A New Proof of Warning’s Second Theorem

Shamil Asgarli

Abstract. We give an elementary proof of Warning’s second theorem on the number of solutions to the system of polynomial equations over finite fields.

1. INTRODUCTION. A basic result in linear algebra states that if a system of $r$ linear equations in $n$ variables has a solution, and $n > r$, then the system has another solution. It is natural to ask if this statement extends to a higher degree system of polynomials. The following result was conjectured by Emil Artin and was first proved by Chevalley [3].

Theorem 0. Let $q = p^k$ be a prime power. Suppose that $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ are polynomials such that

$$n > \sum_{i=1}^{r} \deg(f_i).$$

Let $Z = \{ \mathbf{a} \in \mathbb{F}_q^n : f_i(\mathbf{a}) = 0 \text{ for each } i \}$ be the common zero locus. If $Z \neq \emptyset$, then $\#Z \geq 2$.

Around the same time, Warning [9] strengthened Chevalley’s theorem in two directions. Using the same hypothesis as above, we can state them as follows:

Theorem 1 (Warning’s first theorem). $p \mid \#Z$.

Theorem 2 (Warning’s second theorem). If $Z \neq \emptyset$, then $\#Z \geq q^{n-d}$, where $d = \sum_{i=1}^{r} \deg(f_i)$.

The analogue of this in linear algebra (when $\deg f_i = 1$ for all $i$) is well known: if a system of $r$ linear equations in $n$ variables has a solution with $n > r$, then the solution set is at least $(n - r)$-dimensional.

There are stronger results regarding divisibility of the number of solutions, originating in the work of Ax [2]. Under the same hypothesis as above, Ax proved that $q^b \mid \#Z$ whenever $n > b \sum_{i=1}^{r} \deg(f_i)$. In particular, we get that $q \mid \#Z$ in all cases, which is a deeper result than Theorem 1. This theorem was later strengthened by Katz [7].

It is also worth mentioning the rich combinatorial aspects of these results. First, Chevalley’s theorem has a proof using Alon’s combinatorial Nullstellensatz [1]. By refining this method, Clark [4] proved a restricted-variable generalization of Theorem 1. In the same spirit, Theorem 2 has been vastly generalized in [5].

The main goal of this note is to give an elementary proof of Theorem 2 using a counting argument. The key ingredient is a certain incidence correspondence between the points and hyperplanes in $\mathbb{F}_q^n$. We should mention that Warning’s original proof used a different counting argument, which was recently refined by Heath-Brown [6]. In fact, Warning’s proof of Theorem 2 worked over $\mathbb{F}_q$ directly, while ours works only over $\mathbb{F}_p$ (see Section 3). In Section 4, we explain how to get the statement over $\mathbb{F}_q$ using restriction of scalars.
2. WARNING’S FIRST THEOREM. In our proof of Theorem 2 (see Section 3), we will need Theorem 1 as the base case of the induction. To make the exposition self-contained, we include the proof of Theorem 1 below. This proof is adapted from the one in [2].

Proof of Theorem 1. Let \( f_1, f_2, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n] \) be polynomials satisfying \( \sum_{i=1}^r \deg(f_i) < n \). For any \( a \in \mathbb{F}_q^n \), we have

\[
 f_i(a)^{q-1} = \begin{cases} 
 1 & \text{if } f_i(a) \neq 0, \\
 0 & \text{if } f_i(a) = 0. 
\end{cases}
\]

As a result, the quantity

\[
 N(f_1, \ldots, f_r) = \sum_{a \in \mathbb{F}_q^n} \prod_{i=1}^r (1 - f_i(a)^{q-1})
\]

counts the cardinality of \( Z = \{ a \in \mathbb{F}_q^n : f_i(a) = 0 \text{ for each } i \} \) modulo \( p \). The polynomial \( \prod_{i=1}^r (1 - f_i(x)^{q-1}) \) is a linear combination of monomials \( x^u = x_1^{u_1}x_2^{u_2} \cdots x_n^{u_n} \) with degree at most \( (q-1) \sum_{i=1}^r \deg(f_i) < n(q-1) \). For each such monomial \( x^u \),

\[
 \sum_{a \in \mathbb{F}_q^n} a^u = \prod_{i=1}^n \sum_{a_i \in \mathbb{F}_q} a_i^{u_i} = \prod_{i=1}^n Y(u_i),
\]

where \( Y(u_i) := \sum_{a_i \in \mathbb{F}_q} a_i^{u_i} \). If \( u_i \) is a positive multiple of \( q-1 \), then \( Y(u_i) = q-1 \). Otherwise, we can find some \( b \in \mathbb{F}_q^* \) with \( b^{u_i} \neq 1 \). Then

\[
 Y(u_i) = \sum_{a_i \in \mathbb{F}_q} a_i^{u_i} = \sum_{a_i \in \mathbb{F}_q} (ba_i)^{u_i} = b^{u_i} \sum_{a_i \in \mathbb{F}_q} a_i^{u_i} = b^{u_i}Y(u_i)
\]

so that \( Y(u_i) = 0 \). Consequently,

\[
 Y(u_i) = \begin{cases} 
 q-1 & \text{if } u_i \text{ is a positive multiple of } q-1, \\
 0 & \text{otherwise}. 
\end{cases}
\]

Since \( (q-1) \sum_{i=1}^r \deg(f_i) < n(q-1) \), at least one \( u_i \) is smaller than \( q-1 \). Therefore, \( \sum_{a \in \mathbb{F}_q^n} a^u = 0 \) and so \( N(f_1, \ldots, f_r) = 0 \), implying that \( p \mid \#Z \).  

3. WARNING’S SECOND THEOREM (SPECIAL CASE). The goal of this section is to prove Warning’s second theorem in the special case when \( q = p \) is a prime number.

Proof of Theorem 2 (special case \( q = p \)). Let \( m = n - \sum_{i=1}^r \deg(f_i) \). By hypothesis, \( m > 0 \). We want to show that if a system of equations \( f_1 = f_2 = \cdots = f_r = 0 \) has a solution, then it has at least \( p^m \) solutions. We will proceed by induction on \( m \). After translating the variables, we may assume that \( f_1(0) = \cdots = f_{\ell}(0) = 0 \), because the degrees of \( f_i \) and the size of the zero locus of \( \{ f_i \}_{i=1}^r \) do not change after a linear change of variables.

Base case \( m = 1 \). By Theorem 1, \( p \mid \#Z \). Since \( 0 \in Z \), we get \( \#Z \geq p \).

Inductive step. Assume \( m \geq 2 \) and suppose the result is true for \( m - 1 \).
Before we delve into the proof, we need a few preliminaries. A hyperplane \( H \) is a codimension one \( \mathbb{F}_p \)-subspace of \( \mathbb{F}_p^n \). Each hyperplane \( H \) is the zero locus of some nonzero homogeneous linear polynomial \( L_H \). Note that \( L_H \) is unique up to scaling. As a result, there are \( \frac{p^n - 1}{p-1} \) hyperplanes in \( \mathbb{F}_p^n \). For a given hyperplane \( H \), let

\[
Z_H = \{ a \in \mathbb{F}_p^n \mid f_1(a) = \cdots = f_r(a) = L_H(a) = 0 \}.
\]

For the new system \( f_1, \ldots, f_r, L_H \), we have

\[
n - \sum_{i=1}^r \deg(f_i) - 1 = m - 1.
\]

The induction hypothesis implies that \( \#Z_H \geq p^{m-1} \).

Let \( S = Z \setminus \{(0, \ldots, 0)\} \). If \( \#S \geq p^m - p \), then \( \#Z \geq p^m - p \), which combined with \( p \mid \#Z \) implies the desired result \( \#Z \geq p^m \). Assume, to the contrary, that \( \#S < p^m - p \).

In fact, we will assume that \( \#S \leq p^m - p \). Consider the incidence set

\[
E = \{(x, H) \mid x \in S \text{ and } H \text{ hyperplane with } x \in H \}.
\]

Let us count \( E \) in two different ways. For a fixed \( x \in S \), the number of \( (x, H) \in E \) can be at most the number of hyperplanes \( H \) containing \( x \). The latter is the same as the number of hyperplanes in the quotient space \( \mathbb{F}_p^n / \langle x \rangle \) which has dimension \( n - 1 \). So each \( x \in S \) contributes at most \( \frac{p^{n-1} - 1}{p-1} \) elements to \( E \). Since \( \#S \leq p^m - p \), we obtain

\[
\#E \leq (p^m - p) \frac{p^{n-1} - 1}{p-1}. \tag{1}
\]

On the other hand, as we saw above, each hyperplane \( H \) satisfies \( \#Z_H \geq p^{m-1} \), and so it contributes at least \( p^{m-1} - 1 \) elements to \( E \). This gives us

\[
\#E \geq (p^{m-1} - 1) \frac{p^n - 1}{p-1}. \tag{2}
\]

Combining the inequalities (1) and (2), we get

\[
(p^m - p) \frac{p^{n-1} - 1}{p-1} \geq (p^{m-1} - 1) \frac{p^n - 1}{p-1}.
\]

After dividing both sides by \( p^{m-1} - 1 \) (which is allowed since \( m \geq 2 \)), this becomes

\[
\frac{p(p^{n-1} - 1)}{p-1} \geq \frac{p^n - 1}{p-1},
\]

that is, \( p^n - p \geq p^n - 1 \), which is a contradiction. \( \blacksquare \)
4. WARNING’S SECOND THEOREM (GENERAL CASE). It turns out that Warning’s second theorem over $\mathbb{F}_q$ implies Warning’s second theorem over $\mathbb{F}_p$. This type of reduction was used in [8] in a more general setting, where the degrees are replaced by their $p$-weights. In our situation, the proof is an example of a “restriction of scalars” argument. We are grateful to the referee for explaining this step.

Proof of Theorem 2 (general case). Suppose $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ and $n > \sum_{i=1}^r \deg(f_i)$. We can view $\mathbb{F}_q = \mathbb{F}_p^k$ as a $k$-dimensional vector space over $\mathbb{F}_p$. Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be a basis for this vector space. Next, formally replace each $x_i$ with $\sum_{j=1}^k \alpha_j x_{ij}$. If $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, then $f = 0$ becomes

$$f \left( \sum_{j=1}^k \alpha_j x_{1j}, \ldots, \sum_{j=1}^k \alpha_j x_{nj} \right) = 0.$$  

After expanding the polynomial and collecting the coefficients, this equation can be written as $\alpha_1 g_1((x_{ij})) + \cdots + \alpha_k g_k((x_{ij})) = 0$, where each $g_j((x_{ij}))$ is a polynomial in variables $x_{ij}$ with coefficients in $\mathbb{F}_p$. As a result, $\{a \in \mathbb{F}_q^n : f(a) = 0\}$ is in bijection with the set $\{b \in \mathbb{F}_p^k : g_j(b) = 0 \text{ for each } j = 1, \ldots, k\}$. By the same reasoning,

$$Z = \{a \in \mathbb{F}_q^n : f_i(a) = 0 \text{ for each } i = 1, \ldots, r\}$$

is in bijection with

$$Z' = \{b \in \mathbb{F}_p^r : g^{(i)}_j(b) = 0 \text{ for each } j = 1, \ldots, k \text{ and for each } i = 1, \ldots, r\},$$

where $\{g^{(i)}_j\}_{i=1}^r \text{ and } j=1}^k$ is a collection of $kr$ polynomials in $kn$ variables over $\mathbb{F}_p$. Note that

$$\sum_{i=1}^r \sum_{j=1}^k \deg g^{(i)}_j = \sum_{i=1}^r \sum_{j=1}^k \deg f_i = kd,$$

where $d = \sum_{i=1}^r \deg f_i$. By Theorem 2 (over $\mathbb{F}_p$), $\#Z'$ is at least $p^{kn-kd} = q^{n-kd}$. \qed

ACKNOWLEDGMENTS. I would like to thank my advisor Brendan Hassett for reading and checking the proof. I also owe thanks to Peter McGrath, who first encouraged me to publish this note. Finally, I am grateful to the two anonymous referees for providing me with such detailed and insightful reports.

REFERENCES


© THE MATHEMATICAL ASSOCIATION OF AMERICA [Monthly 125]
A Short Proof That Lebesgue Outer Measure of an Interval Is Its Length

The Lebesgue outer measure $m^*(E)$ of a subset $E$ of the real line is defined as $m^*(E) := \inf\{\sum_{k=1}^{\infty} \ell(I_k) \mid E \subseteq \bigcup_{k=1}^{\infty} I_k\}$, where each $I_k$ is an open interval and $\ell(I_k)$ is its length. Establishing one of the inequalities in the standard proof of the fact in the title above turns out to be tedious in [1, p.31]. Using the connectedness of the interval shortens the proof as follows.

Proof. Given two real numbers $a$ and $b$ with $a < b$, it is enough to prove that $m^*([a, b]) = b - a$. Clearly, $m^*([a, b]) \leq b - a$. Now let $[a, b] \subset \bigcup_{k=1}^{n} I_k$ for some positive integer $n$, which is always possible since $[a, b]$ is compact. Without loss of generality, assume that the set $[a, b] \cap I_k$ is nonempty for each $k$. Observe that the set $\bigcup_{k=1}^{n} I_k$ is connected. (Otherwise, if $(P, Q)$ is its separation, then for each $k$, by connectedness of $I_k$, either $I_k \subset P$ or $I_k \subset Q$. Thus each of $P$ and $Q$ is equal to union of sets from the list $\{I_1, \ldots, I_n\}$. So the pair $(P \cap [a, b], Q \cap [a, b])$ determines a separation of $[a, b]$, which contradicts connectedness of $[a, b]$.) So $\bigcup_{k=1}^{n} I_k$ is an open interval containing $[a, b]$. Thus, $b - a \leq \ell(\bigcup_{k=1}^{n} I_k) \leq \sum_{k=1}^{n} \ell(I_k)$, where the last inequality holds since some intervals overlap. Hence, $b - a \leq m^*([a, b])$. ■

REFERENCES


—Submitted by Jitender Singh, Guru Nanak Dev University Amritsar, India

doi.org/10.1080/00029890.2018.1452512
MSC: Primary 28A12