CHEVALLEY-WARNING AT THE BOUNDARY

PETE L. CLARK, TYLER GENAO, AND FREDERICK SAIA

Abstract. The Chevalley-Warning Theorem is a result on the solution set of a system of polynomial equations $f_1, \ldots, f_r$ in n variables over a finite field $\mathbb{F}_q$ in the low degree case $d := \sum_{j=1}^{r} \deg(f_j) < n$. In this note we reformulate that result in terms of fibers of the associated polynomial map and, following Heath-Brown, show that something weaker continues to hold when $d = n$. This result invites a search for homogeneous degree n polynomials in n variables over $\mathbb{F}_q$ for which the associated polynomial function $\mathbb{F}_q^n \to \mathbb{F}_q$ is not surjective, and we exhibit several families of such polynomials.

Contents

1. Chevalley-Warning

Let p be a prime number, let $a \in \mathbb{Z}^+$ be a positive integer, and put $q = p^a$. Let $\mathbb{F}_q$ be "the" (unique, up to isomorphism) finite field of order q. Let $\mathbb{F}_q[t_1, \ldots, t_n]$ be the ring of polynomials in variables $t_1, \ldots, t_n$ with coefficients in $\mathbb{F}_q$: the elements are finite formal $\mathbb{F}_q$-linear combinations of monomials $t_1^{a_1} \cdots t_n^{a_n}$. The degree of such a monomial is $a_1 + \ldots + a_n$, and the degree of a nonzero polynomial is the maximum degree of a monomial term that appears with nonzero coefficient. There are differing conventions on the degree of the zero polynomial: here, we define $\deg 0 = 0$, so that the degree zero polynomials are precisely the elements of $\mathbb{F}_q$.

Theorem 1.1 (Chevalley-Warning)**.** *Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials of degrees $d_1, \ldots, d_r \in \mathbb{Z}^+$ and suppose that $d := \sum_{j=1}^{r} d_j < n$. Let*

$$Z = Z(f_1, \ldots, f_r) := \{x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid f_1(x) = \ldots = f_r(x) = 0\}$$

be the solution set of the polynomial system. Then $p \mid \#Z$.

Proof. (Ax [Ax64]) If $x \in \mathbb{F}_q$, then $x^{q-1} = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$. It follows that taking

$$\chi := \prod_{j=1}^{r} (1 - f_j^{q-1}) \in \mathbb{F}_q[t_1, \ldots, t_n],$$

then for all $x \in \mathbb{F}_q^n$ we have $\chi(x) = \begin{cases} 1 & x \in Z \\ 0 & x \notin Z \end{cases}$. So as elements of $\mathbb{F}_q$ we have

$$\sum_{x \in \mathbb{F}_q} \chi(x) = \#Z.$$

Since $\mathbb{F}_q$ has characteristic p, we see that $p \mid \#Z$ holds iff $\sum_{x \in \mathbb{F}_q} \chi(x) = 0$. Moreover

$$\deg \chi = \sum_{j=1}^{r} \deg(1 - f_j^{q-1}) = (q-1) \sum_{j=1}^{r} d_j < (q-1)n.$$

We claim that for any polynomial $P \in \mathbb{F}_q[t_1, \ldots, t_n]$ of degree less than $(q-1)n$ we have $\sum_{x \in \mathbb{F}_q^n} P(x) = 0$, which will suffice to complete the proof. To establish the claim, we first observe that

$$P \in \mathbb{F}_q[t_1, \ldots, t_n] \mapsto \sum_{x \in \mathbb{F}_q} P(x) \in \mathbb{F}_q$$

is $\mathbb{F}_q$-linear, so it's enough to show the result for a monomial $t_1^{a_1} \cdots t_n^{a_n}$ of degree less than $(q-1)n$. We have

$$\sum_{x \in \mathbb{F}_q^n} x_1^{a_1} \cdots x_n^{a_n} = (\sum_{x_1 \in \mathbb{F}_q} x_1^{a_1}) \cdots (\sum_{x_n \in \mathbb{F}_q} x_n^{a_n}).$$

If $a_1 + \ldots + a_n = \deg(t_1^{a_1} \cdots t_n^{a_n}) < (q-1)n$, then we must have $a_i < q-1$ for some i, so it's enough to show that if $0 \leq a_i \leq q-2$ then we have $\sum_{x_i \in \mathbb{F}_q} x_i^{a_i} = 0$. If $a_i = 0$ then this sum is q, which is 0 in $\mathbb{F}_q$, so suppose that $1 \leq a_i \leq q-2$. The group $\mathbb{F}_q^\times$ is cyclic [Cl-NT, Cor. B.10]; let ζ be a generator. Then

$$\sum_{x_i \in \mathbb{F}_q} x_i^{a_i} = \sum_{k=0}^{q-2} (\zeta^k)^{a_i} = \frac{(\zeta^{a_i})^{q-1} - 1}{\zeta^{a_i} - 1} = 0. \qquad \square$$

Theorem 1.1 can be viewed as an estimate on the size of $\#Z$, but it is not a usual "Archimedean inequality." Rather it is a "p-adic inequality": namely, for a nonzero ineger n, let $\operatorname{ord}_p(n)$ denote the largest power of p dividing n. Then Theorem 1.1 gives the p-adic inequality $\operatorname{ord}_p(\#Z) \geq 1$. It is thus natural to ask for stronger p-adic inequalities, and we will return to address this later on.

We call Theorem 1.1 the "Chevalley-Warning Theorem" in reference to the papers of Chevalley [Ch35] and Warning [Wa35], published consecutively in the same issue of the same journal. What Chevalley proved is that under the low degree hypothesis $d < n$ we *cannot* have $\#Z = 1$. This is already significant: if each f_j is moreover homogeneous – that is, every nonzero monomial term has the same total degree – then the system has the trivial solution $0 = (0, \ldots, 0) \in \mathbb{F}_q^n$, so Chevalley's result asserts the existence of a nontrivial solution. Specializing further to $r = 1$, we get that a homogeneous polynomial over $\mathbb{F}_q$ in more variables than its degree has a nontrivial solution, proving a conjecture made by Dickson [Di09] and Artin.[1]

The p-divisibility refinement was contributed by Warning, but this stronger conclusion comes just from looking more carefully at Chevalley's proof. See for instance [Cl-NT, §14.2] for an exposition of Chevalley's argument adapted to prove Theorem 1.1. Warning's real contribution in [Wa35] was the following result,[2] which (almost!) gives a more traditional Archimedean inequality on $\#Z$.

Theorem 1.2 (Warning II)**.** *Under the hypotheses of Theorem 1.1, we have $Z = \varnothing$ or $Z \geq q^{n-d}$.*

We said "almost" because Theorem 1.2 allows Z to be empty. So does Theorem 1.1, as 0 is zero modulo p. This is as it must be, for as soon as $d \geq 2$, the set Z can indeed be empty. If $d_j \geq 2$ for some $1 \leq j \leq r$, let $f_j \in \mathbb{F}_q[t_1]$ be irreducible; otherwise we have $d_1 = \cdots = d_r = 1$ with $r \geq 2$, and we take $f_1 = t_1$, $f_2 = t_1 + 1$.

Every proof of Theorem 1.1 that we know uses the "Chevalley polynomial"

$$\chi = \prod_{j=1}^{r}(1 - f_j^{q-1}).$$

Chevalley's original proof exploits the interplay between polynomials and polynomial functions and can be seen as a precursor to Alon's Combinatorial Nullstellensatz [Al99]. Ax's proof (the one we have given) is a thing of wonder that is not of the one-hit variety. His idea can be used to prove other results of Chevalley-Warning type: see e.g. [BBC19, §4].

Theorem 1.2 is not as well known as the Chevalley-Warning Theorem. We will not prove it here, though the idea behind our main result can be traced back to Warning's proof of Theorem 1.2. A good exposition of this proof can be found in [LN97, pp. 273-275]. Forrow and Schmitt observed that Theorem 1.2 is a consequence of a result of Alon-Füredi on polynomials over an arbitrary field. As shown in [CFS17], this method of proof leads to "restricted variable" generalizations of Theorem 1.2. A third proof of Theorem 1.2 was recently given by Asgarli [As18].

In the case when each polynomial f_j is homogeneous, we can also look at the solution locus in projective space $\mathbb{P}^{n-1}(\mathbb{F}_q)$, which is obtained from $\mathbb{F}_q^n$ by removing $0 = (0, \ldots, 0)$ and quotienting out by the equivalence relation $(x_1, \ldots, x_n) \sim (\lambda x_1, \ldots, \lambda x_n)$ for all $\lambda \in \mathbb{F}_q^\times$. If $P \in \mathbb{F}_q[t_1, \ldots, t_n]$ is homogeneous of degree d then for all $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \setminus \{0\}$ and $\lambda \in \mathbb{F}_q^\times$, we have $P(\lambda x) = \lambda^d P(x)$, and thus whether $P(x) = 0$ depends only on the class of x in $\mathbb{P}^{n-1}(\mathbb{F}_q)$. If we denote by $\mathbb{P}Z$ the solution locus in projective space, then we have

$$\#Z = 1 + (q-1)\#\mathbb{P}Z, \tag{1}$$

so Theorem 1.1 tells us that

$$\#\mathbb{P}Z \equiv 1 \pmod{p}.$$

In the homogeneous case, the low degree condition

$$d = \sum_{j=1}^{r} d_j = \sum_{j=1}^{r} \deg(f_j) < n$$

[1]A field that satisfies this property is called "C_1," so Chevalley proved that finite fields are C_1.

[2]Warning stated Theorem 1.2 for $r = 1$ only, but his proof works verbatim in the general case.

is especially natural. Algebraic geometers will recognize that, in the case that the associated projective variety $V_{/\mathbb{F}_q}$ is smooth, geometrically integral and of dimension $n-1-r$, it holds precisely when V is Fano: a sufficiently negative multiple of the canonical bundle embeds V into projective space. If instead of working over $\mathbb{F}_q$ our polynomials had coefficients in $\mathbb{C}$, the compact complex submanifolds of projective space so obtained would be simply connected with positive sectional curvature.

Still keeping the above "nice" geometric conditions, if in contrast we had $d > n$ then the associated projective variety $V_{/\mathbb{F}_q}$ would be of "general type" and (this is somewhat stronger) a sufficiently positive multiple of the canonical bundle would embed V into projective space. In dimension one over $\mathbb{C}$ these varieties are also characterized by being hyperbolic and by having noncommutative fundamental group.

The condition $d = n$ is an interesting boundary case: again keeping the nice geometric conditions, we get a Calabi-Yau variety, for which the canonical bundle is trivial. In dimension one over $\mathbb{C}$ – e.g. when $(r, n, d) = (1, 3, 3)$ – these are elliptic curves: they have zero sectional curvature and infinite but commutative fundamental group. In dimension two – e.g. when $(r, n, d) = (2, 4, 4)$ – we get K3 surfaces: simply connected Ricci-flat compact complex surfaces (topological 4-manifolds).

These geometric considerations will not be needed later. In fact, it counts among the charms of these Chevalley-Warning results that they do not require the polynomial system to have any nice geometric properties and that the proofs use no algebraic geometry whatseover. However, connections to $\mathbb{F}_q$-points on varieties $V_{/\mathbb{F}_q}$ are part of the reason why mathematicians are interested in these results.

2. At the Boundary

If $d \geq n$, then the conclusion of Theorem 1.1 fails very badly. In fact, for all prime powers q and positive integers $n, r, d_1, \ldots, d_r$ such that $d_1 + \ldots + d_r \geq n$, there are homogeneous polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ of degrees $d_1, \ldots, d_r$ such that $Z(f_1, \ldots, f_r) = \{0\}$. Theorem 1.2 still holds when $d \geq n$ but becomes trivial: in this case, clearly either $Z = \varnothing$ or $\# Z \geq 1 \geq q^{n-d}$.

However, we will now reformulate Theorem 1.1 in such a way that something still holds "on the boundary," i.e., when $d = n$. For $g \in \mathbb{F}_q[t_1, \ldots, t_n]$, let $E(g)$ denote the induced function from $\mathbb{F}_q^n$ to F_q:

$$E(g) : x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \mapsto f(x) \in \mathbb{F}_q.$$

Since we have r polynomials $f_1, \ldots, f_r$, we can build a function

$$E \coloneqq \prod_{j=1}^{r} E(f_j) : \mathbb{F}_q^n \to \mathbb{F}_q^r, \ x \mapsto (f_1(x), \ldots, f_r(x)).$$

The fiber of E over $0 \in \mathbb{F}_q^r$ is $Z = Z(f_1, \ldots, f_r)$, and for any $b = (b_1, \ldots, b_r) \in \mathbb{F}_q^r$, the fiber of E over b is $Z(f_1 - b_1, \ldots, f_r - b_r)$. For all $1 \leq j \leq r$ we have $\deg(f_j - b_j) = \deg(f_j)$. So here is an equivalent **fibered form** of Theorem 1.1:

Theorem 2.1 (Chevalley-Warning Restated)**.** *Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials of degrees $d_1, \ldots, d_r \in \mathbb{Z}^+$, and suppose that $d \coloneqq \sum_{j=1}^r d_j < n$. Then every fiber of $E : \mathbb{F}_q^n \to \mathbb{F}_q^r, \ x \mapsto (f_1(x), \ldots, f_r(x))$ has cardinality divisible by p.*

Now what happens if $d = n$? Here is one easy case to build upon: suppose also that $r = n$ and $d_j = 1$ for all j. Since looking at all fibers of E involves translating by all possible constants anyway, we may assume that each f_j has no constant term, and thus $E : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a linear map. Let R be its rank. If $R = n$ then E is invertible, so each fiber has cardinality 1. If $R < n$ then $W := E^{-1}(0)$ is an $\mathbb{F}_q$-subspace of dimension $n - R \geq 1$. For $b \in \mathbb{F}_q^r$, if $E^{-1}(b)$ is empty then it has cardinality zero modulo p; otherwise there is $x \in \mathbb{F}_q^b$ such that $E(x) = b$ and $E^{-1}(b) = x + W$ has cardinality $\#W = q^{n-R} \equiv 0 \pmod{p}$. Thus we find that the fiber cardinalities need not be 0 modulo p, but they are all the same modulo p.

These considerations serve to motivate the following result.

Theorem 2.2 (Chevalley-Warning at the Boundary, Preliminary Form)**.** *Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials of degrees $d_1, \ldots, d_r \in \mathbb{Z}^+$, and suppose that $d := \sum_{j=1}^r d_j \leq n$. Let $E : \mathbb{F}_q^n \to \mathbb{F}_q^r$, $x \mapsto (f_1(x), \ldots, f_r(x))$ be the associated evaluation map. Then:*

a) *For all $b, c \in \mathbb{F}_q^r$ we have $\#E^{-1}(b) \equiv \#E^{-1}(c) \pmod{p}$.*
b) *If the common fiber cardinality in part a) is nonzero modulo p, then E is surjective.*

In Theorem 2.2, part b) follows immediately from part a): if every fiber has nonzero cardinality modulo p, then every fiber is nonempty, so E is surjective. The key to the proof of Theorem 2.2a) is the following observation of Heath-Brown [HB11].[3]

Lemma 2.3 (Heath-Brown)**.** *Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials of degrees $d_1, \ldots, d_r \in \mathbb{Z}^+$ and suppose that $d := \sum_{j=1}^r d_j \leq n$. For all $1 \leq j \leq r$, let $h_j \in \mathbb{F}_q[t_1, \ldots, t_n]$ be such that $\deg h_j < d_j$. Then we have*

$$\#Z(f_1, \ldots, f_r) \equiv \#Z(f_1 - h_1, \ldots, f_r - h_r) \pmod{p}.$$

Proof. For $1 \leq j \leq r$, we may uniquely write $f_j = F_j + r_j$ where F_j is homogeneous of degree d_j and $\deg r_j < d_j$: indeed F_j is the sum of all the monomial terms of f_j of total degree d_j and r_j is the sum of all the other monomial terms. We also put

$$G_j := t_{n+1}^{d_j} f_j \left(\frac{t_1}{t_{n+1}}, \ldots, \frac{t_n}{t_{n+1}} \right) \in \mathbb{F}_q[t_1, \ldots, t_{n+1}] :$$

in other words, we introduce a new variable t_{n+1} and multiply each monomial term by the non-negative power of t_{n+1} needed to bring the degree of the monomial up to d_j. Thus G_j is homogeneous of degree d_j but in $n + 1$ variables. Put

$$Z := \{x \in \mathbb{F}_q^n \mid f_1(x) = \ldots = f_r(x) = 0\},$$

$$Z_1 := \{x \in \mathbb{F}_q^n \mid F_1(x) = \ldots = F_r(x) = 0\},$$

$$Z_2 := \{(x, y) = (x_1, \ldots, x_n, y) \in \mathbb{F}_q^{n+1} \mid G_1(x, y) = \ldots = G_r(x, y) = 0\}.$$

For $x \in \mathbb{F}_q^n$, we have $x \in Z_1$ iff $(x, 0) \in Z_2$. On the other hand, if $y \neq 0$ then $(x, y) \in Z_2$ iff $(\frac{x}{y}, 1) = (\frac{x_1}{y}, \ldots, \frac{x_n}{y}, 1) \in Z_2$, so there are precisely $q - 1$ times as many elements $(x, y) \in Z_2$ with $y \neq 0$ as there are elements $(x, 1) \in Z_2$. Finally we have $(x, 1) \in Z_2$ iff $x \in Z$. This gives

[3] Heath-Brown establishes Lemma 2.3 *en route* to proving [HB11, Thm. 1], which is a generalization of a lemma that Warning used in his proof of Theorem 1.2.

$$\#Z_2 = (q-1)\#Z + \#Z_1. \tag{2}$$

Theorem 1.1 applies to give $p \mid \#Z_2$. Since $p \mid q$, reducing (2) modulo p, we get

$$\#Z \equiv \#Z_1 \pmod{p}.$$

In other words, after reduction modulo p, the number of solutions to the system $f_1 = \cdots = f_r = 0$ depends only on the highest degree homogeneous parts of the f_j's, which do not change if we adjust each f_j by a polynomial h_j of smaller degree. This establishes the result. □

The proof of Theorem 2.2a) follows immediately from Lemma 2.3: indeed it is the special case of Lemma 2.3 in which each h_j has degree 0.

3. A Generalization and Some Related Results

Let's look more carefully at the case in which the finite field $\mathbb{F}_q$ has composite order: $q > p$. For motivation we considered the case of a linear map $E : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Though we managed not to say so, our analysis showed that all fibers have the same cardinality modulo q, not just modulo p. Moreover, while Theorem 1.1 gives a congruence modulo p, Theorem 1.2 gives an inequality involving q. This makes one wonder: in the setting of Theorem 1.1, must we have $\#Z \equiv 0 \pmod{q}$?

The answer – **yes** – was first shown by Ax in 1964 as part of his study of higher p-adic divisibilities on $\#Z$ [Ax64]. Ax's results are optimal when $r = 1$. For $r \geq 2$ Ax's results are not optimal but nevertheless give $\#Z \equiv 0 \pmod{q}$. For $r \geq 2$ the optimal p-adic divisibilities were given by Katz [Ka71].

Theorem 3.1 (Ax-Katz). *Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials of degrees $d_1 \geq \ldots \geq d_r \geq 1$. Let $b \in \mathbb{Z}^+$ be such that $bd_1 + d_2 + \ldots + d_r < n$. Then $q^b \mid \#Z(f_1, \ldots, f_r)$.*

So if $\sum_{j=1}^r d_j < n$ then in Theorem 3.1 we can take $b = 1$ to get $q \mid \#Z$. Using this we see immediately that the conclusion of Lemma 2.3 can[4] be strengthened to

$$\#Z(f_1, \ldots, f_r) \equiv \#Z(f_1 - g_1, \ldots, f_r - g_r) \pmod{q},$$

which in turn gives a strengthening of Theorem 2.2:

Theorem 3.2 (Chevalley-Warning at the Boundary). *Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials of degrees $d_1, \ldots, d_r \in \mathbb{Z}^+$, and suppose that $d := \sum_{j=1}^r d_j \leq n$. Let $E : \mathbb{F}_q^n \to \mathbb{F}_q^r,\ x \mapsto (f_1(x), \ldots, f_r(x))$ be the evaluation map. Then:*

a) *For all $b, c \in \mathbb{F}_q^r$ we have $\#E^{-1}(b) \equiv \#E^{-1}(c) \pmod{q}$.*
b) *More generally, we do not change any fiber cardinality modulo q if we replace each f_j by $f_j + h_j$ with $\deg h_j < \deg f_j$.*
c) *If the common modulo q fiber cardinality is nonzero, then E is surjective.*

Theorem 3.2 is a generalization of the following 1966 result.

Theorem 3.3 (Terjanian [Te66]). *Let $f \in \mathbb{F}_q[t_1, \ldots, t_n]$ have degree n and suppose that $Z(f) = \{0\}$. For all $g \in \mathbb{F}_q[t_1, \ldots, t_n]$ with $\deg g < n$, there is $x \in \mathbb{F}_q^n$ such that $f(x) = g(x)$. In particular f is surjective.*

[4] And was – this is what Heath-Brown proved in [HB11].

We get Theorem 3.3 by applying Theorem 3.2 (or even Theorem 2.2) with $r = 1$ to the polynomial f: the hypothesis $Z(f) = \{0\}$ means that, even after adjusting by a polynomial h of smaller degree, the common fiber cardinality modulo q is 1, so all fibers of $f-h$ are nonempty. Terjanian's proof is different: he uses Theorem 1.1 and the existence of polynomials of degree q in q variables that have exactly one solution.

Theorem 3.2c) is related to the following result, which we state in "fibered form."

Theorem 3.4 (Aichinger-Moosbauer [AM21])**.** *Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials of positive degree, and for $1 \leq j \leq r$, put $Y_j := E(f_j)(\mathbb{F}_q^n)$. If*

$$\sum_{j=1}^{r} (\#Y_j - 1)\deg(f_j) < (q-1)n, \tag{3}$$

then every fiber of $E : \mathbb{F}_q^n \to \mathbb{F}_q^r$, $x \mapsto (f_j(x))$ has size divisible by p.

Proof. The hypotheses are stable under passage from $f_1, \ldots, f_r \mapsto f_1 - b_1, \ldots, f_r - b_r$ for $b_1, \ldots, b_r \in \mathbb{F}_q$, so it suffices to show that assuming (3) we have

$$p \mid \#Z = \#\{x \in \mathbb{F}_q^n \mid f_1(x) = \ldots = f_r(x) = 0\}.$$

If $0 \neq Y_j$ for some j then $Z = \varnothing$ and the conclusion certainly holds, so we may assume that $0 \in Y_j$ for all $1 \leq j \leq r$. For $1 \leq j \leq r$, put

$$\tilde{C}_j := \prod_{x_j \in Y_j \setminus \{0\}} (t - x) \in \mathbb{F}_q[t], \ C_j := \frac{1}{\tilde{C}_j(0)} \tilde{C}_j \in \mathbb{F}_q[t].$$

Thus C_j is a univariate polynomial of degree $\#Y_j - 1$, and the induced function from Y_j to $\mathbb{F}_q$ maps 0 to 1 and everything else to 0. Now put

$$P := \prod_{j=1}^{r} C_j(f_j) \in \mathbb{F}_q[t_1, \ldots, t_n].$$

Then $\deg P = \sum_{j=1}^{r} (\#Y_j - 1)\deg(f_j) < (q-1)n$ and $E(P)$ is the characteristic function of Z. We can now run Ax's proof with P in place of Chevalley's polynomial χ to get the result. □

If we have a polynomial system $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ with $d = \sum_{j=1}^{r} \deg(f_j) = n$ and a non-surjective evaluation map

$$E : \mathbb{F}_q^n \to \mathbb{F}_q^n, \ x \mapsto (f_j(x)),$$

then

$$\sum_{j=1}^{r} (\#Y_j - 1)\deg(f_j) < (q-1)\sum_{j=1}^{r} \deg(f_j) = (q-1)n,$$

so Theorem 3.4 applies to give $p \mid \#Z$. Under the same hypotheses Theorem 3.2 gives the stronger conclusion $q \mid \#Z$. On other hand, Theorem 3.4 applies even when $d > n$ if the Y_j's are small enough. So neither result encompasses the other.

These results become more interesting if have a plenitude of examples of systems $f_1, \ldots, f_r$ with $d = \sum_{j=1}^{r} \deg(f_j) = n$ and non-surjective evaluation map. We turn next to a discussion of such examples, which lie at the heart of the paper.

4. Examples

If in Theorem 3.2 all the f_j's are homogeneous, then using (1) relating $\#Z$ to $\#\mathbb{P}Z$ we get the following reformulation of this case of the result.

Corollary 4.1. *With notation as in Theorem 3.2, suppose moreover that each polynomial f_j is homogeneous, and let $\mathbb{P}Z$ be the solution locus in $\mathbb{P}^{n-1}(\mathbb{F}_q)$. Then at least one of the following holds:*

(i) *We have $\#\mathbb{P}Z \equiv 1 \pmod{q}$.*
(ii) *All fibers of $E(f) : \mathbb{F}_q^n \to \mathbb{F}_q^r$ have a common nonzero cardinality modulo q. In particular f is surjective.*

Let us focus on the case of one homogeneous degree n polynomial $f \in \mathbb{F}_q[t_1, \ldots, t_n]$.

Example 4.2. *For $n \in \mathbb{Z}^+$, let $f(t_1, \ldots, t_n) = t_1 \cdots t_n$. Then we have*

$$\#Z(f) = \#E^{-1}(0) = q^n - (q-1)^n \equiv (-1)^{n+1} \pmod{q},$$

so

$$\#\mathbb{P}Z(f) = \frac{q^n - (q-1)^n - 1}{q-1} = 1+q+\ldots+q^{n-1}-(q-1)^{n-1} \equiv 1+(-1)^n \pmod{q}.$$

For every $b \in \mathbb{F}_q^\times$ we can choose $x_1, \ldots, x_{n-1}$ to be any nonzero elements of $\mathbb{F}_q$ and then x_n is uniquely determined as $x_n = \frac{b}{x_1 \cdots x_{n-1}}$, so $\#E^{-1}(b) = (q-1)^{n-1} \equiv (-1)^{n+1} \pmod{q}$. So in Corollary 4.1, (ii) holds but (i) does not.

In general we may factor f into a product of irreducible homogeneous polynomials $g_1, \ldots, g_r$. Then we have $Z(f) = \bigcup_{i=1}^r Z(g_i)$, so Inclusion-Exclusion gives

$$\#Z(f) = \sum_i \#Z(g_i) - \sum_{i<j} \#(Z(g_i) \cap Z(g_j)) + \ldots + (-1)^r \# \bigcap_{j=1}^r Z(g_j). \tag{4}$$

Example 4.3. *Suppose $L = \prod_{i=1}^n L_i$ with $L_i \in \mathbb{F}_q[t_1, \ldots, t_n]$ degree 1 homogeneous.*

a) *In Example 4.2 we had $L_i = t_i$ for all $1 \leq i \leq n$. The corresponding linear functionals $E(t_1), \ldots, E(t_n)$ are the dual basis of the canonical basis $e_1, \ldots, e_n$ of $\mathbb{F}_q^n$, so they are linearly independent in the dual space $(\mathbb{F}_q^n)^\vee = \operatorname{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^n, \mathbb{F}_q)$. Now suppose that $L_1, \ldots, L_n$ are any n linearly independent linear forms, and let $f = L_1 \cdots L_n$. We can compute $\#Z(f)$ using (4): the linear independence implies that the inersection of any i of the hyperplanes $Z(L_i)$ is a linear subspace of dimension $n-i$, so we get*

$$\#Z(f) = \sum_{i=1}^n (-1)^{i+1} \binom{n}{i} q^{n-i} = q^n - (q-1)^n.$$

As above we have $\#\mathbb{P}Z(f) \not\equiv 1 \pmod{q}$ and $E(f) : \mathbb{F}_q^n \to \mathbb{F}_q$ is surjective.

b) *At the other extreme lies the case of a fixed hyperplane $H \subset \mathbb{F}_q^n$ such that $Z(L_i) = H$ for all $1 \leq i \leq n$. Then we have $\#Z(f) = \#H = q^{n-1}$, so*

$$\#\mathbb{P}Z(f) = \frac{q^{n-1} - 1}{q-1} = 1 + q + \ldots + q^{n-2} \equiv 1 \pmod{n}.$$

The function $E : \mathbb{F}_q \to \mathbb{F}_q,\ x \mapsto x^n$ is surjective iff $\gcd(n, q-1) = 1$. Thus if $\gcd(n, q-1) = 1$ then both (i) and (ii) of Corollary 4.1 hold, while if $\gcd(n, q-1) > 1$ then only (i) holds.

c) *When $n = 3$ there are two other linear algebraic configurations:*

(i) *Precisely two of the hyperplanes* $H_i = Z(L_i)$ *coincide – say* $H_1 = H_2$. *Then* $Z(f) = Z(L_1L_2L_3) = Z(L_1L_3)$ *where* L_1 *and* L_3 *are linearly independent linear forms in three variables, so (4) gives*

$$\#Z(f) = 2q^2 - q, \ \#\mathbb{P}Z(f) = 2q + 1 \equiv 1 \pmod q.$$

In this case $E(f)$ *is surjective. More generally, let* $L_1, \ldots, L_m \in \mathbb{F}_q[t_1, \ldots, t_n]$ *be nonzero linear forms, viewed as elements of* $(\mathbb{F}_q^n)^\vee$. *If for some* $1 \leq j \leq m$ *we have that* L_j *does not lie in the span of* $L_1, \ldots, L_{j-1}, L_{j+1}, \ldots, L_m$, *then after a linear change of variables we have* $L_1, \ldots, L_{m-1} \in \mathbb{F}_q[t_1, \ldots, t_{n-1}]$ *and* $L_m = t_n$. *If also* $\bigcup_{i=1}^{m-1} Z(L_i) \subsetneq \mathbb{F}_q^n$ *– this condition being always satisfied if* $m-1 < q+1$ [Cl12] *– then* $E(L_1 \cdots L_m) : \mathbb{F}_q^n \to \mathbb{F}_q$ *is surjective.*

(ii) *The three hyperplanes* H_1, H_2, H_3 *are distinct, but their intersection is a line. Then (4) gives*

$$\#Z(f) = 3q^2 - 3q + q = 3q^2 - 2q, \ \#\mathbb{P}Z(f) = 3q + 1 \equiv 1 \pmod q.$$

After a linear change of variables we reduce to the case $L_1 = t_1$, $L_2 = t_2$, $L_3 = at_1 + bt_2$ *with* $a, b \in \mathbb{F}_q^\times$. *When* $q = 2$ *we must have* $a = b = 1$ *and the map* $E(f)$ *is identically* 0. *(This reflects the fact that* $\mathbb{F}_2^2$ *can be covered by* 3 *lines.) When* $q = 3$, *after replacing* (t_1, t_2) *by* $(-t_1, -t_2)$ *if necessary, we have that* f *is either* $f_1 = t_1t_2(t_1 + t_2)$ *or* $f_2 = t_1t_2(t_1 - t_2)$, *and both* $E(f_1)$ *and* $E(f_2)$ *are surjective.*

Example 4.4. *Suppose* $d = 2$, *so*

$$f(t_1, t_2) = At_1^2 + Bt_1t_2 + Ct_2^2 \in \mathbb{F}_q[t_1, t_2]$$

is a binary quadratic form over $\mathbb{F}_q$.

• *If* $A = C = 0$, *then* $B \neq 0$ *and* $f = Bt_1t_2$, *so Example 4.3a) applies to give* $\#\mathbb{P}Z(f) = 2$, $\#Z(f) = 2q - 1$, *and every nonzero fiber has size* $q - 1$.

Otherwise $A \neq 0$ *or* $C \neq 0$; *without loss of generality, suppose* $A \neq 0$. *Then there are no solutions* $[X_1 : X_2]$ *in* $\mathbb{P}^1(\mathbb{F}_q)$ *with* $X_2 = 0$, *so* $\mathbb{P}Z$ *is naturally in bijection with solutions to the univariate quadratic equation* $Q(t) = At^2 + Bt + C = 0$.

• *Suppose* Q *has distinct roots in* $\mathbb{F}_q$. *Then* $\#\mathbb{P}Z(f) = 2$, *so* $\#Z(f) = 2q-1$. *Using Corollary 4.1 one finds that every nonzero fiber has size* $q - 1$.

• *Suppose* Q *has no roots in* $\mathbb{F}_q$. *Then* $\#\mathbb{P}Z(f) = 0$, *so* $Z(f) = 1$ *and all fibers have size* 1 *modulo* q *and* E *is surjective. For all* $b \in \mathbb{F}_q^\times$, *the equation*

$$C : At_1^2 + Bt_1t_2 + Ct_2^2 - bt_3^2 = 0$$

is a smooth conic curve in the projective plane. It is known that all such curves have $q + 1$ *points.*[5] *None of these points have* $X_3 = 0$, *so we get* $q + 1$ *solutions to* $At_1^2 + Bt_1t_2 + Ct_2^2 = b$.

• *If* Q *has exactly one root in* $\mathbb{F}_q$, *then* $\#\mathbb{P}Z(f) = 1$ *and* $\#Z(q) = q$. *In fact we are in the situation of Example 4.3b), so* $E(f)$ *is surjective iff* $p = 2$.

Recall that if $\mathbb{F}_q \subset F$ is a field extension and $x \in F$ is such that $x^q = x$, then we must have $x \in \mathbb{F}_q$. This holds, for instance, because the polynomial $t^q - t \in F[t]$ has

[5]We sketch one argument for this: by Theorem 1.1 there is at least one point $P_0 \in C(\mathbb{F}_q) \subset \mathbb{P}^2(\mathbb{F}_q)$. Through the point P_0 there are $q + 1$ lines. One of these lines is the tangent line to C at P_0 so intersects the curve C at P_0 alone. Every other line intersects C at one other point. All points of $C(\mathbb{F}_q)$ arise in this way.

degree q and has every element of $\mathbb{F}_q$ as a root, hence has no other roots. Moreover, if $x \in F$ is such that $x^{q-1} = 1$, then $x^q = x$, so $x \in \mathbb{F}_q$.

Example 4.5. *We consider here the case where $d = 3$ and $f(t_1, t_2, t_3)$ is a smooth, geometrically irreducible plane cubic. Geometrically irreducible means that f does not factor into polynomials of smaller degree (even) over an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. Smooth means that (even) over the algebraic closure $\overline{\mathbb{F}_q}$ the partial derivatives $\frac{\partial f}{\partial t_1}, \frac{\partial f}{\partial t_2}, \frac{\partial f}{\partial t_3}$ do not simultaneously vanish at any point $(x_0, y_0, z_0) \neq (0, 0, 0)$.*

Then f defines a nice curve $C_{/\mathbb{F}_q}$ of genus one, and (for instance) by the Hasse-Weil bounds [S, Thm. 5.2.3] *it follows that $\#C(\mathbb{F}_q) := \#\mathbb{P}Z(f) \geq 1$.*

By Corollary 4.1, the map $E(f) : \mathbb{F}_q^3 \to \mathbb{F}_q$ is surjective unless $\#C(\mathbb{F}_q) \equiv 1 \pmod q$. When does this happen? For any nice genus one curve $C_{/\mathbb{F}_q}$, the Hasse-Weil bounds give

$$\#C(\mathbb{F}_q) = q + 1 - t_C, \ \ |t_C| \leq 2\sqrt{q}. \tag{5}$$

So we need $q \mid t_C$ and $|t_C| \leq 2\sqrt{q}$. This places us within the class of ***supersingular elliptic curves***.[6]

When $q \geq 5$, an integer t_C satisfies $q \mid t_C$ and $|t_C| \leq 2\sqrt{q}$ if and only if $t_C = 0$. By a result of Waterhouse [Wa69, Thm. 4.1], *for a finite field $\mathbb{F}_q = \mathbb{F}_{p^a}$ there is a nice genus one curve $C_{/\mathbb{F}_q}$ with $t_C = 0$ iff (a is odd) or (a is even and $p \not\equiv 1 \pmod 4$)). Using Waterhouse's results or direct computation, one determines all $\#C(\mathbb{F}_q)$ with $\#C(\mathbb{F}_q) \equiv 1 \pmod q$ that arise as we range over all nice curves $C_{/\mathbb{F}_q}$ of genus 1: when $q = 2$ we have $\#C(\mathbb{F}_2) \in \{1, 3, 5\}$; when $q = 3$ we have $\#C(\mathbb{F}_3) \in \{1, 4, 7\}$; when $q = 4$ we have $\#C(\mathbb{F}_4) \in \{1, 5, 9\}$.*

Consider $f = t_1^3 + t_2^3 + t_3^3$ over $\mathbb{F}_4$. For all $x \in \mathbb{F}_4^\times$ we have $x^3 = 1$, while $0^3 = 0$, so $E(f) = \mathbb{F}_2 \subsetneq \mathbb{F}_4$. For $(x, y, z) \in \mathbb{F}_4^3$ we have $x^3 + y^3 + z^3 = 0$ iff either one or all three of x, y, z are zero, so $\#Z = 28$ and $\#\mathbb{P}Z = 9$. Thus f defines a supersingular elliptic curve over $\mathbb{F}_4$ that meets the Hasse-Weil bound by having $4 + 1 + 2\sqrt{4}$ $\mathbb{F}_4$-rational points. There is up to $\mathbb{F}_4$-isomorphism a unique elliptic curve $C_{/\mathbb{F}_4}$ with 9 rational points [M, p. 46]. *This is a very special elliptic curve: it has j-invariant zero and automorphism group $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, the largest automorphism group of any elliptic curve over any field* [Si, Thm. III.10.1].

Example 4.6. *Let $\mathbb{F}_{q_1} \subsetneq \mathbb{F}_{q_2}$ be a proper extension of finite fields, and put $a := \frac{q_2-1}{q_1-1}$. Let $g \in \mathbb{F}_{q_1}[t_1, \ldots, t_n]$ be homogeneous of degree $d \in \mathbb{Z}^+$, and put*

$$f = g(t_1^a, \ldots, t_n^a) \in \mathbb{F}_{q_1}[t_1, \ldots, t_n] \subset \mathbb{F}_{q_2}[t_1, \ldots, t_n],$$

so f is homogeneous of degree ad. For all $x \in \mathbb{F}_{q_2}^\times$ we have

$$(x^a)^{q_1-1} = x^{q_2-1} = 1, \ \text{so } x^a \in \mathbb{F}_{q_1},$$

and it follows that $E(f)(\mathbb{F}_{q_2}^n) \subseteq \mathbb{F}_{q_1} \subsetneq \mathbb{F}_{q_2}$.

If we now take $n = ad$, then Corollary 4.1 implies that all fibers of $E(f)$ have size divisible by q. Example 4.5 is the case of this construction with the smallest possible parameter values: $q_1 = 2$, $q_2 = 4$ and $d = 1$, so $n = a = 3$.

On the other hand, so long as $d < n$ then Theorem 3.4 applies to show that all fibers of $E(f)$ have size divisible by p.

[6] An elliptic curve $C_{/\mathbb{F}_q}$ is supersingular iff $p \mid t_C$.

Example 4.7. *Let*

$$f = t_1 t_2^3 + t_1^3 t_2 + t_3 t_4^3 + t_3^3 t_4 \in \mathbb{F}_9[t_1, t_2, t_3, t_4].$$

Then $E(f) : \mathbb{F}_9^4 \to \mathbb{F}_9$ has image $\mathbb{F}_3 \subsetneq \mathbb{F}_9$. The polynomial f defines a smooth quartic K3 surface, and we have $\#\mathbb{P}Z(f) = 280$; this quantity is 1 mod 9, as promised by Corollary 4.1, and it is not 1 mod 27.

One of us learned of this example from a talk given by U. Whitcher. It lies in the parametrized family L_2L_2 of K3 surfaces of [DKSSVW18, Table (5.1.1)].

Example 4.8. *Let $b \in \mathbb{Z}^+$, and suppose that $q \equiv 1 \pmod{b}$. Put*

$$T_b := t_1 t_2^q \cdots t_b^{q^{b-1}} + t_1^q t_2^{q^2} \cdots t_{b-1}^{q^{b-1}} t_b + \ldots + t_1^{q^{b-1}} t_2 \cdots t_b^{q^{b-2}} \in \mathbb{F}_{q^b}[t_1, \ldots, t_b].$$

Then T_b is homogeneous of degree $1 + q + \ldots + q^{b-1} \equiv 0 \pmod{b}$, so put

$$r := \frac{1 + q + \ldots + q^{b-1}}{b}.$$

Since we have $z^{q^b} = z$ for all $z \in \mathbb{F}_{q^b}$, for all $x_1, \ldots, x_b \in \mathbb{F}_{q^b}$ we have

$$T_b(x_1, \ldots, x_b)^q = x_1^q x_2^{q^2} \cdots x_{b-1}^{q^{b-1}} x_b^{q^b} + x_1^{q^2} \cdots x_{b-1}^{q^b} x_b^q + \ldots + x_1^{q^b} x_2^q \cdots x_b^{q^{b-1}}$$

$$= x_1^q x_2^{q^2} \cdots x_{b-1}^{q^{b-1}} x_b + x_1^{q^2} \cdots x_{b-1} x_b^q + \ldots + x_1 x_2^q \cdots x_b^{q^{b-1}} = T_b(x_1, \ldots, x_b).$$

Thus $T_b(x_1, \ldots, x_b) \in \mathbb{F}_q$ and we have

$$E(T_b(\mathbb{F}_{q^b}^b)) \subset \mathbb{F}_q.$$

Now for $1 \le i \le r$ and $1 \le j \le b$, let $X_{i,j}$ be independent indeterminates, and put

$$f_{b,q} := T_b(X_{1,1}, \ldots, X_{1,b}) + \ldots + T_b(X_{r,1}, \ldots, X_{r,b}) \in \mathbb{F}_{q^b}[X_{1,1}, \ldots, X_{r,b}].$$

Then $f_{b,q}$ is homogeneous of degree $n := 1 + q + \ldots + q^{b-1}$ in $rb = n$ variables and

$$E(f_{b,q})(\mathbb{F}_{q^b}^n) \subset \mathbb{F}_q,$$

so by Corollary 4.1 we have $\mathbb{P}Z(f_{b,q}) \equiv 1 \pmod{q}$.

The polynomial $f_{b,q}$ defines a smooth Calabi-Yau hypersurface over $\mathbb{F}_{q^b}$ of dimension $n-2$. The case of $b = 2$, $q = 3$ is Example 4.7 above. In the case of of $b = 2$, $q = 5$ we have $\#\mathbb{P}Z(f_{2,5}) = 2{,}035{,}026$; this quantity is $1 \pmod{25}$, as promised by Corollary 4.1, and it is not $1 \pmod{125}$.

5. Life Beyond the Boundary

Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_r]$ be polynomials of degrees $d_1, \ldots, d_r \in \mathbb{Z}^+$, and again consider the evaluation map

$$E : \mathbb{F}_q^n \to \mathbb{F}_q^r,\ x \mapsto (f_1(x), \ldots, f_r(x)).$$

When $d = \sum_{j=1}^r d_r < n$ we can view the theorems of Chevalley-Warning, Warning II and Ax-Katz as giving information on fiber cardinalities of E, and when $d = n$ Theorem 3.2 also gives (weaker) such information. Can anything be said if $d > n$?

Yes, in some cases. Here is an old result recast in fibered form.

Theorem 5.1 (Ore [Or22])**.** *For $f \in \mathbb{F}_q[t_1, \ldots, t_n]$, suppose that $d := \deg(f) \le q - 1$. Then for all $c \in \mathbb{F}_q$ we have either $E^{-1}(c) = \mathbb{F}_q^n$ or $\#E^{-1}(c) \le dq^{n-1}$.*

The new aspect of Ore's Theorem is that the "low degree" condition on f is in terms of the size of the finite field, not in terms of the number of variables. It says that when the degree of f is small compared to q then the fiber cardinalities of $E(f) : \mathbb{F}_q^n \to \mathbb{F}_q$ are somewhat equally distributed, except in the trivial case in which $E(f)$ is constant.

Theorem 5.1 is a special case of a result due to DeMillo-Lipton [DeML78], Zippel [Zip79] and Schwartz [Sc80]: if F is any field, $A \subset F$ is a finite subset, and $f \in \mathbb{F}[t_1, \ldots, t_n]$ is a nonzero polynomial of positive degree d, then

$$\#Z_A(f) = \#\{x = (x_1, \ldots, x_n) \in A^n \mid f(x) = 0\} \leq d(\#A)^{n-1}.$$

Wikipedia gives an elegant proof using very basic probability theory [Wk].

There are other results of Chevalley-Warning type that apply to *certain* polynomial systems $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ by taking more into account than the degrees of the polynomials. Here is one such result, again stated in fibered form.

Theorem 5.2 (Morlaye [Mo71])**.** *Let $n, m_1, \ldots, m_n \in \mathbb{Z}^+$. For $1 \leq i \leq n$, put $d_i := \gcd(m_i, q-1)$. Let $a_1, \ldots, a_n, b \in \mathbb{F}_q$ and let*

$$f = a_1 t_1^{m_1} + \ldots + a_n t_n^{m_n}.$$

If

$$\sum_{i=1}^{n} \frac{1}{d_i} > 1,$$

then every fiber of $E(f)$ has size divisible by p.

Morlaye's results have been sharpened by Wan [Wa88] who showed in particular that under the hypotheses of Theorem 5.2 we have that every fiber of $E(f)$ has size divisible by q. A further generalization is given in [BBC19, Cor. 1.17].

A simple example in which Theorem 5.2 applies and Theorem 1.1 does not is $f(t_1, t_2, t_3) = t_1^2 + t_2^3 + t_3^5$. In this case the polynomial has degree 5 but is "sparser" than a general such polynomial. This can be formalized as follows: rather than just the degree of each polynomial f_j one may try to take into account its **support**, i.e., the subset of indices $\underline{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$ such that the monomial $t_1^{i_1} \cdots t_n^{i_n}$ appears in f_j with nonzero coefficient. Adolphson-Sperber give an important result along these lines in terms of the Newton polyhedron of f_j (which is defined in terms of its support) [AS87], and the literature contains further such results as well.

But what if we want results on the fiber cardinalities of *any* system of polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ such that $\sum_{j=1}^{r} \deg(f_j) \leq d$ for some $d > n$? We know of no such results in the literature apart from Theorem 5.1 in the $r = 1$ case.

In fact we claim that *nothing* can be said when $d \geq rn(q-1)$ and that *something* can be said when $d < rn(q-1)$. To explain this, let $x \in \mathbb{F}_q^n$ and put

$$\delta_x := \prod_{i=1}^{n} \left(1 - (t_i - x_i)^{q-1}\right).$$

Then $\deg \delta_x = (q-1)n$ and the associated function $E(\delta_x)$ maps x to 1 and every other element of $\mathbb{F}_q^n$ to 0. The functions $E(\delta_x)$ therefore form a basis for the $\mathbb{F}_q$-vector space of all functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q$, and it follows that every function $E : \mathbb{F}_q^n \to \mathbb{F}_q$ is obtained by evaluating a polynomial of degree at most $(q-1)n$.[7] So as we range over all polynomials $f_1, \ldots, f_r$ with $\sum_{j=1}^r \deg(f_j) \leq rn(q-1)$, the associated evlauation maps $E(f) : \mathbb{F}_q^n \to \mathbb{F}_q^r$ give all functions between these sets, so there is nothing to say about fiber cardinalities of such polynomials maps beyond what is true of fiber cardinalities of all functions $\mathbb{F}_q^n \to \mathbb{F}_q^r$: namely, to each $b \in \mathbb{F}_q^r$ we have a non-negative integer

$$z_b = \# E^{-1}(b)$$

with the sole constraint that $\sum_{b \in \mathbb{F}_q^r} z_b = q^n$.

On the other hand, if $d < rn(q-1)$, then for at least one $1 \leq j \leq r$ we must have $\deg(f_j) < n(q-1)$. In this case, as we saw in the proof of Theorem 1.1, we have $\sum_{x \in \mathbb{F}_q^n} f_j(x) = 0$, so that the jth component of $f \sum_{x \in \mathbb{F}_q^n} E(x)$ is 0. But

$$\sum_{x \in \mathbb{F}_q^n} E(x) = \sum_{b \in \mathbb{F}_q^r} z_b b,$$

so we get a constraint the z_b's. There are maps that do not satisfy this constaint: indeed, for any $y \in \mathbb{F}_q^r$, for $1 \leq j \leq r$ let $E_j = y_j \delta_0$ and put $E = (E_1, \ldots, E_r) : \mathbb{F}_q^n \to \mathbb{F}_q^r$. Then

$$\sum_{b \in \mathbb{F}_q^r} z_b b = \sum_{x \in \mathbb{F}_q^n} E(x) = y.$$

6. Open Questions

Question 6.1. *Under the hypotheses of Theorem 3.4, must every fiber have size a multiple of q? More generally, is there a strengthening of Theorem 3.1 that takes the image cardinalities $\# f_j(\mathbb{F}_q^n)$ into account?*

Question 6.2. *Let $L_1, \ldots, L_m \in \mathbb{F}_q[t_1, \ldots, t_n]$ be linear forms. Is there a general criterion for the surjectivity of $E(L_1 \cdots L_m) : \mathbb{F}_q^n \to \mathbb{F}_q$?*

Question 6.3. *Let $f \in \mathbb{F}_q[t_1, t_2, t_3]$ be a smooth plane cubic curve. Is it true that $E(f) : \mathbb{F}_q^3 \to \mathbb{F}_q$ is surjective unless $q = 4$ and $\# \mathbb{P}Z(f) = 9$? (See the Appendix for some calculations in modest support of an affirmative answer.)*

Question 6.4. *What are the further constraints on fiber cardinalities in the family of all polynomial functions*

$$E : \mathbb{F}_q^n \to \mathbb{F}_q^r, \; x \mapsto (f_j(x))$$

with $\sum_{j=1}^r \deg(f_j) \leq d$ when $d < rn(q-1)$? Can anything nice be said, for instance, when $d = n+1$?

[7] Such considerations form the beginning of Chevalley's proof of Theorem 1.1.

7. Acknowledgments

Partial support for the second and third authors was provided by the Research and Training Group grant DMS-1344994 funded by the National Science Foundation. The second author is also supported in part by the National Science Foundation Graduate Research Fellowship under Grant No. 1842396.

Appendix: Further Study of Homogeneous Ternary Cubic Forms

In this appendix we take a closer look at the evaluation map on a homogeneous cubic $f \in \mathbb{F}_q[t_1, t_2, t_3]$.

7.1. **Singular and Reducible Cubics.** In Example 4.5 we restricted to the case in which f is smooth and geometrcally irreducible, or otherwise put, defines a nice curve of genus one. What are the possible values of $\#\mathbb{P}Z$ for a plane cubic that is singular and/or geometrically reducible? We will now write down all possibilities. We ask the reader with a prior familiarity with elliptic curves to pause and think of what the classification should look like – each of the authors has experience with elliptic curves, and the classification is longer than we would have predicted!

Example 7.1 (Geometrically Irreducible Singular Cubics). *Let $f(t_1, t_2, t_3) \in \mathbb{F}_q[t]$ be a homogeneous cubic that is geometrically irreducible but singular. An irreducible plane cubic has at most one singular point $P = [x_0 : y_0 : z_0]$ in the projective plane, and over a perfect field like $\mathbb{F}_q$, if the cubic is singular there is a unique $\mathbb{F}_q$-rational singular point* [Ca, pp. 22-24]. *At least one of x_0, y_0, z_0 must be nonzero; without loss of generality, suppose $z_0 \neq 0$; then (x_0, y_0) is a singular point of the affine plane curve $f(t_1, t_2, 1)$. The change of variables $f \mapsto g(t_1, t_2) := f(t_1 - x_0, t_2 - y_0)$ brings the unique singular point to $(0, 0)$. Then we may write*

$$g(t_1, t_2) = g_1(t_1, t_2) + g_2(t_1, t_2) + g_3(t_1, t_2),$$

with g_i homogeneous of degree i. To say that the point $(0, 0)$ is singular is to say that $\frac{dg}{dt_1}$ and $\frac{dg}{dt_2}$ both vanish at $(0, 0)$, which means that $g_1 = 0$. If also $g_2 = 0$, then $g = g_3$ is geometrically reducible, which implies that f is geometrically reducible, a contradiction. So we have

$$g_2(t_1, t_2) = At_1^2 + Bt_1t_2 + Ct_2^2, \ A, B, C \in \mathbb{F}_q \text{ are not all zero.}$$

We say that f has a

a) ***split node*** *if g_2 factors into linearly independent linear forms L_1, L_2 over $\mathbb{F}_q$.*
b) ***nonsplit node*** *if g_2 is irreducible over $\mathbb{F}_q$ but factors into linearly independent linear forms L_1, L_2 over an algebraic extension of $\mathbb{F}_q$ (equivalently, over $\mathbb{F}_{q^2}$).*
c) ***cusp*** *if $g_2 = aL^2$ for a linear form L and $a \in \mathbb{F}_q^\times$.*

We claim that

$$\#\mathbb{P}Z = \begin{cases} q & f \text{ has a split node} \\ q+2 & f \text{ has a nonsplit node} \\ q+1 & f \text{ has a cusp} \end{cases}.$$

Thus Corollary 4.1 implies that $E(f) : \mathbb{F}_q^3 \to \mathbb{F}_q$ *is surjective in the nodal cases.*

These are well-known results,[8] *but the interested reader can get a good sense of them as follows: consider a homogeneous degree* d *polynomial* $f(t_1, t_2, t_3)$ *over an algebraically closed field* k*. Then for any linear form* $L \in k[t_1, t_2, t_3]$*, the locus in the projective plane* $\mathbb{P}^2_F$ *of* $f = L = 0$ *has size* d provided that *the intersection points are counted with suitable intersection multiplicities. Each point* $P = [x_0 : y_0 : z_0] \in \mathbb{P}^2_k$ *itself has a multiplicity* $m_P \in \mathbb{Z}^+$*, which is* 1 *iff the point* P *is nonsingular. More precisely, if as above we dehomogenize and move* P *to* $(0, 0)$ *in the affine plane to get a polynomial* $g(t_1, t_2)$ *with* $g(0, 0) = 0$*, then* m_P *is the least* i *such that the degree* i *homogeneous part* g_i *of* g *is nonzero, and the tangent lines at* P *are the linear factors of* g_i*. Moreover, for any line* L *through* P*, the intersection multiplicity of* L *with* f *at* P *is at least* m_P*, with equality iff* L *is not a tangent line at* P*. So:*

a) *A split node* P *has two tangent lines* L_1 *and* L_2*, and each is defined over* $\mathbb{F}_q$*. Since* $m_P = 2$*, if* L *is any nontangent line passing through* P*, its intersection with* P *contributes* $m_P = 2$ *to the multiplicity, whereas* $\deg f = 3$*, leaving exactly one more* k*-rational intersection point. If* L *is a tangent line, then its intersection with* P *contributes at least* 3 *to the multiplicity, so* L *intersects* f *at no other point (even over the algebraic closure). For every point* Q *of* $\mathbb{P}^2(\mathbb{F}_q)$ *different from* P*, there is a unique* $\mathbb{F}_q$*-rational line joining* Q *to* P*, and the set of* $\mathbb{F}_q$*-rational lines through any* $P \in \mathbb{P}^2(\mathbb{F}_q)$ *corresponds to the hyperplanes in a* 3*-dimensional* $\mathbb{F}_q$*-vector space that contain a given line, of which there are* $q+1$*. Therefore the* 2 *tangent lines at* P *contribute no more points to* $\mathbb{P}Z$*, while each of the* $q + 1 - 2 = q - 1$ *nontangent lines contributes a unique point, giving*
$$\#\mathbb{P}Z = 1 + (q - 1) = q.$$

b) *In the case of a nonsplit node, the tangent lines are not* $\mathbb{F}_q$*-rational, which means that each of the* $q+1$ $\mathbb{F}_q$*-rational lines through* P *intersects a unique* $\mathbb{F}_q$*-rational point on the projective curve. This shows that*
$$\#\mathbb{P}Z = 1 + (q + 1) = q + 2.$$

c) *In the case of a cusp, there is a unique tangent line, which again intersects* P *at no other point. Each of the* q *other* $\mathbb{F}_q$*-rational lines through* P *intersects a unique* $\mathbb{F}_q$*-rational point on the projective curve. This shows that*
$$\#\mathbb{P}Z = q + 1.$$

Example 7.2 (Geometrically Reducible Cubics)**.** *Now suppose that* $f(t_1, t_2, t_3) \in \mathbb{F}_q[t]$ *is a geometrically reducible cubic. There are several cases:*

a) *We have* $f = L_1L_2L_3$ *is a product of linear forms. This was analyzed in Example 4.3c). Our analysis was complete except for the case in which the corresponding hyperplanes are distinct and intersect in a line.*

b) *We have* $F = L \cdot C$*, with* L_1 *a linear form and* C *an irreducible quadratic that factors over* $\mathbb{F}_{q^2}$ *into* L_2L_3*.*

In this case we have $\#\mathbb{P}Z(C) = 1$*: we have two lines that are interchanged by the action of Galois, with a unique* $\mathbb{F}_q$*-rational intersection point, and we have* $\#\mathbb{P}Z(L) = q + 1$*. If the line intersects the conic in its*

[8]Unfortunately we have only been able to find them in the literature in the special case of a singular *Weierstrass* cubic, which is why we give a detailed sketch here.

unique $\mathbb{F}_q$-rational point, then $\#\mathbb{P}Z = q+1$. Otherwise the line intersects the conic in two points, neither of which are $\mathbb{F}_q$-rational, so $\#\mathbb{P}Z = q+2$.

c) *We have $f = L \cdot C$, with L a linear form and C a quadratic that is geometrically irreducible. In this case $\#\mathbb{P}Z$ is equal to the number of points on the line, $q+1$, plus the number of points on the conic, $q+1$, minus the number of points I on the intersection, which can be 0, 1 or 2. We have $I = 0$ iff there are two intersection points in $\overline{\mathbb{F}_q}$ but neither is defined over $\mathbb{F}_q$; in the middle case, the line is tangent to the conic, so there is one $\mathbb{F}_q$-rational intersection point; in the last case there are two $\mathbb{F}_q$-rational intersection points. Thus in the tangency case we have $\#\mathbb{P}Z = 2q+1 \equiv 1 \pmod{q}$.*

d) *We have that f is irreducible over $\mathbb{F}_q$ but factors over $\mathbb{F}_{q^3}$ as a product of linear forms. In this case over $\overline{\mathbb{F}_q}$ we have three lines arranged in a triangle and cyclically permuted by the action of Galois, so $\#\mathbb{P}Z = 0$.*

7.2. **Computational Results.** Two of the authors undertook a computer search for instances of homogeneous degree n polynomials $f \in \mathbb{F}_q[t_1, \ldots, t_n]$ with non-surjective evaluation map $E : \mathbb{F}_q^n \to \mathbb{F}_q$. By far the most interesting results were attained with $n = 3$: though in retrospect we should have found the Fermat cubic $t_1^3 + t_2^3 + t_3^3$ over $\mathbb{F}_4$ by pure thought, in fact we first did so via computer search.

7.2.1. *$q = 2$.* Through a complete search of plane cubics over $\mathbb{F}_2$ we find that there are exactly 7 with non-surjective evaluation map. Each such plane cubic factors as a product of three linears over $\mathbb{F}_2$, with the intersection of the corresponding hyperplanes a line, i.e., is the case of Example 6.6c)(ii).

7.2.2. *$q \in \{3, 5, 8, 9, 11\}$.* Through complete searches, we find that there are no plane cubics with non-surjective evaluation map over $\mathbb{F}_q$ for $q \in \{3, 5, 8, 9, 11\}$.

7.2.3. *$q = 4$.* Through a complete search of plane cubics over $\mathbb{F}_4$ we found 840 smooth, geometrically irreducible cubics with non-surjective evaluation map. They are all isomorphic, as elliptic curves, to the Fermat elliptic curve $t_1^3 + t_2^3 + t_3^3 = 0$ of Example 4.5. We also find 2583 reducible cubics f with non-surjective evaluation map, having either 5 or 13 points projectively over $\mathbb{F}_4$. The following cases occur:

a) The cubic f factors over $\mathbb{F}_4$ as a product of linear polynomials L_i with corresponding hyperplanes H_i, and
   (i) the H_i are all equal (the case of Example 4.3b)), for example
   $$f = X^3 + aX^2Z + a^2XZ^2 + Z^3 = (X + aZ)^3,$$
   where a is a generator of $\mathbb{F}_4^*$, or
   (ii) the hyperplanes H_i are distinct with intersection a line (the case of Example 4.4c)(ii)), for example
   $$\begin{aligned} f &= aX^3 + aX^2Y + aX^2Z + aXY^2 + aXZ^2 \\ &= X(X + aY + aZ)(X + a^2Y + a^2Z). \end{aligned}$$

b) The cubic f factors over $\mathbb{F}_4$ as the product of a linear and a conic to which it is tangent, with the conic factoring over $\mathbb{F}_{16}$ as a product of linears (one case of Example 6.6b)). For example:
$$\begin{aligned} f &= aY^3 + a^2Z^3 + aX^2Y + X^2Z + a^2XY^2 + XZ^2 + aYZ^2 \\ &= a^2(aY + z)(aX^2 + a^2XY + aY^2 + aXZ + YZ + Z^2). \end{aligned}$$

The only possibility for factorization that is not determined by Corollary 4.1 to necessarily have surjective evaluation map, and does not occur over $\mathbb{F}_4$, is the product of a linear polynomial and a geometrically irreducible conic to which it is tangent. We have not witnessed this factorization type having non-surjective evaluation map over $\mathbb{F}_q$ for any q.

7.2.4. $q = 7$. Through a complete search of plane cubics over $\mathbb{F}_7$ we find

a) 19494 which have non-surjective evaluation map with 22 points projectively over $\mathbb{F}_7$. Each of these factors as a product of three linears over $\mathbb{F}_7$, with the mutual intersection of the corresponding hyperplanes a line (the case of Example 4.3c)(ii)), and
b) 342 which have non-surjective evaluation map with 8 points projectively over $\mathbb{F}_7$. These consist of the cubes of linear factors over $\mathbb{F}_7$ (Example 4.3b)).

References

[Al99] N. Alon, *Combinatorial Nullstellensatz.* Recent trends in combinatorics (Mátraháza, 1995). Combin. Probab. Comput. 8 (1999), 7–29.

[AM21] E. Aichinger and J. Moosbauer, *Chevalley Warning type results on abelian groups.* J. Algebra 569 (2021), 30–66.

[AS87] A. Adolphson and S. Sperber, *p-adic estimates for exponential sums and the theorem of Chevalley-Warning.* Ann. Sci. École Norm. Sup. (4) 20 (1987), 545–556.

[As18] S. Asgarli, *A new proof of Warning's second theorem.* Amer. Math. Monthly 125 (2018), 549–553.

[Ax64] J. Ax, *Zeroes of polynomials over finite fields.* Amer. J. Math. 86 (1964), 255–261.

[BBC19] I. Baoulina, A. Bishnoi and P.L. Clark, *A generalization of the theorems of Chevalley-Warning and Ax-Katz via polynomial substitutions.* Proc. Amer. Math. Soc. 147 (2019), 4107–4122.

[Ca] J.W.S. Cassels, *Lectures on elliptic curves.* London Mathematical Society Student Texts, 24. Cambridge University Press, Cambridge, 1991.

[CFS17] P.L. Clark, A. Forrow and J.R. Schmitt, *Warning's Second Theorem With Restricted Variables.* Combinatorica 37 (2017), 397–417.

[Ch35] C. Chevalley, *Démonstration d'une hypothèse de M. Artin.* Abh. Math. Sem. Univ. Hamburg 11 (1935), 73–75.

[Cl-NT] P.L. Clark, *Number Theory: A Contemporary Introduction.* `http://math.uga.edu/~pete/4400FULL.pdf`

[Cl12] P.L. Clark, *Covering numbers in linear algebra.* Amer. Math. Monthly 119 (2012), 65–67.

[DeML78] R.A. DeMillo and R. Lipton, *A probabilistic remark on algebraic program testing.* Information Processing Letters 7 (1978), 193–195.

[Di09] L.E. Dickson, *On the representation of numbers by modular forms.* Bull. Amer. Math. Soc. Volume 15, Number 7 (1909), 338–347.

[DKSSVW18] C.F. Doran, T.L. Kelly, A. Salerno, S. Sperber, J. Voight and U. Whitcher, *Zeta functions of alternate mirror Calabi-Yau families.* Israel J. Math. 228 (2018), 665–705.

[HB11] D.R. Heath-Brown, *On Chevalley-Warning theorems.* (Russian. Russian summary) Uspekhi Mat. Nauk 66 (2011), no. 2(398), 223–232; translation in Russian Math. Surveys 66 (2011), no. 2, 427–436.

[Ka71] N.M. Katz, *On a theorem of Ax.* Amer. J. Math. 93 (1971), 485–499.

[LN97] R. Lidl and H. Niederreiter, *Finite fields.* With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

[M] A. Menezes, *Elliptic curve public key cryptosystems.* With a foreword by Neal Koblitz. The Kluwer International Series in Engineering and Computer Science, 234. Communications and Information Theory. Kluwer Academic Publishers, Boston, MA, 1993.

[Mo71] B. Morlaye, *Équations diagonales non homogènes sur un corps fini.* C. R. Acad. Sci. Paris Sér. A-B 272 (1971), A1545–A1548.

[Or22] Ö. Ore, *Über höhere Kongruenzen.* Norsk Mat. Forenings Skrifter Ser. I (1922), no. 7, 15 pages.

[S] H. Stichtenoth, *Algebraic function fields and codes.* Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.

[Sc80] J.T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities.* J. Assoc. Comput. Mach. 27 (1980), no. 4, 701–717.

[Si] J.H. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[Te66] G. Terjanian, *Sur les corps finis.* C. R. Acad. Sci. Paris Sér. A-B 262 (1966), A167–A169.

[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley.* Abh. Math. Sem. Hamburg 11 (1935), 76–83.

[Wa69] W.C. Waterhouse, *Abelian varieties over finite fields.* Ann. Sci. École Norm. Sup. (4) 2 (1969), 521–560.

[Wa88] D.Q. Wan, *Zeros of diagonal equations over finite fields.* Proc. Amer. Math. Soc. 103 (1988), 1049–1052.

[Wk] `https://en.wikipedia.org/wiki/Schwartz-Zippel_lemma`

[Zip79] R. Zippel, *An explicit separation of relativised random polynomial time and relativised deterministic polynomial time.* Inform. Process. Lett. 33 (1979), 207–212.