Generalizing the Chevalley-Warning theorem

by

Lailah Collins

B.S., Fort Hays State University, 2022

A REPORT

submitted in partial fulfillment of the
requirements for the degree

MASTER OF SCIENCE

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2025

Approved by:

Major Professor
Craig Spencer

Copyright

Abstract

The Chevalley-Warning Theorem states that a set of polynomials over a finite field without constant terms has a non-trivial common zero if the number of variables exceeds the sum of the degrees. In this report, we will prove the Chevalley-Warning Theorem along with one of its generalizations. This will be done by using the Combinatorial Nullstellensatz.

Table of Contents

Chapter 1

Chevalley-Warning Theorem

In 1932 Emil Artin conjectured that finite fields are quasi-algebraically closed, which means every non-constant homogeneous polynomial with more variables than degree has a non-trivial zero. Let $\mathbb{F}_q$ be the finite field of q elements. Note that if $e_1, \ldots, e_n$ is a basis of a degree-n extension of the finite field $\mathbb{F}_q$, the norm of $e_1x_1 + \cdots + e_nx_n$ is a degree-n homogeneous polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]$ with no non-trivial zeros. Artin intended for his student Ewald Warning to prove his conjecture, but he revealed his conjecture to Claude Chevalley, who was able to prove the result in 1935 [4].

Chevalley's Theorem [3] states that a finite set of polynomials $f_j\,(x_1, \ldots, x_n)$ over a finite field $\mathbb{F}_q$ without constant terms has a non-trivial common zero $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$ if the number of variables n exceeds the sum of the degrees $\sum\limits_j \deg(f_j)$. Note that the set of polynomials $\{x_1, \ldots, x_n\} \in \mathbb{F}_q[x_1, \ldots, x_n]$ only has the trivial common zero. The purpose behind the theorem was to establish that any such set of polynomials with a trivial solution must have at least one non-trivial solution. Warning [10] in 1935 was able to expand upon the result and discovered that the number of solutions must be divisible by the characteristic of $\mathbb{F}_q$. We first will prove the Chevalley-Warning Theorem for a single polynomial:

Theorem 1.1. *Let q be a prime power, and let $f\,(\vec{x}) \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial of degree d. Let N_f denote the number of distinct roots of $f\,(\vec{x})$ in $\mathbb{F}_q^n$. If $n > d$, then*

$\operatorname{char}(\mathbb{F}_q) \,|N_f$.

We will roughly follow the proof of the Chevalley-Warning Theorem from Ireland and Rosen [7] and Greenburg [5]. First, we must establish an important property.

Lemma 1.2. *Let $m \geq 0$. Then in the field $\mathbb{F}_q$, we have*

$$\sum_{x \in \mathbb{F}_q} x^m = \begin{cases} 0, & \textit{if } m = 0, \\ -1, & \textit{if } (q-1)\,|m \textit{ and } m > 0, \\ 0, & \textit{if } (q-1) \nmid m. \end{cases}$$

Proof. Trivially, we have that $\sum_{x \in \mathbb{F}_q} x^0 = q = 0$. Suppose $m = (q-1)\,k$ where $k \in \mathbb{N}$. Then by Lagrange's Theorem, we have

$$x^m = x^{(q-1)k} = \begin{cases} 1, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0. \end{cases}$$

Thus, $\sum_{x \in \mathbb{F}_q} x^m = q - 1 = -1$ in $\mathbb{F}_q$. Lastly, suppose $(q-1) \nmid m$. Then, there is some element $y \in \mathbb{F}_q \backslash \{0\}$ such that $y^m \neq 1$ in $\mathbb{F}_q$. Let $z = xy^{-1}$. Thus, by rearranging variables, we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_q^\times} x^m &= \sum_{z \in \mathbb{F}_q^\times} (yz)^m \\ &= y^m \sum_{z \in \mathbb{F}_q^\times} z^m \\ &= y^m \sum_{x \in \mathbb{F}_q^\times} x^m. \end{aligned}$$

Thus, $(y^m - 1) \sum_{x \in \mathbb{F}_q^\times} x^m = 0$. Since $y^m \neq 1$, necessarily $\sum_{x \in \mathbb{F}_q^\times} x^m = 0$ in $\mathbb{F}_q$. Therefore, we have shown that

$$\sum_{x\in\mathbb{F}_q} x^m = \begin{cases} 0, & \text{if } m = 0, \\ -1, & \text{if } (q-1)\,|m \text{ and } m > 0, \\ 0, & \text{if } (q-1) \nmid m. \end{cases}$$

□

Now, we shall prove Theorem 1.1.

Proof. Let $\mathrm{char}(\mathbb{F}_q) = p$. Notice that in $\mathbb{F}_q$, by Lagrange's Theorem we have

$$1 - f(\vec{x})^{q-1} = \begin{cases} 1, & \text{if } f(\vec{x}) = 0, \\ 0, & \text{if } f(\vec{x}) \neq 0. \end{cases}$$

Thus,

$$\begin{aligned} N_f &= \sum_{\vec{x}\in\mathbb{F}_q^n} \left(1 - f(\vec{x})^{q-1}\right) \\ &\equiv q^n - \sum_{\vec{x}\in\mathbb{F}_q^n} f(\vec{x})^{q-1} \\ &\equiv - \sum_{\vec{x}\in\mathbb{F}_q^n} f(\vec{x})^{q-1} \pmod{p}. \end{aligned}$$

Then, if $\sum_{\vec{x}\in\mathbb{F}_q^n} f(\vec{x})^{q-1} \equiv 0 \pmod{p}$, we will have that $N_f = pm$ for some $m \in \mathbb{N}\cup\{0\}$.

Since the degree of the polynomial $f(\vec{x})$ is d, then $f(\vec{x})^{q-1}$ is a polynomial of degree $d(q-1)$. Thus, we can write $f(\vec{x})$ as an $\mathbb{F}_q$-linear combination of monomials $x_1^{i_1}\cdots x_n^{i_n}$ where $0 \leq i_1 + \cdots + i_n \leq d(q-1)$. Consider such a monomial $x_1^{i_1}\cdots x_n^{i_n}$. If $i_j \geq q-1$ for all $j \in \{1,\ldots,n\}$, then we would have $i_1 + \cdots + i_n \geq n(q-1) > d(q-1)$, which is a contradiction. Therefore, necessarily there exists some i_j such that $i_j < q-1$. For $0 \leq i_j < q-1$, by Lemma 1.2, we have $\sum_{x_j \in \mathbb{F}_q^n} x_j^{i_j} \equiv 0 \pmod{p}$. Then,

$$\sum_{\vec{x} \in \mathbb{F}_q^n} x_1^{i_1} \cdots x_n^{i_n} = \prod_{\ell=1}^{n} \sum_{x_\ell \in \mathbb{F}_q} x_\ell^{i_\ell} \equiv 0 \pmod{p}$$

since when $\ell = j$, the sum is 0. Therefore, since the sum over each such monomial is congruent to $0 \pmod{p}$, we have $N_f \equiv \sum_{\vec{x} \in \mathbb{F}_q^n} f(\vec{x})^{q-1} \equiv 0 \pmod{p}$. □

We can expand upon this result to handle systems of polynomials.

Theorem 1.3. *Let q be a prime power. Let $g_1(\vec{x}), \ldots, g_m(\vec{x}) \in \mathbb{F}_q[x_1, \ldots, x_n]$ be polynomials with $\deg(g_i) = d_i$ for $1 \leq i \leq m$, and let $N_{\vec{g}}$ denote the number of distinct common zeros for the system of polynomials $g_1, \ldots, g_m$. Assume that $n > \sum_{i=1}^{m} d_i$. Then, $\mathrm{char}(\mathbb{F}_q) \,|\, N_{\vec{g}}$.*

Proof. Let $\mathrm{char}(\mathbb{F}_q) = p$. Notice that in $\mathbb{F}_q$, by Lagrange's Theorem we have for $1 \leq j \leq m$ that

$$1 - g_j(\vec{x})^{q-1} = \begin{cases} 1, & \text{if } g_j(\vec{x}) = 0, \\ 0, & \text{if } g_j(\vec{x}) \neq 0. \end{cases}$$

Then,

$$h(\vec{x}) := \prod_{j=1}^{m} \left(1 - g_j(\vec{x})^{q-1}\right) = \begin{cases} 1, & \text{when all } g_j(\vec{x}) = 0 \\ 0, & \text{if any } g_j(\vec{x}) \neq 0. \end{cases}$$

Thus, in $\mathbb{F}_q$,

$$N_{\vec{g}} = \sum_{\vec{x} \in \mathbb{F}_q^n} h(\vec{x}).$$

Since $h(\vec{x})$ is a polynomial of degree $(q-1)\sum_{j=1}^{m} d_j$, we can write $h(\vec{x})$ as an $\mathbb{F}_q$-linear combination of monomials $x_1^{i_1}\cdots x_m^{i_m}$, where $0 \leq i_1 + \cdots + i_n \leq (q-1)\sum_{j=1}^{m} d_j$. Suppose that $x_1^{i_1}\cdots x_n^{i_n}$ is such a monomial. If $i_j \geq q-1$ for all $0 \leq j \leq n$, then we would have $i_1 + \cdots + i_n \geq n\,(q-1) > (q-1)\sum_{j=1}^{m} d_j$, which is a contradiction. Therefore, necessarily there exists some i_j such that $i_j < q-1$. By Lemma 1.2, we have

$$\sum_{\vec{x}\in\mathbb{F}_q^n} x_1^{i_1}\cdots x_n^{i_n} = \prod_{\ell=1}^{n}\sum_{x_\ell\in\mathbb{F}_q} x_\ell^{i_\ell} = 0$$

in $\mathbb{F}_q$. Thus, $N_{\vec{g}} \equiv 0 \pmod{p}$. $\square$

Chapter 2

Combinatorial Nullstellensatz

Many mathematicians continued to improve upon the Chevalley-Warning Theorem over time. We will discuss one of these generalizations in the next section, but first it is important to lay a foundation for how this expansion was proved.

The original Nullstellensatz Theorem was first proved in 1893 by David Hilbert [6].

Theorem 2.1. *Let k be a field. Let I be an ideal in the polynomial ring $k[x_1, \ldots, x_n]$ such that the algebraic set $V(I)$ consists of all n-tuples $\vec{x} = (x_1, \ldots, x_n)$ such that $f(\vec{x}) = 0$ for all $f \in I$. If p is some polynomial in $k[x_1, \ldots, x_n]$ that vanishes on $V(I)$, i.e., $p(\vec{x}) = 0$ for all $\vec{x} \in V(I)$, then there exists $r \in \mathbb{N}$ such that $p^r \in I$.*

His result was expanded upon by several mathematicians; notably, Noga Alon [1] in 1999 proved two variations. The first version of the Combinatorial Nullstellensatz states the following:

Theorem 2.2. *Let k be a field and $g(\vec{x}) \in k[x_0, \ldots, x_n]$. Let $S_1, \ldots, S_n$ be non-empty subsets of k and $f_i(x_i) = \prod_{s \in S_i} (x_i - s)$ for $1 \le i \le n$. If $g(s_1, \ldots, s_n) = 0$ for all $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, then for $1 \le i \le n$ there exists $h_i(\vec{x}) \in k[x_1, \ldots, x_n]$ with deg$(h_i) \le$ deg$(g) -$ deg(f_i) and*

$$g(\vec{x}) = h_1(\vec{x}) f(\vec{x}) + \cdots + h_n(\vec{x}) f_n(\vec{x}).$$

The second version of the Combinatorial Nullstellensatz by Alon, stated below, has more direct applications to the Chevalley-Warning Theorem. In fact, Alon's paper used it to provide a new proof of Theorem 1.3. We will roughly follow the proof by Tao [9].

Theorem 2.3. *Let K be a field, $d_1, \ldots, d_n$ be nonnegative integers, and $p(\vec{x}) \in K[x_1, \ldots, x_n]$ be a polynomial of degree $d_1 + \ldots + d_n$ with a nonzero coefficient on $x_1^{d_1} \cdots x_n^{d_n}$. Then, $p(\vec{x})$ cannot vanish on a set $E_1 \times \cdots \times E_n \subseteq K^n$ with $|E_i| > d_i$ for all $i \in \{1, \ldots, n\}$.*

Proof. For $1 \leq i \leq n$, since $|E_i| > d_i$, we can assume that $|E_i| = d_i + 1$. Consider a set $E = \{e_1, \ldots, e_{d+1}\} \subseteq K$, where $|E| = d + 1$. Consider the matrix

$$\begin{pmatrix} e_1^d & \cdots & e_{d+1}^d \\ e_1^{d-1} & \cdots & e_{d+1}^{d-1} \\ \vdots & \ddots & \vdots \\ e_1 & \cdots & e_{d+1} \\ 1 & \cdots & 1 \end{pmatrix}.$$

Because a nonzero polynomial over a field cannot have more roots than its degree, there cannot exist a nonzero polynomial $a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$ that is in $K[x]$ with zeros $e_1, \ldots, e_{d+1}$. Thus, there cannot exist a nonzero vector $\begin{pmatrix} a_d & \cdots & a_0 \end{pmatrix} \in K^{d+1}$ with

$$\begin{pmatrix} a_d & \cdots & a_0 \end{pmatrix} \begin{pmatrix} e_1^d & \cdots & e_{d+1}^d \\ e_1^{d-1} & \cdots & e_{d+1}^{d-1} \\ \vdots & \ddots & \vdots \\ e_1 & \cdots & e_{d+1} \\ 1 & \cdots & 1 \end{pmatrix} = \vec{0}.$$

Therefore, the rows are linearly independent in this $(d+1) \times (d+1)$ matrix. Since combinations of these linearly independent columns can form any vector, we can find $f(e_1), \ldots, f(e_{d+1}) \in$

K that solves the system

$$\begin{pmatrix} e_1^d & \cdots & e_{d+1}^d \\ e_1^{d-1} & \cdots & e_{d+1}^{d-1} \\ \vdots & \ddots & \vdots \\ e_1 & \cdots & e_{d+1} \\ 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} f(e_1) \\ f(e_2) \\ \vdots \\ f(e_d) \\ f(e_{d+1}) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}.$$

Thus, for $1 \leq i \leq n$, we can find $f_i : E_i \to K$ with

$$\sum_{x_i \in E_i} f_i(x_i)\, x_i^w = \begin{cases} 1, & \text{if } w = d_i, \\ 0, & \text{if } 0 \leq w < d_i, \end{cases}$$

where $|E_i| = d_i + 1$. Also,

$$\begin{aligned} \sum_{\vec{x} \in E_1 \times \cdots \times E_n} f_1(x_1) \cdots f_n(x_n)\, x_1^{w_1} \cdots x_n^{w_n} &= \prod_{i=1}^{n} \sum_{x_i \in E_i} f_i(x_i)\, x_i^{w_i} \\ &= \begin{cases} 1, & \text{when all } w_i = d_i, \\ 0, & \text{if any } 0 \leq w_i < d_i. \end{cases} \end{aligned}$$

Recall that the degree of $p(\vec{x})$ is $d_1 + \cdots + d_n$. Then, let $p(\vec{x}) = \sum_{\vec{w}} a_{\vec{w}} x^{w_1} \cdots x_n^{w_n}$ with $a_{d_1,\ldots,d_n} \neq 0$, and note that for any other nonzero coefficient $a_{\vec{w}}$, we must have $w_\ell < d_\ell$ for some $1 \leq \ell \leq n$. Then,

$$\begin{aligned}
\sum_{\vec{x} \in E_1 \times \cdots \times E_n} f_1(x_1) \cdots f_n(x_n)\, p(\vec{x}) &= \sum_{\vec{x} \in E_1 \times \cdots \times E_n} f_1(x_1) \cdots f_n(x_n) \sum_{\vec{w}} a_{\vec{w}} x_1^{w_1} \cdots x_n^{w_n} \\
&= \sum_{\vec{w}} a_{\vec{w}} \sum_{\vec{x} \in E_1 \times \cdots \times E_n} f_1(x_1) \cdots f_n(x_n)\, x_1^{w_1} \cdots x_n^{w_n} \\
&= a_{d_1, \ldots, d_n} \\
&\neq 0.
\end{aligned}$$

Hence, $p(\vec{x})$ does not vanish on $E_1 \times \cdots \times E_n$. $\square$

Chapter 3

Brink-Schauz Theorem

Using the Combinatorial Nullstellensatz, Schauz [8] in 2008 and Brink [2] in 2011 were able to prove the following generalization of the Chevalley-Warning Theorem.

Theorem 3.1. *Consider the polynomials $f_1(x_1,\ldots,x_n),\ldots,f_r(x_1,\ldots,x_n)$ over the finite field $\mathbb{F}_q$. Let $A_1,\ldots,A_n$ be non-empty subsets of $\mathbb{F}_q$ such that*

$$\sum_{i=1}^{n}\left(|A_i|-1\right) > \sum_{j=1}^{r}\deg\left(f_j\right)(q-1).$$

Then the solution set

$$V = \{\vec{a} \in \prod_{i=1}^{n} A_i \mid f_j(\vec{a}) = 0 \text{ for } 1 \leq j \leq r\}$$

with the variables restricted to the sets A_i is not a singleton.

Here, we will follow the proof provided by Brink [2].

Proof. We will prove this theorem by contradiction. Assume $V = \{\vec{a}\}$ with $\vec{a} = (a_1,\ldots,a_n)$. Also, let $P(\vec{x})$ be defined as $P(\vec{x}) = \prod_{j=1}^{r}\left(1 - f_j(\vec{x})^{q-1}\right)$. Notice for $\vec{x} = \vec{a}$, we have $f_j(\vec{x}) = 0$ for $1 \leq j \leq r$, and thus $P(\vec{x}) = 1$. However, for all $\vec{x} \in \prod_{i=1}^{n} A_i \backslash \{\vec{a}\}$, we have for some

$1 \leq j \leq r$ that $f_j(\vec{x}) \neq 0$, so $f_j(\vec{x})^{q-1} = 1$ by Lagrange's Theorem, making $P(\vec{x}) = 0$. Therefore, we have

$$P(\vec{x}) = \begin{cases} 1, & \text{for } \vec{x} = \vec{a}, \\ 0, & \text{for } \vec{x} \in \prod_{i=1}^{n} A_i \backslash \{\vec{a}\}. \end{cases}$$

Next, let $Q(\vec{x})$ be defined as $Q(\vec{x}) = \displaystyle\prod_{i=1}^{n} \prod_{b \in A_i \backslash \{a_i\}} (x_i - b)$. For $1 \leq i \leq n$, $a_i - b \neq 0$ for $b \in A_i \backslash \{a_i\}$, and thus we have $Q(\vec{a}) = \delta$, where δ is some nonzero value in $\mathbb{F}_q$. However, for all $\vec{x} \in \prod_{i=1}^{n} A_i \backslash \{\vec{a}\}$, we will necessarily have that $x_j \in A_j \backslash \{a_j\}$ for some $1 \leq j \leq n$, making $Q(\vec{x}) = 0$. Therefore,

$$Q(\vec{x}) = \begin{cases} \delta, & \text{if } \vec{x} = \vec{a}, \\ 0, & \text{if } \vec{x} \in \displaystyle\prod_{i=1}^{n} A_i \backslash \{\vec{a}\}. \end{cases}$$

Notice that $Q(\vec{x}) - \delta P(\vec{x}) = 0$ for all $\vec{x} \in \displaystyle\prod_{i=1}^{n} A_i$. However, because

$$\sum_{i=1}^{n} (|A_i| - 1) > \sum_{j=1}^{r} \deg(f_j)(q-1),$$

the monomial of maximal degree in $Q(\vec{x}) - \delta P(\vec{x})$ is $x_1^{|A_1|-1} \cdots x_n^{|A_n|-1}$. This contradicts Theorem 2.3 since $Q(\vec{x}) - \delta P(\vec{x})$ vanishes on $\displaystyle\prod_{i=1}^{n} A_i$. Thus, the solution set V with variables restricted to the sets A_i is not a singleton. $\square$

Bibliography

[1] Noga Alon. Combinatorial Nullstellensatz. volume 8, pages 7–29. 1999. Recent trends in combinatorics (Mátraháza, 1995).

[2] David Brink. Chevalley's theorem with restricted variables. *Combinatorica*, 31(1):127–130, 2011.

[3] Claude Chevalley. Démonstration d'une hypothèse de M. Artin. *Abh. Math. Sem. Univ. Hamburg*, 11(1):73–75, 1935.

[4] Pete L. Clark. Number theory: A contemporary introduction. Accessed: 02/20/2025.

[5] Marvin J. Greenberg. *Lectures on forms in many variables.* W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[6] David Hilbert. Ueber die vollen Invariantensysteme. *Math. Ann.*, 42(3):313–373, 1893.

[7] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1990.

[8] Uwe Schauz. Algebraically solvable problems: describing polynomials as equivalent to explicit solutions. *Electron. J. Combin.*, 15(1):Research Paper 10, 35, 2008.

[9] Terence Tao. Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. *EMS Surv. Math. Sci.*, 1(1):1–46, 2014.

[10] Ewald Warning. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. *Abh. Math. Sem. Univ. Hamburg*, 11(1):76–83, 1935.