On the Dispersions of the Polynomial Maps over Finite Fields

Uwe Schauz

Department of Mathematics and Statistics
King Fahd University of Petroleum and Minerals
Dhahran 31261, Saudi Arabia
uwe.schauz@kfupm.edu.sa

Submitted: Dec 19, 2007; Accepted: Nov 24, 2008; Published: Nov 30, 2008
Mathematics Subject Classifications: 13M10, 11G25, 11D79, 15A15

Abstract

We investigate the distributions of the different possible values of polynomial maps $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q\,,\ x \longmapsto P(x)$. In particular, we are interested in the distribution of their zeros, which are somehow dispersed over the whole domain $\mathbb{F}_q^n$. We show that if U is a "not too small" subspace of $\mathbb{F}_q^n$ (as a vector space over the prime field $\mathbb{F}_p$), then the derived maps $\mathbb{F}_q^n/U \longrightarrow \mathbb{F}_q\,,\ x+U \longmapsto \sum_{\tilde{x}\in x+U} P(\tilde{x})$ are constant and, in certain cases, not zero. Such observations lead to a refinement of Warning's classical result about the number of simultaneous zeros $x \in \mathbb{F}_q^n$ of systems $P_1,\dots,P_m \in \mathbb{F}_q[X_1,\dots,X_n]$ of polynomials over finite fields $\mathbb{F}_q$. The simultaneous zeros are distributed over all elements of certain partitions (factor spaces) $\mathbb{F}_q^n/U$ of $\mathbb{F}_q^n$. $|\mathbb{F}_q^n/U|$ is then Warning's well known lower bound for the number of these zeros.

Introduction

As described in the abstract, we will investigate the distributions of the different possible values of polynomial maps $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q\,,\ x \longmapsto P(x)$. In particular, we are interested in the distribution of their zeros in the domain $\mathbb{F}_q^n$. It turns out that they are somehow dispersed over the whole domain $\mathbb{F}_q^n$, a property that strongly relies on the finiteness of the ground field $\mathbb{F}_q$. The original goal behind this was to present a new sharpening (supplementation) of the following classical result, due to Chevalley and Warning, about the set of simultaneous zeros $\mathcal{V} := \{\, x \in \mathbb{F}_q^n \mid P_1(x) = \cdots = P_m(x) = 0 \,\}$ of polynomials $\mathcal{V}$
$P_1,\dots,P_m \in \mathbb{F}_q[X_1,\dots,X_n]$ over finite fields $\mathbb{F}_q$ of characteristic p : m, n
$\mathbb{F}_q,\ p$

Theorem 0.1. *If* $\sum_{i=1}^{m} \deg(P_i) < n$ *, then*

$$p \quad \textit{divides} \quad |\mathcal{V}|$$

and hence the P_i *do not have one unique common zero, i.e.,* $|\mathcal{V}| \neq 1$ *.*

This theorem goes back to a conjecture of Dickson and Artin [Ar] and has a short and elegant proof [Scha, Theorem 4.3], [Schm]. There are a lot of different sharpenings and supplementations, which follow two main streams. The first one [MSCK, MoMo, Wan, Ax, Ka] tries to improve the divisibility property and led, e.g., to the following improvement by Katz (see [MSCK, Wan, Wan2, AdSp, AdSp2, Sp] for generalizations to exponential sums):

Theorem 0.2. *If* $\Sigma := \sum_{i=1}^{m} \deg(P_i) < n$ *and* $M := \max_{1\le i\le m}(\deg(P_i))$ *, then* Σ, M

$$q^{\left\lceil \frac{n-\Sigma}{M} \right\rceil} \quad \textit{divides} \quad |\mathcal{V}| \ .$$

The second stream tries to give a lower bound for the cardinality of the set of simultaneous zeros $\mathcal{V}$, if this set is not empty. Warning‘s Theorem 0.3 below (see [Schm]) is the classical result in this direction:

Theorem 0.3. *If there are simultaneous zeros, i.e., if* $\mathcal{V} \neq \varnothing$ *, then*

$$q^{n-\Sigma} \quad \leq \quad |\mathcal{V}| \ .$$

This bound is best possible; only by using measures, more differentiated than the degrees $\deg(P_i)$ of the polynomials P_i , it can be improved further (see [MoMo, Theorem 2]). Our Corollary 2.4 does not improve the Warning bond, but refines the simple enumerative statement by saying more about the location of the zeroes. It uses the same, usually easily assessable, sum $\Sigma := \sum_{i=1}^{m} \deg(P_i)$ of the degrees $\deg(P_i)$, but could be stated for other measures (as in [MoMo]) as well. Note that we formulated Corollary 2.4 only for prime fields, but, in order to apply it to nonprime fields, it can be combined with Lemma 3.1 .

Beside the described two main streams, we found in [Scha] a version that works over $\mathbb{Z}/p^k\mathbb{Z}$ and over $\mathbb{Z}$. We call this version a “Not Exactly One Theorem” as $|\mathcal{V}| \neq 1$ is stated. In that same paper we also demonstrated that some other versions of Theorem 0.1 – other “$\neq$1-Theorems”– which work over subgrids $\mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n$ of the full grid $\mathbb{F}_q^n$, e.g., the important Boolean grid $\{0,1\}^n$, are very useful and flexible in application.

Our paper is structured as follows:

In Section 1 we present the main method behind this paper, the so called “polynomial method” (the well known Combinatorial Nullstellensatz 1.2 and its quantitative version

Theorem 1.3). A generalized kind of permanent, together with some of its properties, is provided in this first section as well.

Section 2 contains our new sharpening (Corollary 2.4) of Chevalley and Warning's Theorem 0.1, as well as our main result Theorem 2.3. They are only formulated for finite prime fields $\mathbb{F}_p$. However, they may also be applied to arbitrary finite fields $\mathbb{F}_q$ by using Lemma 3.1 of the next section. The results in Section 2 are based on a series of lemmas at its beginning. Our generalized kind of permanent plays a major role in them.

Section 3 provides with Lemma 3.1 the keytool for applications in nonprime finite fields. However, this tool lets some space for further questions, so that we close with the two conjectures 3.2 and 3.3.

1 Basics

Throughout the whole paper we will use the following convenient notation:
Let $n \in \mathbb{N} := \{0, 1, 2, \ldots\}$ then $\mathbb{N}$
$(n] = (0, n] := \{1, 2, \ldots, n\}$, $(n]$
$[n) = [0, n) := \{0, 1, \ldots, n{-}1\}$, $[n)$
$[n] = [0, n] := \{0, 1, \ldots, n\}$. (Note that $0 \in [n]$.) $[n]$

In order to introduce the so called "polynomial method" we also need the following definition:

Definition 1.1 (d-grids). Assume $d = (d_j) \in \mathbb{N}^n$, and let $\mathbb{F}$ be a field. A *d-grid* is a Cartesian product $\mathfrak{X} := \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n$ of subsets $\mathfrak{X}_j \subseteq \mathbb{F}$ of size $|\mathfrak{X}_j| = d_j + 1$. $d, \mathbb{F}$ $\mathfrak{X}$

We frequently use Alon and Tarsi's Combinatorial Nullstellensatz [Al, Theorem 1.2], which provides some information about the polynomial map $P|_{\mathfrak{X}} \colon \mathfrak{X} \longrightarrow \mathbb{F},\ x \longmapsto P(x)$ $P|_{\mathfrak{X}}$ when only incomplete information about a polynomial $P \in \mathbb{F}[X] := \mathbb{F}[X_1, \ldots, X_n]$ is given: $\mathbb{F}[X]$

Theorem 1.2 (Combinatorial Nullstellensatz). *Let $\mathfrak{X}$ be a d-grid. For each polynomial $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{F}[X]$ of total degree $\deg(P) \le \sum_j d_j$,* P_d

$$\boxed{P_d \neq 0 \implies P|_{\mathfrak{X}} \not\equiv 0} .$$

In [Scha, Teorem 3.3] we have proven a stronger result. We have shown that

$$P_d = \sum_{x \in \mathfrak{X}} N(x)^{-1} P(x) \tag{1}$$

with a certain map $N \colon \mathfrak{X} \longrightarrow \mathbb{F}$. We will use this sharpening once in the case $\mathfrak{X} = \mathbb{F}_p^n$. In this case $N \equiv (-1)^n$ by [Scha, Lemma 1.4(iv)] so that:

Theorem 1.3 (Coefficient formula). *Let* $d := (p-1, p-1, \ldots, p-1) \in \mathbb{N}^n$. *For polynomials* $P = \sum_{\delta\in\mathbb{N}^n} P_\delta X^\delta \in \mathbb{F}_p[X]$ *of total degree* $\deg(P) \le \sum_j d_j = (p-1)n$,

$$\boxed{P_d \;=\; (-1)^n \sum\nolimits_{x\in\mathbb{F}_p^n} P(x)}\;.$$

This special version of our Coefficient Formula (1) follows also from the well known

$$\sum_{a\in\mathbb{F}_p} a^i \;=\; \begin{cases} 0 & \text{if } 0 \le i \le p-2 \;, \\ -1 & \text{if } i = p-1 \;, \end{cases} \tag{2}$$

and is an easy fact. In [Scha, Section 5] we applied the general Coefficient Formula (1) to the matrix polynomial, a generalization of the graph polynomial (see also [AlTa] or [Ya]). This led to several results about graph colorings and permanents. Here, in this paper, the matrix polynomial occurs in the construction of certain other polynomials, we have to provide it again:

We always assume $A = (a_{i,j}) \in \mathbb{F}^{m\times n}$, and the product of this matrix with $X := (X_1, \ldots, X_n)^T$ is $AX := (\sum_{j\in(n]} a_{ij}X_j)_{i\in(m]} \in \mathbb{F}[X_1, X_2, \cdots, X_n]^m = \mathbb{F}[X]^m$. Now, the matrix polynomial $\Pi(AX)$ is defined as follows: A, X AX

Definition 1.4 (Matrix polynomial). The *matrix polynomial* of $A = (a_{i,j}) \in \mathbb{F}^{m\times n}$ is given by $\Pi(AX)$

$$\Pi(AX) \;:=\; \prod_{i\in(m]} \sum_{j\in(n]} a_{ij}X_j \;\in\; \mathbb{F}[X] \;.$$

It turns out that the coefficients of the matrix polynomial are some kind of permanents. We define:

Definition 1.5 (δ-permanent). For $\delta \in \mathbb{N}^n$ the δ-*permanent* of $A = (a_{i,j}) \in \mathbb{F}^{m\times n}$ is define through $\mathrm{per}_\delta(A)$

$$\mathrm{per}_\delta(A) \;:=\; \sum_{\substack{\sigma:\,(m]\to(n] \\ |\sigma^{-1}|=\delta}} \pi_A(\sigma) \;\;,$$

where $\pi_A(\sigma)$

$$\pi_A(\sigma) \;:=\; \prod_{i\in(m]} a_{i,\sigma(i)} \quad \text{and} \quad |\sigma^{-1}| \;:=\; \big(|\sigma^{-1}(j)|\big)_{j\in(n]} \;.$$

$|\sigma^{-1}|$

Now, indeed:

Lemma 1.6.

$$\boxed{\Pi(AX) \;=\; \sum\nolimits_{\delta\in\mathbb{N}^n} \mathrm{per}_\delta(A)\, X^\delta}\;.$$

Based on this connection to the matrix polynomial, the δ-permanents will play a major roll in this paper. Therefore, some simple properties shall be provided:

At first we see that the maps

$$A \longmapsto \pi_A(\sigma) \quad \text{and} \quad A \longmapsto \operatorname{per}_\delta(A) \quad \text{are multilinear in the rows of } A\,. \tag{3}$$

We also see that $\operatorname{per}_\delta(A) = 0$ if $\sum_j \delta_j \neq m$. If $m = n$ then $\operatorname{per} := \operatorname{per}_{(1,1,\ldots,1)}$ is the usual permanent [Minc]; and, if $\sum_j \delta_j = m$, it is easy to see that

per

$$\bigl(\textstyle\prod_{j\in(n]} \delta_j!\bigr)\ \operatorname{per}_\delta(A) \;=\; \operatorname{per}(A\langle|\delta\rangle), \tag{4}$$

where $A\langle|\delta\rangle$ is a matrix that contains the j^{th} column of A exactly δ_j times. But note that $\operatorname{per}_\delta(A)$ is, in general, not determined by $\operatorname{per}(A\langle|\delta\rangle)$. If $(\prod_{j\in(n]} \delta_j!)\,1 = 0$ in $\mathbb{F}$, the δ-permanent $\operatorname{per}_\delta(A)$ may take arbitrary values, while $\operatorname{per}(A\langle|\delta\rangle) = 0$.

$A\langle|\delta\rangle$

The notation $A\langle k|\rangle$, with a single number $k \in \mathbb{N}$, stands for a matrix that contains each row of A exactly k times. We have some nice roles for the δ-permanent of such matrices with multiple rows:

$A\langle k|\rangle$

Lemma 1.7. *Let $\mathbb{F}$ be a field of characteristic p. For matrices $A = (a_{i,j}) \in \mathbb{F}^{m\times n}$ and tuples $\delta = (\delta_j) \in [p^h)^n$ hold:*

(i) If A contains p^h identical rows, then

$$\operatorname{per}_\delta(A) \;=\; 0 \;\;. \tag{5}$$

(ii) If A' is obtained from A by adding a multiple of one row to another, then

$$\operatorname{per}_\delta(A'\langle p^h - 1|\rangle) \;=\; \operatorname{per}_\delta(A\langle p^h - 1|\rangle) \;\;. \tag{6}$$

(iii) If $\operatorname{rank}(A) < m$, then

$$\operatorname{per}_\delta(A\langle p^h - 1|\rangle) \;=\; 0 \;\;. \tag{7}$$

Proof. To prove (i), we may suppose that the first p^h rows of A coincide. Now let $\tau\colon (m] \to (m]$ be the cyclic permutation of these rows: $\tau = (1\ 2\ \ldots\ p^h)$. For each map $\sigma\colon (m] \to (n]$ with $|\sigma^{-1}| := \bigl(|\sigma^{-1}(j)|\bigr)_{j\in(n]} = \delta$, the maps of the form $\sigma\circ\tau^i\colon (m] \to (n]$ also have the property $|\sigma^{-1}| = \delta$, and

τ

$|\sigma^{-1}|$

T_σ

$$\pi_A(\sigma') \;=\; \pi_A(\sigma'') \quad \text{for each two } \sigma', \sigma'' \in T_\sigma \;:=\; \{\, \sigma\circ\tau^i \mid 0 \le i < p^h \,\}\,. \tag{8}$$

We use this, to partition the summation range in the definition of $\operatorname{per}_\delta$, in order to bundle equal summands. As we will explain below, for every map σ,

$$p \ \text{ divides } \ |T_\sigma| \;\;, \quad \text{i.e.,} \quad |T_\sigma|\,1 \;=\; 0 \;\;, \tag{9}$$

and hence

$$\sum_{\sigma' \in T_\sigma} \pi_A(\sigma') \;=\; 0 \;\; . \tag{10}$$

It follows that indeed

$$\mathrm{per}_\delta(A) \;:=\; \sum_{\sigma\colon |\sigma^{-1}|=\delta} \pi_A(\sigma) \;=\; \sum_{T_\sigma\colon |\sigma^{-1}|=\delta} \; \sum_{\sigma' \in T_\sigma} \pi_A(\sigma') \;=\; \sum_{T_\sigma\colon |\sigma^{-1}|=\delta} 0 \;=\; 0 \;\; . \tag{11}$$

The used statement (9) holds, since the least integer $i \geq 1$ with

$$\sigma \circ \tau^i \;=\; \sigma \tag{12}$$

is a multiple of p . Otherwise,

$$1 \;=\; \gcd(i, p^h) \;=\; \alpha i + \beta p^h \quad \text{with some } \; \alpha, \beta \in \mathbb{Z} \;\; , \tag{13}$$

and hence

$$\sigma \circ \tau^1 \;\;=\;\; \sigma \circ \tau^{\alpha i + \beta p^h} \;\;=\;\; \sigma \circ (\tau^i)^\alpha \circ \mathrm{Id}^\beta \overset{(12)}{=} \sigma \;\; , \tag{14}$$

which would mean that σ is constant on all p^h points of $(p^h]$, i.e.,

$$|\sigma^{-1}(\sigma(1))| \;\geq\; p^h \;\; , \tag{15}$$

and that contradicts

$$|\sigma^{-1}| = \delta \in [p^h)^n \;\; . \tag{16}$$

Part (ii) follows through repeated applications of part (i), using the multilinearity (3) .

The last part (iii) follows from part (ii) and the well known fact that every matrix $A \in \mathbb{F}_p^{m \times n}$ with $\mathrm{rank}(A) < m$ can be transformed, by elementary row operations, into a matrix with a zero row. □

2 Main results

In this section, we investigate the distribution of the different possible values of polynomial maps $\mathbb{F}_p^n \longrightarrow \mathbb{F}_p$, $x \longmapsto P(x)$ using affine linear subspaces $v+U$ of $\mathbb{F}_p^n$ (Theorem 2.3). This leads to a sharpening (Corollary 2.4) of Warning's classical Theorem 0.3 about the number of simultaneous zeros of systems of polynomial equations over finite fields. We formulated this, and most other results of this section, for prime fields $\mathbb{F}_p$. This is a major restriction, as we will see, but it seems to be difficult to handle the more general case of arbitrary finite fields $\mathbb{F}_{p^k}$. The regrettable lack of generality can partially be compensated by Lemma 3.1 in the succeeding section. This lemma enables the application of results over finite prime fields $\mathbb{F}_p$ to arbitrary finite fields $\mathbb{F}_{p^k}$. However, there will remain a certain gap.

$v+U$

We begin this section with a series of lemmas. Already in the proof of the following technical one we will use the Combinatorial Nullstellensatz 1.2 for the first time. To this end we have to ensure that a certain "leading coefficient" is not zero, and that the multinomial coefficients in Equation (27) do not vanish modulo p. This is where we need p to be prime, which causes the restrictions of this section. Nevertheless, even for primes p the following lemma is not trivial. It forms the basis of the results in this paper:

Lemma 2.1. *Let $r \in (n]$, and define $\Delta_r := \{\, \delta \in [p)^n \mid \sum_j \delta_j = r(p-1) \,\}$. To each $0 \not\equiv \lambda = (\lambda_\delta) \in \mathbb{F}_p^{\Delta_r}$, there exists a matrix $A = (a_{i,j}) \in \mathbb{F}_p^{r\times n}$ of rank r such that* Δ_r

$$\sum\nolimits_{\delta\in\Delta_r} \lambda_\delta \operatorname{per}_\delta(A\langle p-1|\rangle) \;\neq\; 0 \;\; .$$

Proof. As $\lambda \not\equiv 0$, there is a $d \in \Delta_r$ with

$$\lambda_d \;\neq\; 0 \;\; . \tag{17}$$

Set $j_0 := 1$, and define $j_i \in (n]$ for all $i \in (r]$ as the least number with

$$\sum_{j\in(j_i]} d_j \;\geq\; (p-1)\,i \;\; . \tag{18}$$

Define

$$A'' = (a''_{i,j})_{\substack{i\in(r]\\ j\in(n]}} \quad \text{through} \quad a''_{i,j} := \begin{cases} 1 & \text{if } j_{i-1} \leq j \leq j_i\,, \\ 0 & \text{else}\,, \end{cases} \tag{19}$$

and set

$$a''_{i,*} \;:=\; (a''_{i,j})_{j\in(n]} \;\in\; \mathbb{F}_p^{1\times n} \;\; . \tag{20}$$

We want to show that

$$\operatorname{per}_d(A''\langle p-1|\rangle) \neq 0 \;\; . \tag{21}$$

To see this, realize that there is just one unique partition

$$d \;=\; d^1 + d^2 + \cdots + d^r \tag{22}$$

of the tuple $d = (d_j) \in \Delta_r \subseteq [p)^n$ into tuples $d^i = (d^i_j) \in [p)^n$ with the properties

$$j_{i-1} \;\leq\; \operatorname{supp}(d^i) \;\leq\; j_i \;\; , \tag{23}$$

i.e.,

$$a''_{i,j} \neq 0 \quad \text{ for all } \; j \in \operatorname{supp}(d^i) \;\; , \tag{24}$$

and

$$d^i_1 + d^i_2 + \cdots + d^i_n \;=\; p-1 \;\; . \tag{25}$$

Here, the last equation means that each of the unique $d^i = (d^i_1, \ldots, d^i_n)$ is itself a partition of $p-1$, so that the multinomial coefficients $\binom{p-1}{d^i} := \binom{p-1}{d^i_1,\ldots,d^i_n}$ are well-defined. From the uniqueness of the d^i follows

$$\operatorname{per}_d(A''\langle p-1|\rangle) \;=\; \prod_{i\in(r]} \operatorname{per}_{d^i}\bigl(a''_{i,*}\langle p-1|\rangle\bigr) \;=\; \prod_{i\in(r]} \binom{p-1}{d^i} 1 \;\neq\; 0 \;\; , \tag{26}$$

since

$$\binom{p-1}{d^i} \;=\; \frac{(p-1)!}{\prod_{j\in(n]} d^i_j!} \tag{27}$$

is not dividable by p for all $i \in (r]$.

Now set

$$A' := (a''_{i,j}\, X_j)_{\substack{i\in(r]\\ j\in(n]}} \;\in\; \mathbb{F}_p[X]^{r\times n} \tag{28}$$

and

$$P(X) \;:=\; \sum_{\delta\in\Delta_r} \lambda_\delta \operatorname{per}_\delta(A'\langle p-1|\rangle) \;\in\; \mathbb{F}_p[X] \;. \tag{29}$$

Then

$$\deg(P) \;\le\; r(p-1) \;=\; \textstyle\sum_j d_j \tag{30}$$

and

$$P_d\, X^d \;=\; \lambda_d \operatorname{per}_d(A'\langle p-1|\rangle) \;=\; \lambda_d \operatorname{per}_d(A''\langle p-1|\rangle)\, X^d \;\ne\; 0 \;. \tag{31}$$

Hence by Theorem 1.2, there is a $x \in \mathbb{F}_p^n$ such that

$$0 \;\ne\; P(x) \;=\; \textstyle\sum_{\delta\in\Delta_r} \lambda_\delta \operatorname{per}_\delta(A\langle p-1|\rangle) \quad \text{with } A := (a''_{i,j}\, x_j) \;\in\; \mathbb{F}_p^{r\times n}. \tag{32}$$

In this the matrix A necessarily has rank r by Lemma 1.7 (*iii*). □

Now we are able to construct our main tool:

Lemma 2.2. *Let $r \in [n]$ and an $\mathbb{F}_p$-subspace $U \le \mathbb{F}_p^n$ of dimension $\dim(U) = n - r$ be given.* U, r

There is a (generally not unique) system of polynomials $\mathbf{1}_{v+U} = \sum_{\delta\in\mathbb{N}^n} (\mathbf{1}_{v+U})_\delta X^\delta \in \mathbb{F}_p[X]$ – corresponding to the cosets $v + U \in \mathbb{F}_p^n/U$ – such that for each coset $v + U$: $(\mathbf{1}_{v+U})_\delta$

(i) $\mathbf{1}_{v+U}(x) \;=\; \begin{cases} 1 & \text{if } x \in v+U, \\ 0 & \text{if } x \in \mathbb{F}_p^n \setminus v+U; \end{cases}$ *and*

(ii) $\deg(\mathbf{1}_{v+U}) \;\le\; r(p-1)$ *; and*

(iii) $(\mathbf{1}_{v+U})_\delta \;=\; (\mathbf{1}_U)_\delta$ *for all* $\delta \;\in\; \Delta_r := \{\, \delta \in [p)^n \;\mid\; \sum_j \delta_j = r(p-1) \,\}$. Δ_r

Let $0 \not\equiv \lambda = (\lambda_\delta) \in \mathbb{F}_p^{\Delta_r}$; then the subspace U (and the polynomials $\mathbf{1}_{v+U}$) may be chosen in such a way that, in addition,

(iv) $\sum_{\delta\in\Delta_r} \lambda_\delta (\mathbf{1}_U)_\delta \;\ne\; 0$.

Proof. Let

$$\sum_{j\in(n]} a_{i,j}X_j \;=\; 0 \quad , \quad i=1,\dots,r \tag{33}$$

be a system of equations defining U ; then the polynomials

$$1_{v+U} \;:=\; \prod_{i\in(r]} \Big(1 - \Big(\sum_{j\in(n]} \big(a_{i,j}(X_j - v_j)\big)\Big)^{p-1} \Big) \;\in\; \mathbb{F}_p[X] \tag{34}$$

fulfill the conditions (i), (ii) and (iii).

Part (iv) holds for $r=0$. For $r>0$, we have to find a matrix $A=(a_{i,j})\in\mathbb{F}_p^{r\times n}$ of rank r such that the polynomial $1_U = 1_{0+U}$ defined by (34) fulfills the inequality in part (iv); the searched $(n{-}r)$-dimensional subspace U is then given through Equation (33) using this same matrix A. For $\delta\in\Delta_r$, we have

$$(1_U)_\delta \;=\; (-1)^r \big((\Pi(AX))^{p-1} \big)_\delta \;=\; (-1)^r \big(\Pi(A\langle p-1|\rangle X)\big)_\delta \overset{1.6}{=} (-1)^r \operatorname{per}_\delta(A\langle p-1|\rangle) \;\;, \tag{35}$$

and we obtain statement (iv) if we choose A by Lemma 2.1 :

$$\sum_{\delta\in\Delta_r} \lambda_\delta (1_U)_\delta \;=\; (-1)^r \sum_{\delta\in\Delta_r} \lambda_\delta \operatorname{per}_\delta(A\langle p-1|\rangle) \overset{2.1}{\neq} 0 \;\; . \tag{36}$$

□

The following main result of this paper, now tells us something about the distribution of the different possible values $P(x)$ of the polynomial maps $\mathbb{F}_p^n \longrightarrow \mathbb{F}_p$, $x \longmapsto P(x)$. We examine certain partitions (factor spaces) $\mathbb{F}_p^n/U$ of $\mathbb{F}_p^n$, and show in part (iv) that the derived maps $\mathbb{F}_p^n/U \longrightarrow \mathbb{F}_p$, $x+U \longmapsto \sum_{\tilde{x}\in x+U} P(\tilde{x})$ are constant. This and the stronger part (iii) already follow easily from [LiNi, Lemma 6.4].

What is new is that in certain cases this constant map is also not zero (part (ii)). It depends on a divisibility property of the degree $\deg(P)$ whether we can guaranty the existence of a suitable subspace U or not. The weaker version of this in part (i) does not require this property. Note also, that the restrictive assumptions about the partial degrees $\deg_{X_j}(P)$ in this theorem may be left away without losing much of its power. We will see this in the subsequent corollary below:

Theorem 2.3. *For polynomials* $0\neq P\in\mathbb{F}_p[X_1,\dots,X_n]$ *with restricted partial degrees* $\deg_{X_j}(P)\le p-1$ *for* $j=1,\dots,n$ *holds:*

(i) There exists a subspace $U\subseteq\mathbb{F}_p^n$ *of dimension* $\dim(U)=\lceil\frac{\deg(P)}{p-1}\rceil$ *such that, for all* $v\in\mathbb{F}_p^n$, $\boxed{P|_{v+U} \;\not\equiv\; 0 \;.}$

(ii) If $p-1$ *divides* $\deg(P)$ *, i.e., if* $\frac{\deg(P)}{p-1}=\lceil\frac{\deg(P)}{p-1}\rceil$ *, then:*
There exists a subspace $U\subseteq\mathbb{F}_p^n$ *of dimension* $\dim(U)=\frac{\deg(P)}{p-1}$ *such that* $\boxed{\sum_{x\in U} P(x) \;\neq\; 0 \;.}$

(iii) For any subspace $U \subseteq \mathbb{F}_p^n$ *of dimension* $\dim(U) > \frac{\deg(P)}{p-1}$ $\boxed{\sum_{x\in U} P(x) \;=\; 0\ .}$

(iv) For any subspace $U \subseteq \mathbb{F}_p^n$ *of dimension* $\dim(U) \geq \frac{\deg(P)}{p-1}$ *, and for all* $v \in \mathbb{F}_p^n$*,* $\boxed{\sum_{x\in v+U} P(x) \;=\; \sum_{x\in U} P(x)\ .}$

Proof. To prove part (i), let $d := (p-1, p-1, \ldots, p-1) \in \mathbb{N}^n$, and let X^μ be a monomial in P of maximal degree ($\mu \leq d$).
We set

$$r \;:=\; \left\lfloor \frac{\sum_j d_j - \sum_j \mu_j}{p-1} \right\rfloor \;=\; n - \left\lceil \frac{\sum_j \mu_j}{p-1} \right\rceil \;\in\; \mathbb{Z} \tag{37}$$

and

$$\Delta_r \;:=\; \{\, \delta' \in [p)^n \;\mathrel{¦}\; \textstyle\sum_j \delta'_j = r(p-1) \,\}\ . \tag{38}$$

Choose a $\delta \in \Delta_r$ with

$$\delta \;\leq\; d - \mu\ , \tag{39}$$

and set

$$\bar{d} \;:=\; \mu + \delta\ . \tag{40}$$

Define $\lambda = (\lambda_{\delta'}) \in \mathbb{F}_p^{\Delta_r}$ by setting

$$\lambda_{\delta'} \;:=\; P_{\bar{d}-\delta'} \quad (\,= 0 \ \text{ if }\ \bar{d} - \delta' \not\geq 0\ )\,. \tag{41}$$

Note that

$$\lambda \not\equiv 0 \quad \text{as} \quad \lambda_\delta = P_\mu \neq 0\ . \tag{42}$$

Now, for every $v \in \mathbb{F}_p^n$, the monomial $X^{\bar{d}}$ occurs in

$$Q \;:=\; P\,\mathbb{1}_{v+U}\ , \tag{43}$$

where U and the $\mathbb{1}_{v+U}$ are as in Lemma 2.2 (iv) . That is so, since only the monomials of maximal degree in P, respectively in $\mathbb{1}_{v+U}$, may contribute something to the coefficient $Q_{\bar{d}}$, so that

$$Q_{\bar{d}} \;=\; \sum_{\delta'\in\Delta_r} P_{\bar{d}-\delta'}(\mathbb{1}_{v+U})_{\delta'} \;\overset{2.2}{=}\; \sum_{\delta'\in\Delta_r} \lambda_{\delta'}(\mathbb{1}_U)_{\delta'} \;\overset{2.2}{\neq}\; 0\ . \tag{44}$$

It follows that for each $\bar{d}$-subgrid $\bar{\mathfrak{X}}$ of the d-grid $\mathbb{F}_p^n$

$$Q|_{\bar{\mathfrak{X}}} \;\overset{1.2}{\not\equiv}\; 0\ , \tag{45}$$

so that finally

$$Q|_{\mathbb{F}_p^n} \;\not\equiv\; 0 \quad \text{and} \quad P|_{v+U} \;\not\equiv\; 0\ . \tag{46}$$

The proofs of the parts (ii),(iii) and (iv) work almost identically. The following equation can be used instead of conclusion (45):

$$\textstyle\sum_{x\in v+U} P(x) \;=\; \sum_{x\in\mathbb{F}_p^n} Q(x) \;\overset{1.3}{=}\; (-1)^n\, Q_d\ . \tag{47}$$

Part (ii) follows from the equations (44) and (47) as $d = \bar{d}$ in this case.

As we do not need property 2.2 (iv) (and the resulting Inequality (44)) in the proof of parts (iii) and (iv), we may take Equation (43) with an arbitrary $U \leq \mathbb{F}_p^n$ to define Q. Part (iii) follows now from $\sum_j d_j > \deg(Q)$ as $Q_d = 0$ in this case. Part (iv) follows, as Q_d does not depend on v (2.2 (iii)). □

The assumption of restricted partial degrees, $\deg_{X_j}(P) \leq p-1$ for $j = 1, \ldots, n$, may seam rather restrictive. However, every map on $\mathbb{F}_p^n$ can (uniquely) be described by a (interpolation) polynomial of this type (see, e.g., [Scha, Equivalence 2.4 (i)&(iv)]). If a concrete polynomial $P \in \mathbb{F}_p[X]$ is already given, then the unique (interpolation) polynomial $P/\mathbb{F}_p^n$ with the properties $P/\mathbb{F}_p^n$

$$(P/\mathbb{F}_p^n)|_{\mathbb{F}_p^n} \;=\; P|_{\mathbb{F}_p^n} \qquad \text{and} \qquad \deg_{X_j}(P/\mathbb{F}_p^n) \;\leq\; p-1 \quad \text{for } j = 1, \ldots, n \tag{48}$$

can easily be derived from P by reduction of exponents, using that

$$x^p \;=\; x^1 \quad \text{in} \quad \mathbb{F}_p \;. \tag{49}$$

Even more, it may not even be necessary to perform this reduction, because the total degree $\deg(P)$ is an upper bound to $\deg(P/\mathbb{F}_p^n)$,

$$\deg(P/\mathbb{F}_p^n) \;\leq\; \deg(P) \;. \tag{50}$$

This is important, since in more abstract situations, when we are dealing with whole classes of polynomials, we may not be able to determine $\deg(P/\mathbb{F}_p^n)$. Then, the conclusions of Theorem 2.3, applied to $P/\mathbb{F}_p^n$, can be combined with the upper bound (50).

Furthermore, if $p-1$ divides the degrees of the homogenous components of P, then reduction of exponents, using Equation (49), does not affect this property. Therefore, $p-1$ divides also the degrees of the homogenous components of $P/\mathbb{F}_p^n$ and also $\deg(P/\mathbb{F}_p^n)$. Thus, by part (ii) and part (iv) of Theorem 2.3, there exists a subspace $U \subseteq \mathbb{F}_p^n$ of dimension

$$\dim(U) \;=\; \tfrac{\deg(P/\mathbb{F}_p^n)}{p-1} \;\leq\; \tfrac{\deg(P)}{p-1} \tag{51}$$

with the property:

$$\textstyle\sum_{x \in v+U} P(x) \;=\; \sum_{x \in U} P(x) \;\neq\; 0 \quad \text{for all } v \in \mathbb{F}_p^n \;. \tag{52}$$

With this kind of observations, we are prepared to prove the following corollary, which is a sharpening of Warning's classical result [Schm] about the number of simultaneous zeros of systems of polynomial equations over finite fields (i.e., the second inequality in part (i) below). The sharpening tells us that the simultaneous zeros are distributed over all elements of certain partitions (factor spaces) $\mathbb{F}_q^n/U$ of $\mathbb{F}_q^n$, and $p^{n-\sum_i \deg(P_i)} \leq |\mathbb{F}_q^n/U|$ is then the well known lower bound for the number of these zeros:

Corollary 2.4. *Let* $P_1, \ldots, P_m \in \mathbb{F}_p[X]$ *be polynomials with a simultaneous zero, and* $\mathcal{V} := \{\, x \in \mathbb{F}_p^n \mid P_1(x) = \cdots = P_m(x) = 0 \,\} \neq \varnothing$ *, then:*

(i) There exists a subspace $U \subseteq \mathbb{F}_p^n$ *of dimension* $\dim(U) \leq \sum_i \deg(P_i)$ *such that, for all* $v \in \mathbb{F}_p^n$*,*

$$\boxed{\mathcal{V} \cap (v+U) \neq \varnothing \ .}$$

In particular,

$$\boxed{|\mathcal{V}| \geq p^{n-\sum_i \deg(P_i)} \ .}$$

(ii) If, in addition, the polynomials P_i *are homogeneous modulo* $p-1$ *, i.e., if the homogeneous components inside any* P_i *have the same degree modulo* $p-1$ *, then:*

There exists a subspace $U \subseteq \mathbb{F}_p^n$ *of dimension* $\dim(U) \leq \sum_i \deg(P_i)$ *such that, for all* $v \in \mathbb{F}_p^n$*,*

$$\boxed{\big|\mathcal{V} \cap (v+U)\big| \equiv \big|\mathcal{V} \cap (U)\big| \not\equiv 0 \pmod{p} \ .}$$

(iii) For any subspace $U \subseteq \mathbb{F}_p^n$ *of dimension* $\dim(U) > \sum_i \deg(P_i)$

$$\boxed{\big|\mathcal{V} \cap (U)\big| \equiv 0 \pmod{p} \ .}$$

(iv) For any subspace $U \subseteq \mathbb{F}_p^n$ *of dimension* $\dim(U) \geq \sum_i \deg(P_i)$ *, and all* $v \in \mathbb{F}_p^n$*,*

$$\boxed{\big|\mathcal{V} \cap (v+U)\big| \equiv \big|\mathcal{V} \cap (U)\big| \pmod{p} \ .}$$

Proof. Define

$$P := \prod_{i \in (m]} (1 - P_i^{p-1}) \ ; \tag{53}$$

then, for each $x \in \mathbb{F}_p^n$,

$$x \in \operatorname{supp}(P) \iff P(x) \neq 0 \iff P_1(x) = \cdots = P_m(x) = 0 \iff x \in \mathcal{V} \ . \tag{54}$$

By Theorem 2.3 (i), there is a subspace $U \leq \mathbb{F}_p^n$ with

$$\dim(U) = \left\lceil \tfrac{\deg(P/\mathbb{F}_p^n)}{p-1} \right\rceil \leq \left\lceil \tfrac{\deg(P)}{p-1} \right\rceil = \sum\nolimits_i \deg(P_i) \ , \tag{55}$$

and

$$\varnothing \neq \operatorname{supp}(P|_{v+U}) = \operatorname{supp}(P) \cap (v+U) = \mathcal{V} \cap (v+U) \quad \text{for all } v \in \mathbb{F}_p^n. \tag{56}$$

This is the main statement of part (i), and the remaining lower bond for $|\mathcal{V}|$ in part (i) follows from it.

Since

$$P(x) \in \{0,1\} \quad \text{for all } x \in \mathbb{F}_p^n \ , \tag{57}$$

the parts (iii) and (iv) follow from the corresponding parts of Theorem 2.3, as part (ii) follows from observation (52). □

Our sharpening Corollary 2.4(i) could suggest that, for any subset $\tilde{\mathcal{V}} \subseteq \mathbb{F}_p^n$ with at least p^{n-m} elements, there is a subspace $U \leq \mathbb{F}_p^n$ of dimension m such that

$$\tilde{\mathcal{V}} \cap (v+U) \neq \varnothing \quad \text{for all } v \in \mathbb{F}_p^n\,. \tag{58}$$

This is not the case. If, for example, $p = 5$, $n = 2$ and $m = 1$, then any subset $\tilde{\mathcal{V}} := \{ (0,0),(0,1),(1,0),(2,2),(a,b) \} \subseteq \mathbb{F}_5^2$ of $5 = p^{n-m}$ points does not have this property. To any subspace $U \leq \mathbb{F}_p^n$ of dimension 1, there is a $v' \in \mathbb{F}_5^2$ such that $v' + U$ contains two of the "first" four elements of $\tilde{\mathcal{V}}$, so that there must be another $v \in \mathbb{F}_5^2$ with $\tilde{\mathcal{V}} \cap (v+U) = \varnothing$. In other words, the first property of the sets $\mathcal{V}$ of simultaneous zeros in Corollary 2.4(i), is something special for sets of this size.

3 Generalizations

We formulated all our results in the last section for prime fields $\mathbb{F}_p$, but we may also apply them to arbitrary finite fields $\mathbb{F}_{p^k}$ by using the following lemma. It is based on elementary techniques from field theory which were used in a similar way in [Ba, Prop. 3.3] and [MoMo, Lemma 1]. The degree restriction $\deg(\bar{P}) \leq k \deg(P)$ in this lemma can be sharpened using the so-called p-weight degree $w_p(P)$ of P. See [MoMo] for the simple idea behind this improvement, and for the definition of w_p. We provide:

Lemma 3.1. *Let $\alpha \in \mathbb{F}_{p^k}$ be a primitive element of the extension $\mathbb{F}_{p^k} \supseteq \mathbb{F}_p$, $\mathbb{F}_{p^k} = \mathbb{F}_p(\alpha)$. For each $x = (x_j) \in \mathfrak{X} := \mathbb{F}_{p^k}{}^{(n]}$, let $\bar{x} = (\bar{x}_{i,j}) \in \bar{\mathfrak{X}} := \mathbb{F}_p^{[k)\times(n]}$ be the unique point with $x_j = \bar{x}_{0,j}\alpha^0 + \cdots + \bar{x}_{k-1,j}\alpha^{k-1}$ for all $j \in (n]$, so that $x \longmapsto \bar{x}$ is a bijection $\mathfrak{X} \longrightarrow \bar{\mathfrak{X}}$.*

For each polynomial $P \in \mathbb{F}_{p^k}[X]$ with $X = (X_j)_{j\in(n]}$, there is a polynomial $\bar{P} \in \mathbb{F}_p[\bar{X}]$ with $\bar{X} = (X_{i,j})_{(i,j)\in[k)\times(n]}$ of degree $\deg(\bar{P}) \leq k\deg(P)$ such that, for all $x \in \mathfrak{X}$,

$$\boxed{\bar{P}(\bar{x}) \,=\, \mathcal{N}(P(x))}\,,$$

where $\mathcal{N} \colon \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_p$ is the norm of the field extension $\mathbb{F}_{p^k} \supseteq \mathbb{F}_p$.

If P is homogeneous then $\bar{P}$ is homogeneous as well. If all homogenous components of P have degree t modulo s, then the homogenous components of $\bar{P}$ have degree kt modulo s.

Proof. Let $A \in \mathbb{F}_p^{[k)\times[k)}$ be the companion matrix of the minimal polynomial f_α of α. We may identify $\mathbb{F}_p[A]$ with $\mathbb{F}_{p^k}$ and A with α. In this way $\mathbb{F}_{p^k}$ is a $\mathbb{F}_p$-vector space with basis $A^0,\ldots,A^{k-1}$ and a subfield of the matrix ring $\mathbb{F}_p^{[k)\times[k)}$. The norm $\mathcal{N}$ of the extension $\mathbb{F}_p(A) \supseteq \mathbb{F}_p$ is given by the determinant $\det$. (See, e.g., [DuFo] for more information about the norm and field extensions.) Now define

$$\tilde{P}(\bar{X}) \,=\, (\tilde{P}_{i,j}(\bar{X})) \;\in\; \mathbb{F}_p[A][\bar{X}] \;\subseteq\; \mathbb{F}_p^{[k)\times[k)}[\bar{X}] \;=\; \mathbb{F}_p[\bar{X}]^{[k)\times[k)} \tag{59}$$

by

$$\tilde{P}(\bar{X}) := P\big((X_{0,j}A^0 + \ldots + X_{k-1,j}A^{k-1})_{j\in(n]} \big) \ . \tag{60}$$

The entries $\tilde{P}_{i,j}(\bar{X})$ of this matrix have degree at most $\deg(P)$, so that

$$\bar{P}(\bar{X}) := \det(\tilde{P}(\bar{X})) \tag{61}$$

has degree at most $k\deg(P)$, and

$$\bar{P}(\bar{x}) = \det\big(P\big((\bar{x}_{0,j}A^0 + \ldots + \bar{x}_{k-1,j}A^{k-1})_{j\in(n]} \big) \big) = \mathcal{N}(P(x)) \ . \tag{62}$$

Since the set of the degrees of the monomials of the entries $\tilde{P}_{i,j}(\bar{X})$ is a subset of the set of the monomial degrees of P, the last part of the lemma follows immediately. □

When we combine this Lemma with Corollary 2.4(i) we obtain that, to any system of polynomial $P_1, \ldots, P_m \in \mathbb{F}_q[X]$ (where $q := p^k$), with $q := p^k$

$$\mathcal{V} := \{ x \in \mathbb{F}_q^n \mid P_1(x) = \cdots = P_m(x) = 0 \} \neq \varnothing \ , \tag{63}$$

there exists an $\mathbb{F}_p$-linear subspace $U \subseteq \mathbb{F}_q^n$ of $\mathbb{F}_p$-dimension

$$\dim_{\mathbb{F}_p}(U) \leq k \sum_{i\in(m]} \deg(P_i) \tag{64}$$

such that

$$\mathcal{V} \cap (v + U) \neq \varnothing \quad \text{for all } v \in \mathbb{F}_q^n \ . \tag{65}$$

If it happens that this subspace is also an $\mathbb{F}_q$-linear subspace, then it has $\mathbb{F}_q$-dimension

$$\dim_{\mathbb{F}_q}(U) = \tfrac{\dim_{\mathbb{F}_p}(U)}{k} \leq \sum_{i\in(m]} \deg(P_i) \tag{66}$$

and Corollary 2.4(i) would hold with q in the place of p. The only reason why we have not been able to prove the existence of such an $\mathbb{F}_q$-subspace is, that the multinomial coefficient in Equation (27) (in the proof of the main Lemma 2.1), with $q > p$ in the place of p, usually vanishes modulo p. This leads us to the following concluding conjectures:

Conjecture 3.2. *Let $P_1, \ldots, P_m \in \mathbb{F}_q[X]$ be polynomials with a simultaneous zero, and define $\mathcal{V} := \{ x \in \mathbb{F}_p^n \mid P_1(x) = \cdots = P_m(x) = 0 \} \neq \varnothing$:*

There exists an $\mathbb{F}_q$-subspace $U \subseteq \mathbb{F}_p^n$ of $\mathbb{F}_q$-dimension $\dim_{\mathbb{F}_q}(U) \leq \sum_i \deg(P_i)$ such that $\mathcal{V} \cap (v + U) \neq \varnothing$ for all $v \in \mathbb{F}_q^n$.

This conjecture would follow from the following stronger one:

Conjecture 3.3. *To any polynomial $P \in \mathbb{F}_q[X_1, \ldots, X_n]$ with $P|_{\mathbb{F}_q^n} \not\equiv 0$, there exists an $\mathbb{F}_q$-linear subspace $U \subseteq \mathbb{F}_q^n$ of $\mathbb{F}_q$-dimension $\dim_{\mathbb{F}_q}(U) \leq \lceil \frac{\deg(P)}{q-1} \rceil$ such that $P|_{v+U} \not\equiv 0$ for all $v \in \mathbb{F}_q^n$.*

Note that, in the case of the second conjecture, not even an adequate $\mathbb{F}_p$-subspace U, with corresponding $\mathbb{F}_p$-dimension

$$\dim_{\mathbb{F}_p}(U) \;\leq\; k\left\lceil \tfrac{\deg(P)}{q-1} \right\rceil \;, \tag{67}$$

can be guaranteed using Lemma 3.1 and our prime field version Theorem 2.3. Only a $\mathbb{F}_p$-subspace U of $\mathbb{F}_p$-dimension

$$\dim_{\mathbb{F}_p}(U) \;\leq\; \left\lceil \tfrac{k\deg(P)}{p-1} \right\rceil \tag{68}$$

(with $p-1$ instead of $q-1$ in the nominator) can be guaranteed in this way.

Acknowledgement:
We are grateful to the referee for his/her interesting and useful comments. Furthermore, the author gratefully acknowledges the support provided by the King Fahd University of Petroleum and Minerals, the Technical University of Berlin and the Eberhard Karls University of Tübingen during this research.

References

[AdSp] A. Adolphson, S. Sperber:
p-adic Estimates for Exponential Sums and the Theorem of Chevalley-Warning.
Ann. Sci. École Norm. Sup. (4) 20 (1987), 545-556.

[AdSp2] A. Adolphson, S. Sperber: p-adic Estimates for Exponential Sums.
Lecture Notes in Math., Vol. 1454, Springer, Berlin and New York, 1990, 11-22.

[Al] N. Alon: Combinatorial Nullstellensatz.
Combin. Probab. Comput. 8, No. 1-2 (1999), 7-29.

[AlTa] N. Alon, M. Tarsi: A Nowhere-Zero Point in Linear Mappings.
Combinatorica 9 (1989), 393-395.

[Ar] E. Artin: Collected Papers.
Springer, New York 1965.

[Ax] J. Ax: Zeros of Polynomials over Finite Fields.
Amer. J. Math. 86 (1964), 255-261.

[Ba] D. A. M. Barrington:
Some Problems Involving Razborov-Smolensky Polynomials.
Boolean Function Complexity, ed. M. S. Patterson, London Math. Soc. Lecture Note Series 169, Cambridge University Press 1992a, 109-128.

[DuFo] D. S. Dummit, R. M. Foote: Abstract Algebra.
John Wiley and Sons, Inc. 2004.

[Ka] N. M. Katz: On a Theorem of Ax.
Amer. J. Math. 93 (1971), 485-499.

[LiNi] R. Lidl, H. Niederreiter: Finite Fields.
Encyclo. Math. and its Appl. 12, Cambridge University Press 1997.

[Minc] H. Minc: Permanents. *Addison-Wesley, London 1978.*

[MSCK] O. Moreno, K. W. Shum, F. N. Castro, P. V. Kumar:
Tight Bounds for Chevalley-Warning-Ax-Katz Type Estimates, with Improved Applications. *Proc. London Math. Soc. (3) 88 (2004), 545-564.*

[MoMo] O. Moreno, C. J. Moreno:
Improvements of the Chevalley-Warning and the Ax-Katz Theorems.
American Journal of Mathematics, Vol. 117, No. 1, (1995), 241-244.

[Scha] U. Schauz: Algebraically Solvable Problems: Describing Polynomials as Equivalent to Explicit Solutions. *The Electronic Journal of Combinatorics 15 (2008), #R10.*

[Schm] W. M. Schmidt: Equations over Finite Fields.
Lecture Notes in Math., Vol. 536, Springer, Berlin and New York 1976.

[Sp] S. Sperber: On the p-adic Theory of Exponential Sums.
Amer. J. Math. 108 (1986), 255-296.

[Wan] D. Wan: An Elementary Proof of a Theorem of Katz.
Amer. J. Math. 111 (1989), 1-8.

[Wan2] D. Wan: A Chevalley-Warning Approach to p-adic Estimates of Character Sums.
Proceedings of the American Mathematical Society, Vol. 123 No. 1 (1995), 45-54.

[Ya] Yu Yang: The Permanent Rank of a Matrix.
J. Combin. Theory Ser. A 85(2) (1999), 237-242.