POLYNOMIAL METHODS: RECENT ADVANCEMENTS IN COMBINATORICS

by

Thomas Fleming

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

Major: Mathematical Sciences

The University of Memphis

December 2021

ACKNOWLEDGMENTS

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

ABSTRACT

Fleming, Thomas Rexford. M.Sc. The University of Memphis. May 2021. Polynomial Methods: Recent Advancements in Combinatorics. Major Professor: Dr. David Grynkiewicz.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

TABLE OF CONTENTS

Contents **Pages**

Chapter 1

Introduction

This is my introduction.

1.1 Background

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

1.1.1 Problems

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

1.2 Research Objectives

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec

ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Capitalize Combinatorial Nullstellensatz and remove verbosity in places where equations can be referenced by index instead of lin-

Chapter 2

Combinatorial Nullstellensatz

We begin by examining the primary theorem of this investigation, the Combinatorial Nullstellensatz. This theorem, a powerful generalization of the fundamental theorem of algebra, builds on Hilbert's Nullstellensatz. In fact, so powerful is this theorem that it will serve as the central tool in proofs from graph theory, additive combinatorics, and many other branches of math. To begin, let us indulge a bit of notation:

Notation (Coefficient of a polynomial)**.** For a polynomial

$f(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ let us define the coefficient of the monomial term $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ to be $[x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}] f\,(x_1, x_2, \ldots x_n)$. Hence, we have

$$f(x_1, x_2, \ldots, x_n) = \sum_{k_1, k_2, \ldots, k_n \in \mathbb{N}_0} \left([x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}] f\,(x_1, x_2, \ldots x_n) \right) x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}.$$

Let us also define the following notation for a polynomial of n variables :

Notation (Polynomial of n variables)**.** For simplicity, let us denote

$f\,(x_1, x_2, \ldots, x_n) = f\,(\mathbf{x})$ where it would not introduce unnecessary ambiguity.

Let us define one more notation, the degree of a polynomial projected onto a single variable x_j :

Notation (Degree of projected polynomial)**.** Let $\deg_{x_j} f\,(\mathbf{x})$ refer to the degree of $f\,(a_1, a_2, \ldots, x_j, \ldots, a_n)$. That is, the degree of f in a single variable, x_j.

With this bookkeeping out of the way let us now introduce the primary theorem, the Combinatorial Nullstellensatz:

Theorem 2.0.1 (Generalized Combinatorial Nullstellensatz)**.** Let R be an integral domain, and let $A_1, A_2, \ldots, A_n \subseteq R$ be finite and nonempty. Let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial and define $g_i(x_i) = \prod_{a \in A_i}(x_i - a) \in R[x_i]$ for $1 \leq i \leq n$. Then, we have that $f(a_1, a_2, \ldots, a_n) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ if and only if there are polynomials $h_1(\mathbf{x}), h_2(\mathbf{x}), \ldots, h_n(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ such that $f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) h_i(\mathbf{x})$ with $\deg g_i + \deg h_i \leq \deg f$ for each $1 \leq i \leq n$ and $\deg_{x_j} g_i(x_i) + \deg_{x_j} h_i \leq \deg_{x_j} f$ for all $1 \leq i, j \leq n$.

In order to prove this powerful theorem let us first state and prove the following lemma:

Lemma 2.0.1. Let R be an integral domain, $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$, and $A_1, A_2, \ldots, A_n \subseteq R$ be finite and nonempty. Suppose $\deg_{x_i} f < |A_i|$ for each $1 \leq i \leq n$ and $f(a_1, a_2, \ldots, a_n) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$. Then f is the zero polynomial.

Proof. Let F be the quotient field of R. Clearly, any polynomial in R is a polynomial in F and as $f = 0$ in F implies $f = 0$ in R we may only consider the case $F = R$. We will induce on n. For the case $n = 1$ this is a simple corollary of the fundamental theorem of algebra, hence we will omit the proof. Now, under the assumption that the case $n - 1$ is true, let us prove the case n. First, let us define $f_i(x_1, x_2, \ldots, x_{n-1})$ to be the polynomial such that

$$f(\mathbf{x}) = \sum_{i=0}^{\deg_{x_n} f} f_i(x_1, x_2, \ldots, x_{n-1}) x_n^i.$$

We see each $f_i \in F[x_1, x_2, \ldots, x_{n-1}]$ and $\deg_{x_j} f_i \leq \deg_{x_j} f \leq |A_i|$ for all $1 \leq j \leq n-1$ and $0 \leq i \leq \deg_{x_n} f$. Let $a_i \in A_i$ for each such i be an arbitrary element. As $f(a_1, a_2, \ldots, a_{n-1}, a) = 0$ for all $a \in A_n$ and $\deg_{x_n} f < |A_n|$, the $n = 1$ case implies that

$f(a_1, a_2, \ldots, a_{n-1}, x_n) = 0$ must be the zero polynomial, hence $f_i(a_1, \ldots, a_{n-1}) = 0$ for each i and $(a_1, \ldots, a_{n-1}) \in \prod_{i=1}^{n-1} A_i$. Hence, by the inductive hypothesis ($n-1$ case) we must have that each f_i is the zero polynomial, and hence f is the zero polynomial. □

This lemma comprises the majority of the intellectual heavy lifting for our main theorem and hence its proof will appear very simple in comparison to its powerful statement:

Proof of Generalized Combinatorial Nullstellensatz [1]. First, examining the backwards implication, it is clear that any polynomial of the form in the theorem (one that splits on x_i for each i into a polynomial which is implicitly zero on the whole of the product) will be zero on the whole of $\prod_{i=1}^{n} A_i$. Now, let us examine the converse (the forwards implication). First, let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial which is zero on the whole of such a product. We want to show that such a polynomial h_i exists for each i. For each $1 \leq j \leq n$ let us define

$$g_j(x_j) = \prod_{a \in A_j} (x_j - a) = x_j^{|A_j|} - \sum_{i=0}^{|A_j - 1|} g_{ji} x_j^i, \tag{2.0.1}$$

where each $g_{ji} \in R$ as well. Hence, as $a_j \in A_j$ implies that $g_j(a_j) = 0$ we must have that $a_j^{|A_j|} = \sum_{i=0}^{|A_j - 1|} g_{ij} a_j^i$. Now, define $\overline{f}$ to be the polynomial for which we repeatedly apply this substitution for each j to the polynomial f. We see that $\deg_{x_i}\left(\overline{f}\right) < |A_i|$ for each i(as any monomial term of such degree can be substituted for terms of lesser degree), and as $\overline{f}(\mathbf{a}) = f(\mathbf{a}) = 0$ for each $\mathbf{a} \in \prod_{i=1}^{n} A_i$ (This fact is trivial by the construction of f and $\overline{f}$), then by the preceding lemma we must have that $\overline{f} = 0$. Next, consider the polynomial $f(\mathbf{x}) - \overline{f}(\mathbf{x})$. Define $f_0 = f$ and f_i to be f after the i'th such substitution. Furthermore, let $N \in \mathbb{N}$ be such that $f_N = \overline{f}$. Then, the polynomial f_i is obtained by examining a term of f_{i-1} with a degree in x_j of atleast $|A_j|$ and replacing an individual factor of $x_j^{|A_j|}$ by the sum as we defined earlier. For simplicity let us take the term $c x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \cdot x_j^{|A_j|}$ (where $k_j \geq 0$ by our construction) and apply such a substitution. Then, we see that the difference

$$f_{i-1} - f_i = c x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \left(x_j^{|A_j|} - \sum_{i=0}^{|A_j| - 1} g_{ji} x_j^i \right) = c x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \cdot g_j(x_j)$$

by our original definition. Furthermore, as $f_N = \overline{f}$ we have that

$$f - \overline{f} = (f_0 - f_1) + (f_1 - f_2) + \ldots + (f_{N-1} - f_N).$$

Hence, as $f = f - 0 = f - \overline{f} = \sum_{j=1}^{n} g_j(x_j)\, h_j$ where each $h_j \in R[x_1, x_2, \ldots, x_n]$ is simply the sum of all of these preceding terms $cx_1^{k_1} \ldots x_n^{k_n}$ as a result of these substitutions.

Furthermore, by construction we had that $\deg g_j = |A_j| > \deg\left(\sum_{i=0}^{|A_j|-1} g_{ji} x_j^i\right)$, so we see that such a substitution will never increase the degree of our polynomial and hence $\deg f_i \leq \deg f$. Then, as $\deg g_j = |A_j|$ we see that

$$\deg\left(cx_1^{k_1} \ldots x_n^{k_n} g_j(x_j)\right) \leq \deg f_{i-1} \leq \deg f.$$

Using the additive nature of polynomial degree yields

$\deg\left(cx_1^{k_1} \ldots x_n^{k_n}\right) + \deg g_j \leq \deg f$, and as each h_j is simply the sum of such terms we may substitute its degree to yield $\deg g_j + \deg h_j \leq \deg f$. Applying the same argument but with the projected degree of g and f yields

$\deg_{x_i} g_j + \deg_{x_i} h_j \leq \deg_{x_i} f$ for all i, j. Hence the converse is true and this completes the proof. □

This theorem is perhaps too general and too powerful for use in proving our simpler results. As a corollary, many authors include a sort of "Combinatorial Nullstellensatz 2" wherein the splitting of a polynomial with certain requirements on degree is replaced by the existence of a member of the product $\prod_{i=1}^{n} A_i$ for which f is nonzero. This is the statement that we will declare as the Combinatorial Nullstellensatz and which will be used in the proof of all subsequent results which permit the use of such a theorem:

Theorem 2.0.2 (Combinatorial Nullstellensatz)**.** Let R be an integral domain, $A_1, A_2, \ldots, A_n \subseteq R$ be finite and nonempty, and
$f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial. Suppose

$$[x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}] f(\mathbf{x}) \neq 0$$

and that $\deg f = \sum_{i=1}^{n} d_i$ with $0 \leq d_i \leq |A_i| - 1$. Then, there exists an element $\mathbf{a} \in \prod_{i=1}^{n} A_i$ such that $f(\mathbf{a}) \neq 0$. That is, given a nontrivial "maximal degree" monomial of f such that the degree of this monomial in each variable individually is strictly less than the size of the corresponding set A_i, f cannot be zero on the whole of the product of the A_i.

This is the generalization of the Fundamental theorem of Algebra to which we referred earlier and it is precisely this simple statement about the size of the kernel of a particular polynomial which provides our combinatorial power. The proof follows rather directly from the negation of the generalized version and it is as follows:

Proof. Let $g_i = \prod_{a \in A_i} (x_i - a)$ for $1 \leq i \leq n$ and suppose the contrary. That is, $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ despite the assumptions of the construction. Then, applying the generalized combinatorial nullstellensatz yields polynomials $h_1, h_2, \ldots, h_n \in R[x_1, x_2, \ldots, x_n]$ with the desired properties. Now let us examine the nature of $[x_1^{d_1} \ldots x_n^{d_n}] f(\mathbf{x})$. As this is a maximal degree monomial of f, then only maximal degree monomials of $h_i(\mathbf{x}) g_i(x_i)$ can contribute to its coefficient in f as $\deg(h_i) + \deg(g_i) = \deg h_i g_i \leq \deg f$. However, by the construction of g_i, all such monomials will be taken from the $h_i(\mathbf{x}) \cdot x_i^{|A_i|}$ portion of this polynomial. Thus $\deg_{x_i} h_i g_i > d_i$ by our requirement that each $d_i < |A_i|$, hence all maximal degree monomials of f must be of the form $x_1^{k_1} x_2^{k_2} \ldots x_j^{|A_j|} \ldots x_n^{k_n}$. Thus, we must have

$[x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}] f(\mathbf{x}) = 0$, $\lightning$. Hence, there must be an $\mathbf{a} \in \prod_{i=1}^{n} A_i$ such that $f(\mathbf{a}) \neq 0$. □

Our last version of the Combinatorial Nullstellensatz will examine what happens when f vanishes over not all, but most (in a certain set-theoretic perspective) of the members of the product. This is known as the Punctured Combinatorial Nullstellensatz and it builds on the original generalized version. The proof will involve division of polynomials of many variables, so let us first examine the nature of such an operation.

Lemma 2.0.2 (Multivariate Polynomial Division)**.** Let R be an integral domain and let $g_1(x_1), \ldots, g_k(x_k) \in R[x_1, x_2, \ldots, x_n]$ be polynomials of one variable with leading coefficient 1 for $1 \leq k \leq n$. Multivariate polynomial division is well behaved if one of the following holds:

1: $f(\mathbf{x}) \in \sum_{i=1}^{k} R[x_1, x_2, \ldots, x_n] \cdot g_i(x_i)$ is nonzero implies that there is a $1 \leq i \leq k$ such that $\deg_{x_i}(f) \geq \deg(g_i)$.

2: For a polynomial $f \in R[x_1, x_2, \ldots, x_n]$ there are functions $w(\mathbf{x}), h_1, (\mathbf{x}), \ldots, h_k(\mathbf{x})$ such that all of the following hold:

$$f(\mathbf{x}) = \sum_{i=1}^{k} h_i(\mathbf{x})\, g_i(x_i) + w(\mathbf{x}), \tag{2.0.2}$$

$\deg_{x_j}(w) < \deg(g_j)$ for $1 \leq j \leq k$,

$\deg_{x_j}(g_i(x_i)) + \deg_{x_j}(h_i) \leq \deg_{x_j}(f)$, $\deg(g_i) + \deg(h_i) \leq \deg(f)$ for $1 \leq i \leq k, 1 \leq j \leq n$,

$\deg_{x_i}(w) \leq \deg_{x_i}(f)$ for $1 \leq i \leq n$, and

$\deg(w) \leq \deg(f)$.

Furthermore, the polynomial $w(\mathbf{x})$ is unique provided it satisfies the first condition of (2). Lastly, a simple substitution allows us to assume these cases to be mutually exclusive for the purposes of the proof of the punctured Combinatorial Nullstellensatz.

The proof of this lemma is ommitted (for now).

include proof of lemma

Theorem 2.0.3 (Punctured Combinatorial Nullstellensatz)**.** Let R be an integral domain and let $A_1, A_2, \ldots, A_n \subset R$ be finite and nonempty. Furthermore, for each $1 \leq i \leq n$ let $B_i \subseteq A_i$ be nonempty.

Let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial and set $g_i(x_i) = \prod_{a \in A_i}(x_i - a)$ and $l_i(x_i) = \prod_{b \in B_i}(x_i - b)$. If

$$f(\mathbf{a}) = 0 \; \forall \; \mathbf{a} \in \left(\prod_{i=1}^{n} A_i\right) \setminus \left(\prod_{i=1}^{n} B_i\right) \tag{2.0.3}$$

but there exists a $\mathbf{b} \in \prod_{i=1}^{n} B_i$ such that $f(\mathbf{b}) \neq 0$ then there are polynomial $h_i \in R[x_1, x_2, \ldots, x_n]$ with $1 \leq i \leq n$ such that

$$f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) h_i(\mathbf{x}) + w(\mathbf{x}) \text{ with } w(\mathbf{x}) = u(\mathbf{x}) \prod_{i=1}^{n} \frac{g_i(x_i)}{l_i(x_i)}.$$

with the following conditions holding:

$\deg(w) \leq \deg(f) \deg_{x_j}(w) \leq \deg_{x_j}(f)$ for all $1 \leq j \leq n$, $\deg_{x_i}(w) < |A_i|$,

$\deg(g_i) + \deg(h_i) \leq \deg(f)$ for $1 \leq i \leq n$ and

$\deg_{x_j}(g_i(x_i)) + \deg_{x_j}(h_i) \leq \deg_{x_j}(f)$ for $1 \leq i, j \leq n$. Consequently $\sum_{i=1}^{n}(|A_i| - |B_i|) \leq \deg(w) \leq \deg(f)$.

Proof. The preceding lemma guarantees there to be polynomials

$$w(\mathbf{x}), h_1(\mathbf{x}), \ldots, h_n(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$$

of the desired form and for which the proper conditions hold (case 2). Our task, then, is to ensure that the form of $w(\mathbf{x})$ is that of our statement. First, let $1 \leq i \leq n$ and without loss of generality select $i = 1$. First, we consider $w(\mathbf{x}) l_1(x_1)$. Then as f and the first sum of equation (2) must be zero on all $\mathbf{a} \in \prod_{i=1}^{n} A_i \setminus \prod_{i=1}^{n} B_i$, we see $w(\mathbf{x})$ must also vanish on this difference of products. Furthermore, by the construction of l_1 we must have that

$w(\mathbf{x})\, l_1(x_1)$ vanishes on $\prod_{i=1}^{n} B_i$ as well, hence it vanishes on all of $\prod_{i=1}^{n} A_i$. Applying theorem 1 (Generalized Combinatorial Nullstellensatz) yields polynomials $v_1, \ldots, v_n \in R[x_1, \ldots, x_n]$ such that

$$w(\mathbf{x})\, l_1(x_1) = \sum_{i=1}^{n} g_i(x_i)\, v_i(\mathbf{x}). \tag{2.0.4}$$

Now, by the preceding lemma we may assume that $v_j(\mathbf{x})$ is not of the form in case 1. Furthermore, for $n > 1$, we see $\deg_{x_n}(w(\mathbf{x})\, l_i(x_i)) > |A_n|$ as a consequence of the stipulations of $w(\mathbf{x})$. Now, for a polynomial $h \in f[x_1, ..., x_n]$ define $\overline{h}$ to be h reduced modulo the ideal generated by $g_1(x_1), \ldots, g_{n-1}(x_{n-1})$. Applying this operation to equation (4) yields

$$\overline{w(\mathbf{x})\, l_1(x_1)} = \overline{g_n(x_n)\, v_n(\mathbf{x})}.$$

□

Finish Proof of Punctured Nullstellensatz

With all three variations of the Combinatorial Nullstellensatz fully stated and proven, allow us to move on to the examination of some of the most powerful results which these theorems prove, namely in combinatorics. We will begin with a proof of the Chevalley-Warning theorem as well as several results of additive combinatorics concerning sumsets, both standard and restricted.

Maybe change proof to the one found in Simeon and Ball

Chapter 3

Chevalley-Warning Theorem and Sumsets

Move Chevalley-Warning to its own section and proved 1-2 more statements and proofs on sumsets

Our first major theorem of this section concerns the theorem of Chevalley and Warning which declares the conditions under which a certain nontrivial solution to a polynomial in a finite field of characteristic p can exist:

Theorem 3.0.1 (Chevalley-Warning Theorem)**.** Let F be a finite field of characteristic p and let $f_1, f_2, \ldots, f_k \in F[x_1, x_2, \ldots, x_n]$ be polynomials and N to be the number of points $\mathbf{x} \in F^n$ such that $f_1(\mathbf{x}) = \ldots = f_k(\mathbf{x}) = 0$. If $\sum_{i=1}^{k} \deg(f_i) < n$, then $N \equiv 0 (\text{mod } p)$.

In order to provide a proof of this statement, let us first state and prove the following lemma:

Lemma 3.0.1 (Lemma)**.** Let F be a finite field and $k_1, k_2, \ldots, k_n \geq 0$ such that $\min_{1 \leq i \leq n} k_i \leq |F| - 2$. Then, $\sum_{x_1, x_2, \ldots, x_n \in F} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = 0$. (Note: if a 0^0 occurs in the expressions it will be treated as a 1).

Proof. Assume without loss of generality that $k_1 < |F| - 1$. Then, by factoring out a $x_1^{k_1}$ from each term of the sum and grouping all such x_1's, we have $\sum_{x_1, x_2, \ldots, x_n \in F} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = \left(\sum_{x_1 \in F} x_1^{k_1}\right) \sum_{x_2, \ldots, x_n \in F} x_2^{k_2} \ldots x_n^{k_n}$, hence we must only show that $\sum_{x_1 \in F} x_1^{k_1} = 0$. Suppose $k_1 = 0$, then $\sum_{x_1 \in F} x_1^{k_1} = |F|$ and, since p divides $|F|$ we see the case $k_1 = 0$ is trivially true. Now, let $\omega \in F^\times$ be a generator of $F^\times$. Then, we have that

$$\sum_{x_1 \in F} x_1^{k_1} = \sum_{x_1 \in F^\times} x_1^{k_1} = \sum_{x_1 \in F^\times} (\omega x)^{k_1} = \omega^{k_1} \sum_{x_1 \in F^\times} x_1^{k_1} = \omega^{k_1} \sum_{x_1 \in F} x_1^{k_1}.$$

Taking the difference of the first and last terms of the above equality yields $\left(\omega^{k_1} - 1\right)\left(\sum_{x_1 \in F} x_1^{k_1}\right) = 0$, so we must have either the sum is 0 or $\omega^{k_1} - 1 = 0$.

However, as ω is a generator of the cyclic group $F^{\times}$, we may only have that $\omega^{k_1} = 1$ if $k_1 \equiv -1 \pmod{|F|}$. But, as $0 < k_1 < |F| - 1$ this case cannot occur, hence we see $\sum_{x_1 \in F} x_1^{k_1} = 0$, so the lemma is proven. □

Proof of Chevalley-Warning Theorem. Recalling that $x^{|F|} = x$ (and thus $x^{|F|-1} = 1$ for nonzero x). Then, define

$$M = \sum_{\mathbf{x} \in F^n} \prod_{i=1}^{k} \left(1 - f_i(\mathbf{x})^{|F|-1}\right).$$

We see, by the earlier proposition, that a term of the sum will be 1 if and only if **x** is a solution to the system $f_1, f_2, \ldots, f_k$, else it will be 0. Furthermore, it is clear by the construction that M will be exactly equal to the number of solutions to our system $f_1, \ldots, f_k$, and hence it precisely N.

Now, let us define the product from our construction to be a polynomial g, that is $g(\mathbf{x}) = \prod_{i=1}^{k} \left(1 - f_i(\mathbf{x})^{|F|-1}\right)$. Then, repeatedly applying the substitution $x_j^{|F|} \to x_j$ to g yields a polynomial $\overline{g} = g$ for all $\mathbf{x} \in F^n$. Furthermore, $\deg_{x_j}(\overline{g}) \leq |F| - 1$ for $1 \leq j \leq n$(This is clear as , if it were not we would be able to apply the substitution once again). Then, substituting $\overline{g}$ in place of g yields

$$M = \sum_{\mathbf{x} \in F^n} \overline{g}(\mathbf{x}).$$

Then, applying our lemma, we see that all monomials with degree $|F| - 2$ or less will equal 0 and hence the only possible nonzero terms of $\overline{g}$ are those of the form $\prod_{i=1}^{n} x_i^{|F|-1}$. Expanding the product, we see that such a monomial would be of degree $n(|F| - 1)$, however as $\deg f_i^{|F|-1} = (|F| - 1)\deg(f_i)$, we see that $\deg(g) \leq (|F| - 1)\sum_{i=1}^{k} f_i < n(|F| - 1)$ by construction. Consequently, any such monomial of $\overline{g}$ (and hence g) will have a zero coefficient, and thus $M = N \equiv 0 \pmod{p}$. □

This theorem allows us to prove certain constraints (and in the case of prime p, the exact value) on the size of the davenport constant for a certain group. This result is too advanced for now, but we will return to it later. Next, let us examine theorems concerning sumsets such as the Cauchy-Davenport Theorem and the Erdős-Heilbronn conjecture on the lower bound of the size of sumsets.

Theorem 3.0.2 (Cauchy-Davenport Theorem)**.** Given a prime p and nonempty $A, B \subseteq Z_p$, then $|A+B| \geq \min\{p, |A|+|B|-1\}$.

Proof. Suppose $|A|+|B| > p$, we must have that for any element $x \in Z_p$, $(A) \cap (x \setminus B) \neq \varnothing$ (As there are only p possible elements which could be in each set). Hence, $A+B = Z_p$. Thus, let us assume $|A|+|B| \leq p$ and suppose indirectly that $|A+B| \leq |A|+|B|-2$. Let $A+B \subseteq C \subseteq Z_p$ such that $|C| = |A|+|B|-2$. Next, define $f(x,y) = \prod_{c \in C}(x+y-c)$ and note that we must have $f(a,b) = 0$ for all $(a,b) \in A \times B$ as $A, B \subseteq C$. Now, note that $\deg(f) = |C| = |A|+|B|-2$, and hence $[x^{|A|-1}y^{|B|-1}]f(x,y) = \binom{|A|+|B|-2}{|A|-1} \neq 0$ as $|A|-1 < |A|+|B|-2 < p$. Hence, by the Combinatorial Nullstellensatz (Theorem 1.2), we must have a pair $(a,b) \in A \times B$ such that $f(a,b) \neq 0$ ↯. Thus, the theorem must be true. □

With this basic theorem about sumsets proven, we now take a look at restricted sumsets, those being sumsets where a sum is excluded if it satisfies a certain property, normally being the root of a particular polynomial.

Notation (Restricted Sumset)**.** For a polynomial $h(x_0, x_1, \ldots, x_k)$ and subsets $A_0, A_1, \ldots, A_k \subseteq Z_p$ define

$$\oplus_h \sum_{i=0}^{k} A_i = \{a_0 + a_1 + \ldots + a_k : a_i \in A_i, h(a_0, a_1, \ldots, a_k) \neq 0\}$$

to be the restricted sumset over the A_is with respect to h.

Theorem 3.0.3 (General Restricted Sumset Theorem)**.** For a prime p and a polynomial $h(x_0, .., x_k)$ over Z_p and nonempty $A_0, A_1, \ldots, A_k \subseteq Z_p$, define $c_i = |A_i| - 1$ and $m = \sum_{i=0}^{k} c_i - \deg(h)$.
If $[x_0^{c_0} \ldots x_k^{c_k}]((\sum_{i=0}^{k} x_i)^m \cdot h(\mathbf{x})) \neq 0$, then

$$\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq m + 1 \text{ (consequently m < p).}$$

Proof. Suppose indirectly that the inequality does not hold (and hence $m \geq p$), then we may define $E \subseteq Z_p$ such that E is a multi-set containing m elements and $\oplus_h \sum_{i=0}^{k} A_i \subseteq E$. Let $Q(\mathbf{x}) = h(\mathbf{x}) \prod_{e \in E} \left(\sum_{i=0}^{k} x_i - e \right)$. By our construction we must have that $Q(\mathbf{x}) = 0$ for all $\mathbf{x} \in \prod_{i=0}^{k} A_i$ as either $h(\mathbf{x}) = 0$ or $\sum_{i=0}^{k} x_i \in \oplus_h \sum_{i=0}^{k} A_i \subseteq E$. Furthermore $\deg(Q) = m + \deg(h) = \sum_{i=0}^{k} c_i$ by construction. From this we see $m \geq \sum_{i=0}^{k} c_i$ and hence $[x_0^{c_0} \ldots c_k^{c_k}]Q \neq 0$ (as it is binomial in nature).

Therefore, applying Combinatorial Nullstellenstaz (Theorem 1.2) yields an $\mathbf{a} \in A$ such at $Q(\mathbf{a}) \neq 0$ ↯. Thus $m < p$ and $\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq m + 1$. □

With this powerful result proven let us now take specific functions for h and prove superior lower bounds where possible. First, we examine the function $h(a_0, \ldots, a_k) = \prod_{0 \leq i < j \leq n} (a_i - a_j)$:

Theorem 3.0.4 (Restricted Sumset Theorem)**.** For a prime p, nonempty $A_0, A_1, \ldots, A_k \subseteq Z_p$ with $|A_i| \neq |A_j|$ for any $i \neq j$ and for the h defined above. If $\sum_{i=0}^{k} |A_i| \leq p + \binom{k+2}{2} - 1$, then

$$\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

A special case of this theorem for only two sets is the following:

Theorem 3.0.5 (Erdős-Heilbronn Conjecture)**.** For a prime p and nonempty $A, B \subseteq Z_p$, then $|A \oplus_h B| \geq \min\{p, |A| + |B| - \delta\}$ where $\delta = 3$ for the case $A = B$ and $\delta = 2$ in all other cases.

In order to prove these theorems, let us first state and prove a lemma concerning the coefficient of a particular polynomial:

Lemma 3.0.2. Let $0 \leq c_0, \ldots, c_k \in \mathbb{Z}$ and define $m = \sum_{i=0}^{k} c_i - \binom{k+1}{2}$ (it is trivial that m is nonnegative). Then,

$$[x_0^{c_0} \ldots x_k^{c_k}] \left(\left(\sum_{i=0}^{k} x_i \right)^m \prod_{k \geq i > j \geq 0} (x_i - x_j) \right) = \frac{m!}{c_0! c_1! \ldots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j).$$

Provide proof of this lemma based on proof of Ballot problem

With this out of the way, we now prove proposition 2.4:

Proof of Restricted Sumset Theorem. For this proof we will take the aforementioned

$$h(\mathbf{x}) = \prod_{0 \leq i < j \leq k} (x_i - x_j).$$

Now, let us define $c_i = |A_i| - 1$ and $m = \sum_{i=0}^{k} c_i - \binom{k+1}{2}$. Rearranging the assumptions of this theorem yields $\sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1 \leq p$ and, applying the trivial combinatorial identity $\binom{k+2}{2} = \binom{k+1}{2} + (k+1)$ yields

$\sum_{i=0}^{k} c_i - \binom{k+1}{2} + 1 = m + 1 \leq p$ (hence $m < p$). Then

$$[x_0^{c_0} \ldots x_k^{c_k}] \left(\left(\sum_{i=0}^{k} x_i \right) h \right) = \frac{m!}{c_0! \ldots c_k!} \prod_{0 \leq i < j \leq k} (c_i - c_j).$$

We know this product to be nonzero modulo p as $c_i \neq c_j$ for $i \neq j$ by construction and $m < p$. Finally, as the coefficient is nonzero and as $\deg(h) = \binom{k+2}{2}$ (as there are $k+2$ possible x_i's and each term of the product will contain two distinct x_i's so there are $\binom{k+2}{2}$ terms each of degree 1), we have $m = \sum_{i=0}^{k} c_i - \deg(h)$. Hence, applying theorem 2.3

Ask grynkiewicz about this as

yields $\left|\oplus_h \sum_{i=0}^{k} A_i\right| \geq m+1 = \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1$ by construction. □

We conclude this section with the proof of the Erdős-Heilbronn Conjecture:

Proof of Erdős-Heilbronn Conjecture. □

Add proof

Chapter 4

Zero-Sum Sequences, and the q-Dyson Theorem

Let us begin with some notation:

Notation (Subpower)**.** For a given independent variable q, define

$$(x)_k = (1-x)(1-xq)\left(1-xq^2\right)\ldots\left(1-xq^{k-1}\right).$$

For simplicity, define $(t)_0 = 1$.

The following theorems, concerned with the constant term of a particular laurent polynomial, serve to further demonstrate the power of our previous results. The special case $q = 1$ yields the Dyson conjecture:

Theorem 4.0.1 (Dyson Conjecture)**.**

$$[x_1^0 \ldots x_n^0]\left(\prod_{1\le i<j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i}\right) = \frac{(\sum_{i=1}^n a_i)!}{\prod_{i=1}^n (a_i!)}.$$

This case, originally proven by Gunson and Wilson using lagrange interpolation yields the following generalization:

Theorem 4.0.2 (q-Dyson Conjecture)**.** First, let us define the following polynomial:

$$f_q(\mathbf{x}) = f_q(x_1, x_2, \ldots, x_n) \coloneqq \prod_{1\le i<j\le n}\left(\frac{x_i}{x_j}\right)_{a_i}\left(\frac{qx_j}{x_i}\right)_{a_j}.$$

Then,

$$[x_1^0 \ldots x_n^0] f_q(\mathbf{x}) = \frac{(q)_{\sum_{i=1}^n a_i}}{\prod_{j=1}^n (q)_{a_j}}.$$

Proof. First, we note that if $a_i = 0$, then $(x)_{a_i} = (1-x)$, hence we may omit all of these

terms as they will not affect the constant. Hence, we know each (relevant) a_i is a positive integer. Let

$$F(\mathbf{x}) = \prod_{1 \le i < j \le n} \left(\prod_{i=0}^{a_i - 1} \left(x_j - x_i q^t \right) \cdot \prod_{t=1}^{a_j} \left(x_i - x_j q^t \right) \right).$$

Then, we note that the constant term in $f_q(\mathbf{x})$ will be equal to the coefficient $\prod_{i=1}^{n} x_i^{\sum_{i=1}^{n} a_i}$ in $F(\mathbf{x})$. $\square$

REFERENCES

[1] David J. Grynkiewicz. *The Polynomial Method: The Erdos:Heilbronn Conjecture*, volume 30. Springer, 2013.