, suppose that $|A| = n > 1$ and that the claim holds for all natural numbers less than n. Further, we may assume that $|A| \neq p$ and $|B| \neq p$, since then the theorem holds trivially. Suppose first that $|A+B| = |B|$. If $0 \notin A$, we can subtract the smallest element of A from all of its elements, since it doesn't affect the cardinality. So we may just assume that $0 \in A$. Then, since $0 \in A$, we get that $B \subseteq A+B$, and hence $A+B = B$. This implies that $a+B = B$ for all $a \in A$. Define $H = \{h \in \mathbb{Z}/p\mathbb{Z} : h+B = B\}$. It is routine to verify that H is a subgroup of $\mathbb{Z}/p\mathbb{Z}$. Moreover, by the remark above, $A \subseteq H$. Since we assumed that $|A| > 1$, H is non-trivial. Moreover, if $H = \mathbb{Z}/p\mathbb{Z}$, then $h+B = B$ for all $h \in \mathbb{Z}/p\mathbb{Z}$. But then $B = H$, so $|B| = |H| = p$, yet we assumed $|B| \neq p$, a contradiction. So, we get that H is a non-trivial proper subgroup of $\mathbb{Z}/p\mathbb{Z}$, but since p is prime, it is not possible.

Thus, we we may assume that $|A+B| > |B|$. Then $A+B \not\subseteq B$, so there exists some $b' \in B$ such that $A+b' \not\subseteq B$. Let $A_0 = \{a \in A : a+b' \notin B\}$, then $|A_0| \geq 1$. Let $A' = A \setminus A_0$ and $B' = (A_0+b') \cup B$. Since $A_0 \subseteq A$, we have that

$|A'| = |A| - |A_0|$, and hence $|A'| < |A|$. Note also that by the way we defined A_0, we have that $a_0 + b' \notin B$ for all $a_0 \in A_0$. So, $(A_0 + b') \cap B = \varnothing$ and hence, $|B'| = |A_0 + b'| + |B| = |A_0| + |B|$. Finally, we claim that $A' + B' \subseteq A + B$. It suffices to show that $(A \setminus A_0) + (A_0 + b') \subseteq A + B$. Let $a \in A \setminus A_0, a_0 \in A_0$ be given. Then since $a \notin A_0$, there is some $b \in B$ such that $a + b' = b$. Hence:

$$a + a_0 + b' = a_0 + (a + b') = a_0 + b \in A + B.$$

Hence, indeed $A' + B' \subseteq A + B$ and thus, applying the inductive hypothesis to A' and B', we get:

$$\begin{aligned} |A + B| &\geq |A' + B'| \\ &\geq \min\{p, |A| - |A_0| + |A_0| + |B| - 1\} \\ &= \min\{p, |A| + |B| - 1\} \end{aligned}$$

which concludes the proof. □

4.1.2 Proof 2

Proof 2. [2] First, note that if $|A| + |B| > p$, then A and B must intersect. Let $q \in \mathbb{Z}/p\mathbb{Z}$. Then, clearly, $q - B = \{q - b : b \in B\} \subseteq \mathbb{Z}/p\mathbb{Z}$ and $|q - B| = |B|$, since all the elements in B are distinct. Hence, $q - B$ and A must intersect as well, so there exists some $b \in B$ and $a \in A$ such that $q - b = a \implies q = a + b \implies q \in A + B$. Since this is true of all $q \in \mathbb{Z}/p\mathbb{Z}$, we get that $\mathbb{Z}/p\mathbb{Z} = A + B$. In this case, $|A + B| = p$ and the theorem holds.

So, we may assume $|A| + |B| \leq p$. Then, toward a contradiction, suppose that

the result of the theorem is false. Then, as $|A| + |B| - 1 < p$, we get that $|A+B| \leq |A| + |B| - 2$. Then, there exists some $C \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $A + B \subseteq C$ and $|C| = |A| + |B| - 2$. Define $f(x, y) \in \mathbb{Z}/p\mathbb{Z}[x, y]$ as follows:

$$f = f(x, y) = \prod_{c \in C} (x + y - c).$$

Since $A + B \subseteq C$, then for all $a \in A$ and $b \in B$, we have $a + b = c$ for some $c \in C$. It follows that $f(a, b) = 0$ for all $(a, b) \in A \times B$. Let $t_1 = |A| - 1$ and $t_2 = |B| - 1$. Note that:

- $t_1 + t_2 = |A| + |B| - 2 = |C| = \deg(f)$.
- The coefficient of $x^{t_1} y^{t_2}$ in f is $\binom{|A|+|B|-2}{|A|-1}$ by the Binomial Theorem. Since $|A| + |B| - 2 < p$, p can't divide the coefficient, so it is non-zero in $\mathbb{Z}/p\mathbb{Z}$.

Hence, we can apply Theorem 2 (with $n = 2, A_1 = A, A_2 = B$) and get that there is some $a' \in A$ and $b' \in B$ such that $f(a', b') \neq 0$, a contradiction.

□

4.2 Graph and Hypergraph Coloring

In this section we will explore the applications of the Combinatorial Nullstellensatz II in graph and hypergraph coloring. The theorem turns out to be extremely useful in providing a necessary and sufficient condition for a certain graph (or hypergraph) to be k-colorable for some $k \in \mathbb{N}$. Let us state some basic definitions first.

For any graph $G = (V, E)$ on n vertices, it is useful to enumerate the vertices, i.e. identify $V = [n]$. To each vertex $v \in V$, we will then associate a variable x_v. We

define the *graph polynomial* as follows:

$$f_G(x_1, x_2, \cdots, x_n) = \prod_{\substack{i<j \\ \{v_i,v_j\}\in E(G)}} (x_i - x_j).$$

A *vertex coloring* (or simply *coloring*) of a graph $G = (V, E)$ is a map $c : V \to C$ where C is a set of colors. A *proper vertex coloring* of a graph $G = (V, E)$ is a vertex coloring such that $c(u) \neq c(v)$ whenever $\{u, v\} \in E(G)$. In other words, it is an assignment of a color to each vertex such that no adjacent vertices have the same color. We say that a graph G is *k-colorable* if there exists a proper coloring of G that uses k colors or less.

Theorem 5. [2] A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof. First, suppose G is not k-colorable. Let A be the set of the kth roots of unity. Define $g_v(x_v) = \prod_{a\in A}(x_v - a) = x_v^k - 1$ for each $v \in V$. The common zeros of these polynomials are the kth roots of unity. Note that any coloring c of G gives an evaluation of the polynomial f_G, namely $f_G(c(x_1), \cdots, c(x_n))$. Since G is not k-colorable, any coloring of its vertices with the kth roots of unity has two adjacent vertices sharing the same color. Hence, the graph polynomial f_G vanishes for any coloring of the vertices in G with the kth roots of unity, i.e. it vanishes any assignment of points in A^n to $(x_1, \cdots, x_n)$. Hence, it vanishes at all common zeros of g_v for all $v \in$ V. Therefore, by Theorem 1, we get that f_G is a $\mathbb{C}[x_v : v \in V]$-linear combination of those polynomials, and therefore, has to lie in the ideal generated by them.

Next, suppose that f_G is in the specified ideal. Then, it is a combination of the

polynomials $x_v^k - 1$, $v \in V$. Hence, f_G vanishes whenever each x_v attains a value that is a kth root of unity. Thus, every coloring of f_G with the kth roots of unity makes f_G vanish, which means that for any such coloring, there is an edge whose adjacent vertices are colored the same. Thus, G is not k-colorable. □

A *hypergraph* $H = (V, E)$ is the finite set V (vertices) and a collection E of non-empty subsets of vertices (hyperedges). A hypergraph is a generalization of the notion of graph where each edge can be incident to any number of vertices. A hypergraph is m-uniform for some positive integer m if each hyperedge has cardinality m. We say that a hypergraph H is k-colorable if there exists a coloring of its vertices with k or less colors such that no edge is monochromatic.

Theorem 6. An m-uniform hypergraph $H = (V, E)$ is not k-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \Big(\big(\sum_{v \in e} x_v \big)^k - m^k \Big)$$

lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof. Let H be an m-uniform hypergraph. First, suppose H is not k-colorable. Then any k-coloring will produce a monochromatic edge. Then for any coloring with kth roots of unity, there is an edge e' all of vertices in which have the same color assigned to them, call it z. Then, for that edge, $\big(\sum_{v \in e'} z \big)^k = (mz)^k = m^k z^k = m^k$. Therefore, g_H vanishes at all roots of unity, which are all the common zeros of the polynomials of the form $g_v(x_v) = x_v^k - 1$, $v \in V$. Thus, it has to lie in the ideal generated by them, by Theorem 1.

On the other hand, suppose the polynomial g_H lies in the specified ideal. Then,

it vanishes whenever each $x_v, v \in V$ is assigned a value that is a kth root of unity. So, consider any coloring of the vertices of H with the kth roots of unity. Since g_H vanishes, it must be the case that one of the terms in the product is 0. So, for some edge e', we have $\left(\sum_{v \in e'} x_v\right)^k = m^k$ for the specified assignment of colors to $x_v, v \in e'$. Let $z_1, z_2, \cdots, z_m$ be the colors assigned to the vertices of e'. Then we claim that $z_1 = z_2 = \cdots = z_m$. To prove this claim, first, to each kth root of unity z, we will associate a vector w_z from the origin of the complex plane that has its head at z. Clearly, the length of each such vector is $|z| = 1$. Since we know that $(z_1 + \cdots + z_m)^k = m^k$ and both m and k are positive integers, we have that $|z_1 + \cdots + z_m|^k = |w_{z_1} + \cdots + w_{z_m}|^k = m^k$. It is easy to see that the equality holds when $z_1 = z_2 = \cdots = z_m$, so we just need to show that no other solutions are possible. It suffices to show that $|w_{z_i} + w_{z_j}| < 2$ whenever $z_i \neq z_j$ for any $i, j \in [m]$, because then we would have:

$$\begin{aligned} |z_1 + \cdots + z_i + z_j + \cdots + z_m| &= |w_{z_1} + \cdots + w_{z_i} + w_{z_j} + \cdots + w_{z_m}| \\ &\leq |w_{z_1}| + \cdots + |w_{z_i} + w_{z_j}| + \cdots + |w_{z_m}| \\ &= |w_{z_i} + w_{z_j}| + m - 2 \\ &< m \end{aligned}$$

Which would mean that such a solution isn't possible. Let θ be the angle between

the vectors w_{z_i} and w_{z_j}. Since they are not collinear, $\cos\theta < 1$. Notice that:

$$\begin{aligned}
|w_{z_i} + w_{z_j}| &= \sqrt{(w_{z_i} + w_{z_j}) \cdot (w_{z_i} + w_{z_j})} \\
&= \sqrt{|w_{z_i}|^2 + 2w_{z_i} \cdot w_{z_j} + |w_{z_j}|^2} \\
&= \sqrt{|w_{z_i}|^2 + 2|w_{z_i}||w_{z_j}| \cos\theta + |w_{z_j}|^2} \\
&= \sqrt{2 + 2\cos\theta} < 2
\end{aligned}$$

Therefore, it has to be the case that $z_1 = \cdots = z_m$. But this means that e' is a monochromatic edge. Since the coloring of H was arbitrary, we conclude that H is not k-colorable. □

The above theorem is a generalization of the theorem proved in [2] for the special case when $m = 3$ and $k = 2$.

4.3 Sudoku Puzzle as a Graph Coloring Problem

In this section, we will describe the famous Sudoku puzzle as a graph coloring problem and apply Theorem 5 to obtain a necessary and sufficient condition for a given Sudoku puzzle to have solutions.

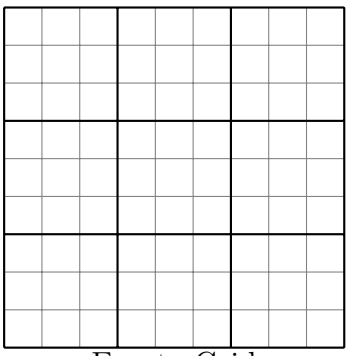
Sudoku is a recreational logic puzzle, which consists of a 9×9 grid divided into nine 3×3 subgrids (called *blocks*). Given a grid with partial filling, the objective is to fill in the remaining blank cells with the numbers $\{1, 2, \cdots, 9\}$ such that the following three rules are satisfied:

1. no numbers in the same row are the same;

2. no numbers in the same column are the same;

3. no numbers in the same block are the same.

If such a filling is possible, we say that a puzzle has a solution. We will refer to partial fillings as *restrictions* or *constraints*.



Empty Grid

			4					
	5		7					9
			9			6		1
9	6	4					8	
		7				9		
3	1				2			
			8					7
2						1		3

Grid with Restrictions

The problem of finding solutions to a Sudoku puzzle can be restated as a problem of extending a partial coloring of a graph to a full proper 9-coloring. We define the *Sudoku graph* S by associating a vertex to each cell in the grid and placing an edge between two vertices if and only if they are in the same row or the same column or the same block. This way, we obtain a graph with 81 vertices, and each cell/row/block is associated to a complete subgraph on 9 vertices. Note there are 27 such complete subgraphs in total; denote each of them by H_i, where $i \in [27]$.

It is clear that restrictions in a puzzle correspond to a partial coloring of vertices in S — for each cell filled with $k \in [9]$, the corresponding vertex in S is assigned the color k. Let S_R denote the graph S with the partial vertex coloring that corresponds to the restrictions, denoted by R, of a given puzzle. Then, a puzzle with restrictions R has solutions if and only if S_R is 9-colorable with the colors in $[9]$.

As before, to each vertex v in S, we will associate a variable x_v. In total, we will be working in a polynomial ring with 81 variables. For each $i \in [27]$, let q_i denote the graph polynomial of the subgraph H_i. That is,

$$q_i = \prod_{\{v,w\} \in E(H_i)} (x_v - x_w).$$

For each H_i, we will encode restrictions by modifying each graph polynomial as follows. For each vertex $u \in V(S)$ that must be colored $k_u \in [9]$, let $H_{i_1}, H_{i_2}, H_{i_3}$ be the subgraphs in which u appears. Then, for each $j \in [3]$, we modify q_{i_j} by substituting the value k_u for the variable x_u. Call the resulting polynomial f_{i_j}. Doing so for each vertex specified in the restrictions and letting $f_i = q_i$ whenever H_i has no restrictions, we obtain new polynomials f_i for each $i \in [27]$ which now encode the partial coloring corresponding to the restrictions. Define

$$h_R = \prod_{i=1}^{27} f_i.$$

Clearly, there exists a bijection between $\{1, \cdots, 9\}$ and the 9th roots of unity. Pick any such bijection. Thus, we may equivalently talk about coloring the graph S or filling out the Sudoku with the 9th roots of unity. This turns out to be helpful, as it gives us the following theorem:

Theorem 7. S_R is not 9-colorable if and only if h_R lies in the ideal generated by $\{x_v^9 - 1 : v \in [81]\}$.

Proof. The proof is very similar to that of the Theorem 5. First, suppose that S_R is not 9-colorable. Then any coloring with the 9th roots of unity will yield two adjacent vertices with the same color. Hence, $f_i = 0$ for some $i \in [27]$ for such

coloring, and so $h_R = 0$ as well. Let A be the set of the 9th rooths of unity. Also, let $g_v = \prod_{a \in A}(x_v - a) = x_v^9 - 1$ for all $v \in [81]$. Then, since h_R vanishes at all common zeros of g_v polynomials, by Theorem 1 we have that it lies in the ideal generated by them.

Conversely, suppose that h_R lies in the specified ideal. Then, it must vanish at all assignments of the 9th roots of unity to the variables x_v, $v \in [81]$. Hence, in any coloring of S_R with the 9th roots of unity, there is an edge whose vertices are assigned the same color. This means S_R is not 9-colorable. □

Note that this gives us a purely algebraic necessary and sufficient condition for a given Sudoku puzzle to have a solution. We also briefly remark that the above result generalizes to an $n \times n$ puzzle, by modifying the proof in the obvious way.

4.4 Minimum Bandwidth of a Graph

The *bandwidth* of a graph $G = (V, E)$ with n vertices is defined to be the minimum integer k such that there is a bijection $f : V \to \{1, \cdots, n\}$ satisfying $|f(u) - f(v)| \leq k$ for all $\{u, v\} \in E$. Any bijection satisfying the requirements above is called an optimal numbering.

A *sparse matrix* is defined to be a matrix, most of whose entries are zero. A *band matrix* is a sparse $n \times n$ matrix whose non-zero elements appear only on the diagonal band, which is the main diagonal together with diagonals adjacent to it on either or both sides. Bandwidth is an important notion in matrix theory, since optimal numberings describe the permutations of the rows and columns of the adjacency matrix of a graph so that 1-entries appear close to the main diagonal,

thus making the adjacency matrix a band matrix. This can be extremely helpful in speeding up the calculation of the inverse for large matrices (West, [15]). Calculating the bandwidth of a graph is known to be NP-complete, due to [7].

The next theorem provides a necessary and sufficient condition for a graph to have the bandwidth of at least $k+1$ for some $k \in \mathbb{N}$.

Theorem 8. [2] The bandwidth of a graph $G = (V, E)$ where $V = [n]$, is at least $k+1$ if and only if the polynomial

$$f_{G,k}(x_1, \cdots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \prod_{\substack{\{i,j\} \in E \\ i<j}} \prod_{k < |\ell| < n} (x_i - x_j - \ell)$$

lies in the ideal $\langle g_1(x_1), \cdots, g_n(x_n) \rangle$ where $g_i(x_i) = \prod_{j \in [n]} (x_i - j)$ for all $i \in [n]$.

Proof. First, suppose that the bandwidth of G is greater than k. Then, we claim that for any assignment of numbers in $\{1, \cdots, n\}$ to the variables $x_1, \cdots, x_n$ makes the polynomial $f_{G,k}$ vanish. To prove the claim, consider one such assignment. If two of the variables attain the same value, then $f_{G,k}$ vanishes because the first big product vanishes. So, we may assume that each variable is assigned a distinct value in $[n]$, so we get a bijection from V to $[n]$. But then, by the assumption on the bandwidth, there is an edge $\{i, j\} \in E$ for which $|x_i - x_j| = r > k$. So, the term of the form $(x_i - x_j - r)$ appears in the second product, thus making $f_{G,k}$ vanish in this case too. Hence, indeed $f_{G,k}$ vanishes on all elements in $[n]$. Now observe that these are exactly the common roots of the polynomials $g_i(x_i)$, so by Theorem 1, the desired conclusion follows.

For the other direction, suppose $f_{G,k}$ lies in the specified ideal. Then, since all

$g(x_i)$ vanish for any assignment of the values in $[n]$ to the variables $x_1, \cdots, x_n$, any $\mathbb{C}[x_1, \cdots, x_n]$-linear combination of these polynomials vanishes too. So, $f_{G,k}$ vanishes for any such assignment. In particular, it vanishes when we substitute distinct values for $x_1, \cdots, x_n$. This implies $\prod_{1 \leq i < j \leq n}(x_i - x_j)$ is nonzero, so the second product of $f_{G,k}$ must be zero. This means that there is some edge $\{i, j\} \in E$ such that $x_i - x_j = r$ for some $k < |r| < n$. But then $|x_i - x_j| = |r| > k$. Since the labeling of the vertices with distinct values of $[n]$ was arbitrary, we conclude that the bandwidth of G is at least $k + 1$, as desired. □

It may be useful to note that in the above theorem, the choice of the polynomial becomes very clear once one analyzes the proof. That is, the polynomial that is chosen is precisely the polynomial that will make both directions hold. Different terms in the product make sure the polynomial indeed vanishes for different cases, as we may see in the proof.

4.5 f-choosability of Graphs

The *chromatic number* of a graph is defined to be the minimum number of colors needed to properly color it. Let $G = (V, E)$ be a graph and let $f : V \to \mathbb{N}^+$ be a function. We say that G is *f-choosable* if for every assignment of a set $S(v)$ of integers to the vertex $v \in V$ such that $|S(v)| = f(v)$, there exists a proper coloring c of G such that $c(v) \in S(v)$ for all $v \in V$. An *orientation* of an (undirected) graph G is an assignment of a direction to each of the edges of G, thus making it a directed graph. We will denote an edge between two vertices u and v by $\{u, v\}$ in an undirected graph and by uv in a directed graph.

A directed subgraph H of a directed graph D is called Eulerian if the indegree of

every vertex of H is equal to its outdegree. We call such directed subgraph H *even* if it has an even number of edges and we call it *odd* if it has an odd number of edges. We let $EE(D)$ and $EO(D)$ denote the numbers of even and odd Eulerian subgraphs of D, respectively.

The next theorem is an application of the Combinatorial Nullstellensatz II in the choosability of graphs. The sketch of the proof is given in [2] and we fill in the details with the help of [10] and [4].

Theorem 9. [2] Let $G = (V, E)$ where $V = \{1, 2, \cdots, n\}$ be an undirected graph, and consider an orientation D of G. For each $k \in [n]$, let d_k be the outdegree of the vertex k in D and define $f : V \to \mathbb{Z} : k \mapsto d_k + 1$. If $EE(D) \neq EO(D)$, then G is f-choosable.

Proof. For each $k \in [n]$, let $A_k \subseteq \mathbb{Z}$ be a set of cardinality $d_k + 1$. If G is f-choosable, there exists a proper coloring of G that assigns each vertex k a color from the set A_k. This is equivalent to saying that there must exist some n-tuple of colors $(c_1, c_2, \cdots, c_n) \in A_1 \times A_2 \times \cdots \times A_n$ such that $f_G(c_1, c_2, \cdots, c_n)$ doesn't vanish, where f_G is the graph polynomial of G.

It is clear that the number of edges in an undirected graph is the sum of outdegrees of its vertices in any orientation. Hence, $\deg(f_G) = |E| = \sum_{k=1}^{n} d_k$. In order to apply Combinatorial Nullstellensatz II, it remains to show that the coefficient of $\prod_{k=1}^{n} x_k^{d_k}$ is non-zero in f_G.

Let us call an orientation of G *even* if the number of its directed edges $i \to j$ such that $i > j$ is even; otherwise, call it *odd*. For a fixed tuple $(d_1, d_2 \cdots, d_n)$, let

$DE_G(d_1, d_2 \cdots, d_n)$ denote the set of all even orietations of G where the outdegree of the vertex k is d_k for all $k \in [n]$. Similarly, define $DO_G(d_1, d_2 \cdots, d_n)$ to be the set of all odd orietations of G where the outdegree of the vertex k is d_k for all $k \in [n]$. Define the polynomial h_G as follows:

$$h_G(x_1, ..., x_n) = \sum_{d_1,...,d_n \geq 0} \left(\left(|DE_G(d_1, d_2 \cdots, d_n)| - |DO_G(d_1, d_2 \cdots, d_n)| \right) \cdot \prod_{k=1}^{n} x_k^{d_k} \right)$$

We claim that $f_G = h_G$. To show this, we proceed by induction on the size of the edge set, $|E|$. For the base case, suppose $|E| = 0$, i.e. G is an independent set of vertices. Then, if $(d_1, d_2 \cdots, d_n) = (0, 0, \cdots, 0)$, we have that $DE(0, 0, \cdots, 0) = 1$ (since 0 edges is an even orientation) and $DO(0, 0, \cdots, 0) = 0$. For a non-zero tuple $(d_1, d_2 \cdots, d_n)$, we get both $DE(d_1, d_2 \cdots, d_n)$ and $DO(d_1, d_2 \cdots, d_n)$ equal zero, as there are no orientations possible with no edges and a non-zero outgoing degree for some vertices. Thus, $h_G = 1 = f_G$, since the degree of f_G is zero in this case, and so it must be the constant function 1.

For the inductive step, assume that the claim holds for all graphs with $|E| - 1$ or fewer edges. So if $G = (V, E)$ is a graph with $|E|$ edges, let $e = \{u_k, u_\ell\} \in E(G)$ be an arbitrary edge such that $k < \ell$. Let $E' = E \setminus \{e\}$ and define $G' = (V, E')$ to be the subgraph obtained by removing e from G. Then G' is a graph with $|E| - 1$ edges, and by the inductive hypothesis, we get:

$$h_{G'} = \sum_{d_1,...,d_n \geq 0} \left(\left(|DE_{G'}(d_1, d_2 \cdots, d_n)| - |DO_{G'}(d_1, d_2 \cdots, d_n)| \right) \cdot \prod_{k=1}^{n} x_k^{d_k} \right) = f_{G'}$$

If e is oriented as $u_k \to u_\ell$, then, since $k < \ell$, we have that the number of directed edges $i \to j$ such that $i > j$ in G is the same as in G'. Similarly, if e is oriented

as $u_\ell \to u_k$, then the number of edges $i \to j$ such that $i > j$ in G goes up by one compared to G', and thus the parity of an orientation is changed. Since e has to be oriented in exactly one of the above ways, then, for a given tuple $(d_1, d_2 \cdots, d_n)$, we can write:

$$\begin{aligned} |DE_G(d_1, d_2 \cdots, d_n)| &= |DE_G(d_1, \cdots, d_{k-1}, d_k - 1, d_{k+1}, \cdots, d_n)| \\ &\quad + |DO_G(d_1, \cdots, d_{\ell-1}, d_\ell - 1, d_{\ell+1}, \cdots, d_n)| \end{aligned}$$

$$\begin{aligned} |DO_G(d_1, d_2 \cdots, d_n)| &= |DO_G(d_1, \cdots, d_{k-1}, d_k - 1, d_{k+1}, \cdots, d_n)| \\ &\quad + |DE_G(d_1, \cdots, d_{\ell-1}, d_\ell - 1, d_{\ell+1}, \cdots, d_n)| \end{aligned}$$

Finally, observe that, by the definition of f_G, it is clear that $f_G = f_{G'}(x_k - x_\ell)$. Therefore, we obtain:

$$
\begin{aligned}
&f_G(x_1, \cdots, x_n) = f_{G'}(x_1, \cdots, x_n)(x_k - x_\ell) \\
&= \sum_{d_1,\ldots,d_n \geq 0} \left(\left(|DE_{G'}(d_1, \cdots, d_n)| - |DO_{G'}(d_1, \cdots, d_n)| \right) \cdot \prod_{k=1}^{n} x_k^{d_k} \right) \cdot (x_k - x_\ell) \\
&= \sum_{d_1,\ldots,d_n \geq 0} \left(\left(|DE_{G'}(d_1, \cdots, d_n)| - |DO_{G'}(d_1, \cdots, d_n)| \right) \cdot (x_k - x_\ell) \cdot \prod_{k=1}^{n} x_k^{d_k} \right) \\
&= \sum_{d_1,\ldots,d_n \geq 0} \Bigg(\Big(|DE_{G'}(d_1, \cdots, d_{k-1}, d_k - 1, d_{k+1}, \cdots, d_n)| \\
&\qquad\qquad - |DO_{G'}(d_1, \cdots, d_{k-1}, d_k - 1, d_{k+1}, \cdots, d_n)| \\
&\qquad\qquad - |DE_{G'}(d_1, \cdots, d_{\ell-1}, d_\ell - 1, d_{\ell+1}, \cdots, d_n)| \\
&\qquad\qquad + |DO_{G'}(d_1, \cdots, d_{\ell-1}, d_\ell - 1, d_{\ell+1}, \cdots, d_n)| \Big) \cdot \prod_{k=1}^{n} x_k^{d_k} \Bigg) \qquad (*) \\
&= \sum_{d_1,\ldots,d_n \geq 0} \left(\left(|DE_G(d_1, d_2 \cdots, d_n)| - |DO_G(d_1, d_2 \cdots, d_n)| \right) \cdot \prod_{k=1}^{n} x_k^{d_k} \right) \\
&= h_G(x_1, \cdots, x_n)
\end{aligned}
$$

Note that (*) follows from bringing the term $(x_k - x_\ell)$ inside the function $h_{G'} = f_{G'}$ and analyzing possible orientations of the edge $\{x_k, x_\ell\}$.

Now, that we know the two functions are equal, it suffices to show that the coefficient of $\prod_{k=1}^{n} x_k^{d_k}$ is non-zero in h_G. We will consider the given orientation D. Let $C \in DE_G(d_1, d_2 \cdots, d_n) \cup DO_G(d_1, d_2 \cdots, d_n)$ be another orientation of G and let $D \oplus C$ denote the set of all edges of D (preserving their orientation) that are oriented in the opposite direction in C. Since both D and C have the same outdegrees to maintain for each vertex, if some edge has the opposite orientation in C compared to D, then other edges incident to its endpoints would have to

have opposite orientations as well. It is then clear that the resulting graph $D \oplus C$ is Eulerian, as reversing the orientation of some edge $a \to b$ from out to in, guarantees the reversal of another edge that had its sink in a (similarly for the other case). Consider the following map

$$\varphi : C \mapsto D \oplus C$$

It is not hard to see that the map is a bijection between all orientations of G and all of its Eulerian subgraphs. Given an Eulerian subgraph H of G, we construct an orientation C that maps to it by reversing all of the edges of H in the orientation D, and keeping remaining edges the same. Clearly, such construction is unique for each H and thus indeed φ is bijective.

We now claim that if D is an even orientation, then φ sends even orientations to even Eulerian graphs, and odd orientations to odd Eulerian subgraphs. On the other hand, if D is an odd orientation, then φ sends even orientations to odd Eulerian graphs, and odd orientations to even Eulerian subgraphs. We will prove the case when D is even, since the proofs for the other cases are similar. Suppose D and C are both even. Then D has $2k$ edges oriented $i \to j$ with $i > j$ and C has 2ℓ such edges. Let $|E(D \oplus C)| = n$. We would like to show that n is even. Let n_1 be the number of edges in $D \oplus C$ such that $i \to j$ with $i > j$ in D. Let n_2 be the number of edges in $D \oplus C$ such that $i \to j$ with $i > j$ in C. Note that $n_1 + n_2 = n$. Then $2k - n_1$ represents the number of edges $i \to j$ with $i > j$ in $D \setminus (D \oplus C)$. Similarly, $2\ell - n_2$ represents the number of edges $i \to j$ with $i > j$ in $C \setminus (D \oplus C)$. Since these edges are outside of $D \oplus C$, where C and D agree on

edge orientation, we conclude that:

$$\begin{aligned} 2k - n_1 = 2\ell - n_2 &\implies 2k - 2\ell = n_1 - n_2 \\ &\implies 2(k-\ell) = n_1 - n_2 \\ &\implies 2(k-\ell) + 2n_2 = n_1 + n_2 = n \qquad (**) \end{aligned}$$

Therefore, n is indeed even and this concludes the proof. For the case when D is even and C is odd, the exact argument as above will work, except we replace 2ℓ by $2\ell + 1$ and thus get an extra $+1$ term on the left hand side in (**).

Using the claim above and the fact that φ is a bijection, we can see that this implies that:

$$\Big||DE(d_1, \cdots, d_n)| - |DO(d_1, \cdots, d_n)|\Big| = \Big|EE(D) - EO(D)\Big| \neq 0$$

Therefore, the coefficient of the desired term in h_G is non-zero, and we apply the Combinatorial Nullstellensatz II to conclude that there exists some n-tuple of colors $(c_1, c_2, \cdots, c_n) \in A_1 \times A_2 \times \cdots \times A_n$ at which $f_G = h_G$ doesn't vanish. Hence, G is f-choosable. □

4.6 An Application of the Generalized Combinatorial Nullstellensatz

Before we introduce an interesting graph-theoretic application of the Generalized Combinatorial Nullstellensatz, we shall state and prove two useful basic facts from graph theory. As before, the definitions below come from West [15] but we also

present them here for completeness.

A graph G is called *bipartite* if its vertex set can be written as a union of two disjoint sets, such that no vertices in the same set are adjacent. The specification of the two sets that satisfy these conditions is called a *bipartition* of G. Each of such sets is called a *partition*.

A *walk* in a graph is a sequence $v_0e_1v_1e_2v_2\cdots v_{k-1}e_kv_k$ of vertices v_i and edges e_i such that for all $i \in [k]$, the edge e_i has endpoints v_{i-1} and v_i. A walk is called *closed* if $v_0 = v_k$. We will say a walk is a u, v-walk to indicate that the start vertex is u and the end vertex is v. A *path* in a graph is a walk in which no vertices or edges are repeated. A *cycle* is a closed walk with no repeated edges and exactly one repeated vertex. The *length* of a walk is defined to be the number of edges in it. We will call a walk even (or odd) if it has an even (or odd) length. A walk W is said to *contain* a cycle C if the sequence of vertices and edges of C occurs as a subsequence of W (in order, but not necessarily consecutively).

Lemma 2. [15] Every closed odd walk contains an odd cycle.

Proof. Let W be a closed u, u-walk in some graph. Suppose W has length n where n is odd. We proceed by induction on n. The base case when $n = 1$ holds trivially, since in this case W is a loop, and is itself a cycle. Assume now the lemma holds for all closed odd walks of length $k < n$. If u is the only repeated vertex in W, then it is a cycle itself, and we're done. Suppose it isn't the case, so there is another vertex v that is traversed at least twice in W. Then v breaks W into two v, v-walks joined by the single vertex v. Call these two walks W_1 and W_2. Since W is odd by assumption, one of these walks is even and another one

is odd. Without loss of generality, assume W_1 is odd. Then note that W_1 is a closed odd walk of a shorter length than W, so, by the inductive hypothesis, it contains an odd cycle C. But then C is also contained in W, and this concludes the proof. □

The next theorem is due to König, and it gives a necessary and sufficient condition for a graph to be bipartite.

Theorem 10. [15] A graph is bipartite if and only if it has no odd cycle.

Proof. Let G be a bipartite graph with the patritions X and Y. Since the edges of G only connect the vertices in X to the vertices in Y, the vertices of any cycle have to alternate between the two partitions. Hence, in order come back to the same partition, an even number of steps is required.

Conversely, suppose we have a graph G that contains no odd cycle. We may assume G is connected (otherwise simply consider each of its components separately). Let $u \in V(G)$ be arbitrary. Define $f : V(G) \to \mathbb{N}$ to be the function such that for any vertex $v \in V(G)$, $f(v)$ returns the distance of the shortest path between u and v. Note $f(v)$ is defined for each $v \in V(G)$, since we assume G was connected. Let $X = \{v \in V(G) : f(v) \text{ is even}\}$ and $X = \{v \in V(G) : f(v) \text{ is odd}\}$. It is clear that X and Y are disjoint and exhaust the vertex set of G. We also claim that X and Y form a bipartition of G. Indeed, if two vertices v_1 and v_2 in X are adjacent, then since the distances between v_1 and u and v_2 and u are even, we get an odd walk that traverses u, v_1 and v_2. By Lemma 2, we get an odd cycle, which is a contradiction. Hence, no vertices within X are adjacent. Applying a similar argument to Y, we get that no vertices within Y are adjacent

either. Therefore, G is bipartite, as desired.

□

For a graph $G = (V, E)$, the *neighborhood* of a vertex v, denoted by $N(v)$, is defined to be the set of all vertices that are adjacent to v. A *vertex labeling* of a graph $G = (V, E)$ is a map $c : V \to \mathbb{N}$. We will refer to the elements in the image of such a map as *labels*. A *lucky labeling* is a vertex labeling such that for any two adjacent vertices u and v in G we have that $\sum_{w \in N(u)} c(w) \neq \sum_{w \in N(v)} c(w)$.

A graph is *planar* if it can be drawn in a plane without any edges crossing. It has been shown in [5] that any bipartite planar graph has a lucky labeling with the labels in the set $\{1, 2, 3\}$ only. This result turns out to be a special case of the next theorem.

Theorem 11. [12] Let $G = (V, G)$ be a bipartite graph, which has an orientation with outgoing degree bounded by k. Suppose every vertex is equipped with a non-constant polynomial $f_v \in \mathbb{R}[x]$ of degree at most ℓ and positive leading coefficient. Then there is a labeling $c : V \to \{1, 2, ..., k\ell + 1\}$ such that for any two adjacent vertices u and w:

$$c(u) - \sum_{v \in N(u)} f_v(c(v)) \neq c(w) - \sum_{v \in N(w)} f_v(c(v)).$$

Let us provide the proof of this theorem, which was first outlined in [12], filling some details.

Proof of Theorem 11. We begin by assigning every vertex $v \in V(G)$ a variable x_v.

Consider the polynomial:

$$h = \prod_{uw \in E(G)} \Big(\sum_{v \in N(u)} f_v(x_v) + x_w - \sum_{v \in N(w)} f_v(x_v) - x_u \Big).$$

It suffices to show that there exists some assignment of values a_v to x_v for all $v \in V(G)$ from the set $\{1, 2, ..., k\ell + 1\}$ such that $h(a_v : v \in V(G)) \neq 0$. This would mean that none of the terms of the product vanish for this assignment, and by letting $c(v) = a_v$, the result would follow immediately.

We will fix an orientation of G with outgoing degree of every vertex bounded by k. Consider some edge $uw \in E(G)$, oriented $u \to w$. When we take the term in the big product of h corresponding to this edge, we note that f_u appears as one of the terms in the sum $\sum_{v \in N(w)} f_v(x_v)$. So for every such edge $u \to w$, we take the leading monomial in f_u from the product term corresponding to this edge in h. (For example if $f_u(x) = x^2 - 6$, then we would take $-x^2$ where the minus sign comes from the definition of h). Taking the product of these terms over all edges, we obtain some monomial, which we denote by M. Note that the degree of M in every variable is bounded by $k\ell$, i.e. $\deg_{x_v}(M) \leq k\ell$ for all $v \in V$. This is because the leading monomial in $f_v(x_v)$ for some v is taken at most k times and the degree of that monomial is at most ℓ.

Note that there may be other monomials in h that have the same support, i.e., if $M = C_M x^{s_1} ... x^{s_n}$ where $C_M \in \mathbb{R}$ is a constant, then there may exist monomials $N_1, ..., N_m$ in h such that $N_i = C_{N_i} x^{s_1} ... x^{s_n}$, where $C_{N_i} \in \mathbb{R}$ are corresponding constants for all $i \in [m]$. We will denote the sum of these monomials, including M, by M'. It now suffices to show that M' is maximal and has a non-zero

coefficient in h. (Then, since $s_i \leq k\ell$ for all i, the result is obtained by letting $A_v = \{1, ..., k\ell + 1\}$ for all v and applying Theorem 3).

Now we claim that the resulting monomial M' has maximal support in h, i.e., $(s_1, ..., s_n)$ is maximal in $S(h)$. Clearly, it suffices to show that M has maximal support. Note that every term in M is the leading monomial of the polynomial f_u assigned to some source vertex u. Thus, it can only appear in M in its highest power. Since we're only interested in maximal support, we can "collapse" all the polynomials to degree one polynomials. So, by the way M is composed, we add one to the power of x_u whenever x_u appears as a source. If we were to pick some other term, it could increase the power of M in some other variable, but would decrease the power in x_u, and so it couldn't have larger support. Thus, M has a maximal support in h.

Now, we want to ensure M' is non-vanishing. Note that since $M' = M + N_1 + ... + N_m$, it would suffice to show that all of $M, N_1, ..., N_m$ have the same sign (then, since we are in the field $\mathbb{R}$, they would never cancel out). Suppose, toward a contradiction that M and N_i have different signs, for some $i \in [m]$. Clearly, since all leading coefficients are positive, the sign of M is $(-1)^{|E|}$. Suppose the ways M and N_i are composed from the product terms of h differ in k places. We know, since the signs of M and N_i are different, there must me an odd number of places where instead of a negative term, we take a positive one. Note that every "switch" from a negative to a negative term forces precisely two edges to exist (i.e. if instead of $-x_a$ we take $-x_b$, then we know that a and b have a common neighbor, but are not adjacent, since otherwise we would get a K_3, which would

contradict the assumption that G is bipartite). Similarly, every "switch" from a negative term to a positive one results in exactly one edge. Since the number of negative to positive switches is odd and a switch from negative to negative always produces an even number of edges, we are forced to have a closed odd walk in our graph G. By Lemma 2, it follows that there must also exist an odd cycle, which, by Theorem 10, contradicts the hypothesis that G is bipartite. Hence, M and N_i have the same sign, and since i was arbitrary, $M, N_1, ..., N_m$ all have the same sign. Thus, M' is non-vanishing and by Theorem 3 we obtain the desired conclusion. □

Note that in the above theorem, the relaxation of the polynomial degree requirement was helpful. As noted in [12], the original Combinatorial Nullstellensatz doesn't seem to work for this problem.

Let us now briefly remark why the lucky labeling result for bipartite planar graphs proved in [5] is a special case of the above theorem. It is well-known that every planar graph $G = (V, E)$ with $|V| = n$ where $n \geq 3$ has at most $3n - 6$ edges. Moreover, if such a graph is triangle-free, the number of edges is at most $2n - 4$. Proofs of these facts can be found in [15]. Furthermore, it can be proven that any graph $G = (V, E)$ has an orientation with maximum outdegree d if and only if $|E| \leq d \cdot |V|$ (e.g. see [6]). Since bipartite graphs have no odd cycles (in particular, no triangles), we conclude that every bipartite planar graph has an orientation with outdegree bounded by 2. Let $f_v = x$ for each $v \in V$. Then, replacing the polynomial h in the proof of Theorem 11 by

$$h' = \prod_{uw \in E(G)} \Big(\sum_{v \in N(u)} f_v(x_v) - \sum_{v \in N(w)} f_v(x_v) \Big) = \prod_{uw \in E(G)} \Big(\sum_{v \in N(u)} x_v - \sum_{v \in N(w)} x_v \Big)$$

and proceeding similarly, we get that there is a labeling $c : V \to \{1, 2, 3\}$ such that for any adjacent vertices u and w,

$$\sum_{v \in N(u)} c(v) \neq \sum_{v \in N(w)} c(v)$$

holds. This is exactly what has been shown in [5].

5 Conclusion

The main purpose of this thesis was to demonstrate the power of the Combinatorial Nullstellensatz in discrete mathematics and inspire the reader to search for other applications of the two main theorems. As shown by Alon [2], there are also applications in linear algebra, number theory, and other areas. In graph theory, Combinatorial Nullstellesatz has also been useful in analyzing zero-sum flows (e.g. see [1]). Thus one direction for future work could be to look whether the Combinatorial Nullstellensatz could be useful in finding solutions to the existing open problems in these areas.

References

[1] S. Akbari et al. "Zero-Sum Flows in Regular Graphs". In: *Graphs and Combinatorics* 26.5 (2010), pp. 603–615.

[2] Noga Alon. "Combinatorial Nullstellensatz". In: *Combinatorics, Probability and Computing* 8 (1999), pp. 7–29.

[3] M.F. Atiyah and I.G MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, Inc., 1969.

[4] Courtney L. Baber. *An Introduction to List Colorings of Graphs*. Master's Thesis. Blacksburg, Virginia, 2009.

[5] Sebastian Czerwiński, Jarosław Grytczuk, and Wiktor Żelazny. "Lucky labelings of graphs". In: *Information Processing Letters* 109 (2009), pp. 1078–1081.

[6] Zdeněk Dvořák. *List coloring*. Lecture Notes for Kombinatorika a grafy III. 2015. eprint: https://iuuk.mff.cuni.cz/~rakdver/kgiii/lesson14-8.pdf.

[7] M. R. Garey et al. "Complexity Results for Bandwidth Minimization". In: *SIAM Journal on Applied Mathematics* 34.3 (1978), pp. 477–495.

[8] darij grinberg (https://math.stackexchange.com/users/586/darij grinberg). *Vishnoi's Proof of Combinatorial Nullstellensatz*. Mathematics Stack Exchange. eprint: https://math.stackexchange.com/q/3013824.

[9] R. Hartshorne. *Algebraic Geometry. Graduate Texts in Mathematics, 52*. Springer-Verlag, 1977.

[10] Brad R. Jones. *Combinatorial Nullstellensatz*. Math 800 Project at SFU, 2013. eprint: http://people.math.sfu.ca/~kya17/teaching/math800/Math800project.pdf.

[11] Swastik Kopparty. *The Cauchy Davenport Theorem*. Class Notes for Arithmetic Combinatorics, 2016.

[12] Michal Łason. "A generalization of Combinatorial Nullstellensatz". In: *The Electronic Journal of Combinatorics* 17 (2010). N32.

[13] Mateusz Michałek. "A short proof of combinatorial Nullstellensatz". In: *American Mathematical Monthly* 117 (2010), pp. 821–823.

[14] Nisheeth K. Vishnoi. "An algebraic proof of Alon's Combinatorial Nullstellensatz". In: *Congressus Numerantium* (2001).

[15] Douglas B. West. *Introduction to Graph Theory*. 2nd ed. Prentice Hall, 2000.