SYSTEMS OF POLYNOMIALS OVER FINITE FIELDS

KARIM JOHANNES BECHER

ABSTRACT. We present a famous theorem about systems of polynomial equations over a finite field, the *Chevalley-Warning theorem*. We mention some questions of recent study in this context.

1. Introduction

Let F be a finite set and let $n, r \in \mathbb{N}$. We consider a function $g : F^n \to F^r$. We can ask what a value $g(x)$ tells us about the input $x \in F$, depending on our knowledge about the function g. Formally, we consider for a point $y \in F^r$ the preimage $g^{-1}(y) = \{x \in F^n \mid g(x) = y\}$, also called the *fibre of* y (w.r.t. g).

We will now delve into a context of algebra where the function g is given by some computation rule. We will then encounter some conditions on g that have a strong impact on the fibres and their cardinalities.

The context is that of a finite field. By a *field*, we mean a structure $(F, +, \cdot, 0, 1)$ where F is a set, 0 and 1 are two different distinguished elements of F, and where $+$ and $\cdot$ are binary operations $F \times F \to F$ called *addition* and *multiplication* satisfying the usual rules of arithmetic. (By this, we mean that each of $+$ and $\cdot$ are commutative and associative and that together they satisfy the distributivity law, further that 0 and 1 are neutral elements for $+$ and for $\cdot$, respectively, that elements of F have inverses for $+$ and elements of $F \smallsetminus \{0\}$ have inverses for the multiplication. This allows one to define the derived operations *subtraction* $- : F \times F \to F$ and *inversion* $^{-1} : F \smallsetminus \{0\} \to F$.)

Typical fields used in all areas of mathematics are $\mathbb{Q}$ (the rational numbers), $\mathbb{R}$ (the real numbers) and $\mathbb{C}$ (the complex numbers). But there are also finite fields. Those are very interesting for applications, such as in cryptography. Note that the set of integers $\mathbb{Z}$ satisfies most of the prerequisites of a field, but is lacking inverses for the multiplication.

We fix now a prime number p. Modular arithmetic for integers modulo p defines a field with p elements. As a set, this is $\{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$, where we define the operations just as for integers, but apply division with residue to any sum or product, so as to always end up with a computation result in this set. We denote this field by $\mathbb{Z}/p\mathbb{Z}$ or by $\mathbb{F}_p$.

These give a crucial class of examples of finite fields, which have a prime number as their cardinality. There also exists for any $k \in \mathbb{N} \smallsetminus \{0\}$ a field with p^k elements,

Date: 20.11.2023.

and their construction is a bit more involved. In the sequel, the field $\mathbb{F}_p$ may serve as a guiding example.

Given a field F, we can consider functions $g : F^n \to F^r$ given by polynomials. In fact, in the case where F is a finite field, all functions are given by the evaluation of some system of polynomials $g = (g_1, \ldots, g_r)$, that is, where $g_i \in F[X_1, \ldots, X_n]$ for $1 \leqslant i \leqslant r$, that is, $g_1, \ldots, g_r$ are polynomials with coefficients in F in the variables $X_1, \ldots, X_n$. In our main case of interest, we can understand these polynomials given with coefficients in $\mathbb{Z}$. An example is $X_1X_2 - 4X_3^2 - 3X_2X_4$. A product $cX_1^{e_1} \cdots X_n^{e_n}$ with $(e_1, \ldots, e_n) \in \mathbb{N}^n$ and $c \in F \smallsetminus \{0\}$ is called a *monomial*, and we call the number $e = e_1 + \cdots + e_n$ its *degree*. The *degree* of an arbitrary polynomial g is defined as the maximum of the degrees of the monomials that occur in it and denoted by $\mathsf{deg}(g)$.

2. The Chevalley-Warning theorems

Let p be a prime number and $F = \mathbb{Z}/p\mathbb{Z}$. Let $g_1, \ldots, g_r \in F[X_1, \ldots, X_n]$. Let $d = \mathsf{deg}(g_1) + \cdots + \mathsf{deg}(g_r)$. Consider the evaluation function

$$g : F^n \to F^r, x \mapsto (g_1(x), \ldots, g_r(x)) .$$

2.1. **Theorem** (Chevalley-Warning, 1935). *Assume that $d < n$. For any $y \in F^r$, $|g^{-1}(y)|$ is a multiple of p, and if $g^{-1}(y) \neq \emptyset$, then $|g^{-1}(y)| \geqslant p^{n-d}$.*

The proof is surprisingly simple. If makes crucial use of *Fermat's Little Theorem*, which says that $x^{p-1} = 1$ for any $x \in F \smallsetminus \{0\}$.

The proof can be reduced to the case where $n = d + 1$. In that case, the theorem needs only to be proven for $y = 0$. Indeed, if $y = (y_1, \ldots, y_r)$, we set $g_i' = g_i - y_i$ for $1 \leqslant i \leqslant r$, and obtain for the resulting $g' : F^n \to F^r$ the same degree and $g^{-1}(y) = g'^{-1}(0)$.

In the proof, one considers the *Chevalley polynomial* given by g, which is

$$\chi_g = \textstyle\prod_{i=1}^r (1 - g_i^{p-1}) .$$

It has $\mathsf{deg}(\chi_g) = d(p-1)$ and the curious property that, for any $x \in F^n$,

$$\chi_g(x) = \begin{cases} 1 & \text{if } g(x) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

A new proof of the refined statement above can be found in [1].

2.2. **Theorem** (Heath-Brown, 2011). *Assume that $d < n$ and that $y \in F^r$ is such that $|g^{-1}(y)| = p^{n-d}$. Then $g^{-1}(y)$ is an $(n-d)$-dimensional affine subspace of F^r.*

2.3. **Theorem** (Heath-Brown 2011, Leep-Petrik, 2023). *Assume that $d < n$ and $p \geqslant 3$. Let $y \in F^r$. Then $g^{-1}(y) = \emptyset$ or $|g^{-1}(y)| = p^{n-r}$ or $|g^{-1}(y)| \geqslant 2p^{n-r}$.*

A particular study for the case $p = 2$ was recently undertaken by D. Leep, reaching optimal results on the lowest possible cardinalities of the fibres larger than 2^{n-d}, for all pairs (n, d).

2.4. **Theorem** (Clark-Genao-Saia, 2021)**.** *Assume that* $d = n$. *For any* $y, y' \in F^r$, *we have* $|g^{-1}(y)| \equiv |g^{-1}(y')| \bmod p$. *In particular, either* $|g^{-1}(y)|$ *is a multiple of* p *for all* $y \in F^r$, *or* $g : F^n \to F^r$ *is surjective.*

In the case where $d = n$, sufficient conditions of a different type for all fibres having cardinality a multiple of p were given in [7, Theorem 3.1].

Most of the above results hold more generally for finite fields F with $p = |F|$ being a prime power. In that situation, the fact that in the case $d < n$ the fibres have cardinality divisible by p is more difficult, and goes back to [2].

For example, one can look at the field with 4 elements

$$\mathbb{F}_4 = \{\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)\} .$$

Over this field, the *Fermat cubic* $g = X_1^3 + X_2^3 + X_3^3$ gives a nice example of a polynomial of degree 3 in 3 variables such that $g : F^3 \to F$ is not surjective and the fibres have cardinality 28 and 36.

References

[1] S. Asgarli. A new proof of Warning's second theorem. Amer. Math. Monthly 125 (2018) 549–553.
[2] J. Ax. Zeroes of polynomials over finite fields. Am. J. Math. 86 (1964) 255–261.
[3] C. Chevalley. Démonstration d'une hypothèse de M. Artin. Abh. Math. Semin. Univ. Hamb. 11 (1) (1935) 73–75.
[4] P.L. Clark, T. Genao, F. Saia. Chevalley-Warning at the boundary. Expo. Math. 39 (2021), 604–623.
[5] D.R. Heath-Brown. On Chevalley-Warning theorems. Usp. Mat. Nauk 66 (2(398)) (2011) 223–232.
[6] D.B. Leep, R.L. Petrik. Further improvements to the Chevalley-Warning theorems. Finite Fields Appl.89 (2023), Paper No. 102194, 16 pp.
[7] H. Pasten. On the Chevalley-Warning theorem when the degree equals the number of variables. Combinatorica 42 (2022), 1481–1486.
[8] E. Warning. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. Abh. Math. Semin. Univ. Hamb. 11 (1) (1935) 76–83.

University of Antwerp, Department of Mathematics, Middelheimlaan 1, 2020 Antwerp, Belgium.

Email address: karimjohannes.becher@uantwerpen.be