ON THE CHEVALLEY-WARNING THEOREM WHEN THE DEGREE EQUALS THE NUMBER OF VARIABLES

HECTOR PASTEN

Abstract. Let f be a degree d polynomial in n variables defined over a finite field k of characteristic p and let N be the number of zeros of f in k^n. The Chevalley-Warning theorem asserts that if $d < n$ then N is divisible by p. In this note we show a version of the result for $d = n$.

1. Introduction

Let p be a prime, let $q = p^s$ for some integer $s \geq 1$, and let $k = \mathbb{F}_q$. Let us recall the classical Chevalley-Warning theorem [5, 13].

Theorem 1.1. *Let $n \geq 2$. Let $f_1, ..., f_r \in k[x_1, ..., x_n]$ be polynomials of degrees $d_j = \deg(f_j) \geq 1$ for each $1 \leq j \leq r$ and let $d = d_1 + ... + d_r$. Let Z be the set of common zeros of these polynomials in k^n. If $d < n$, then $\#Z \equiv 0 \bmod p$.*

Several generalizations are available in the literature, see for instance [1, 2, 3, 7, 9, 11, 12]. In this note we give an extension to the case $d = n$. More precisely, to the polynomials $f_1, ..., f_r$ we attach a certain additive sub-monoid Δ of the natural numbers, and show that $\#Z \equiv 0 \bmod p$ provided that $q - 1 \notin \Delta$. As we will see in Section 4, the hypothesis $q - 1 \notin \Delta$ is optimal in some cases. We also discuss various conditions that imply the aforementioned hypothesis.

From a geometric point of view, the case $d = n$ naturally appears when one considers the k-rational points of varieties with trivial canonical sheaf. Namely, if $X \subseteq \mathbb{P}^{n-1}$ is a smooth projective complete intersection variety defined over k by homogeneous polynomials $f_1, ..., f_r \in k[x_1, ..., x_n]$ with $\dim X = n - 1 - r$, the condition that X has trivial canonical sheaf means $\deg(f_1) + ... + \deg(f_r) = n$. See Exercise II.8.4(e) in [8] for details. In fact, the example that we discuss in Section 4 regarding optimality of the condition $q - 1 \notin \Delta$ arises from an elliptic curve, and elliptic curves are precisely the curves with trivial canonical sheaf.

2. Notation

We write $\mathbb{N} = \{0, 1, 2, ...\}$. The support of $x_1^{e_1} \cdots x_n^{e_n}$ is $(e_1, ..., e_n) \in \mathbb{N}^n$. If $f \in k[x_1, ..., x_n]$ is homogeneous, its support is the set $\mathrm{supp}(f) \subseteq \mathbb{N}^n$ consisting of the support of each monomial appearing in f. If $f_1, ..., f_r \in k[x_1, ..., x_n]$ are homogeneous, we let $\mathrm{supp}(f_1, ..., f_r) = \bigcup_{j=1}^r \mathrm{supp}(f_j)$.

The highest degree homogeneous part of a polynomial $f \in k[x_1, ..., x_n]$ is denoted by $\widehat{f}$. Given $f_1, ..., f_r \in k[x_1, ..., x_n]$ (not necessarily homogenous) we define $\mathrm{supp}(f_1, ..., f_r) = \mathrm{supp}(\widehat{f}_1, ..., \widehat{f}_r)$.

If $S \subseteq \mathbb{N}^n$, let $\mathrm{Mon}(S) \subseteq \mathbb{N}^n$ be the monoid generated by S. For $f_1, ..., f_r \in k[x_1, ..., x_n]$ let

$$\Delta(f_1, ..., f_r) = \{m \in \mathbb{N} : (m, ..., m) \in \mathrm{Mon}(\mathrm{supp}(f_1, ..., f_r))\}$$

and observe that $\Delta(f_1, ..., f_r)$ is an additive sub-monoid of $\mathbb{N}$.

In the following examples we take $n \geq 2$.

Date: November 8, 2021.

2010 *Mathematics Subject Classification.* Primary 11T06; Secondary 05E14, 11G25.

This research was supported by ANID (ex CONICYT) FONDECYT Regular grant 1190442 from Chile.

Example 2.1. Let $f_1, ..., f_r \in k[x_1, ..., x_n]$. Suppose that the convex hull of $\mathrm{supp}(f_1, ..., f_r)$ in $\mathbb{R}^n$ does not contain a vector of the form $(\lambda, ..., \lambda)$ for $\lambda \in \mathbb{R}_{>0}$. Then $\Delta(f_1, ..., f_r) = \{0\}$.

Example 2.2. Let $f_1, ..., f_r \in k[x_1, ..., x_n]$ be polynomials of degree $d_j = \deg(f_j)$ such that for each $1 \leq j \leq r$ we have $\widehat{f_j} = a_j x_1^{d_j} + h_j$ for certain $a_j \in k$ and $h_j \in k[x_2, ..., x_n]$. Then $\Delta(f_1, ..., f_r) \subseteq \delta\mathbb{N}$ where $\delta = \gcd(d_1, ..., d_r)$.

Example 2.3. For $m = (m_1, ..., m_n) \in \mathbb{N}^n$ let $\|m\| = \max_i m_i$, and for $S \subseteq \mathbb{N}^n$ let $\mu(S) = \min_{m \in S} \|m\|$. Given $f_1, ..., f_r \in k[x_1, ..., x_n]$ we define $\mu(f_1, ..., f_r) = \mu(\mathrm{supp}(f_1, ..., f_r))$. Then we have $\Delta(f_1, ..., f_r) \cap \{0, 1, ..., \mu - 1\} = \{0\}$ where $\mu = \mu(f_1, ..., f_r)$.

3. Chevalley-Warning when $d = n$

Our main result is the following.

Theorem 3.1. *Let $n \geq 2$. Let $f_1, ..., f_r \in k[x_1, ..., x_n]$ be polynomials of degrees $d_j = \deg(f_j) \geq 1$ for each $1 \leq j \leq r$, such that $d_1 + ... + d_r = n$. Let Z be the set of common zeros of these polynomials in k^n. If $q - 1 \notin \Delta(f_1, ..., f_r)$, then $\#Z \equiv 0 \bmod p$.*

For other results related to the case $d = n$ in the Chevalley-Warning theorem, see [6].

Remark 3.2. In the setting of Theorem 3.1, if each f_j is homogeneous, we can consider the set $V \subseteq \mathbb{P}^{n-1}(k)$ of its common zeros defined over k in the $(n-1)$-dimensional projective space. Since the trivial zero belongs to Z, the conclusion $\#Z \equiv 0 \bmod p$ becomes $\#V \equiv 1 \bmod p$. In particular, V is non-empty.

For a function $g : k^n \to k$ we define $S_n(g) = \sum_{a \in k^n} g(a)$. In particular, this definition applies when g is a polynomial with coefficients in k. The following lemma is straightforward.

Lemma 3.3. *Let $e \geq 0$. Consider the monomial $x^e \in k[x]$, with the convention that x^0 is 1. If $e < q - 1$ then $S_1(x^e) = 0$. On the other hand, $S_1(x^{q-1}) = -1$.*

Proof of Theorem 3.1. We follow the strategy in Ax's proof of the Chevalley-Warning theorem [2].

Consider $F = \prod_{j=1}^r (1 - f_j^{q-1}) \in k[x_1, ..., x_n]$. One readily checks that the function $F : k^n \to k$ defined by F is the characteristic function of Z with values in k. In particular, $S_n(F) = \#Z \bmod p$.

Notice that F is a k-linear combination of monomials of the form $x_1^{e_1} \cdots x_n^{e_n}$ where $\sum_{i=1}^n e_i \leq \deg(F) = (q-1)n$. Thus, $S_n(F)$ is a k-linear combination of terms of the form $S_n(x_1^{e_1} \cdots x_n^{e_n})$ with $\sum_{i=1}^n e_i \leq (q-1)n$. The assumption $q - 1 \notin \Delta(f_1, ..., f_r)$ implies that the monomial $x_1^{q-1} \cdots x_n^{q-1}$ does not appear in F. By Lemma 3.3, $S_n(x_1^{e_1} \cdots x_n^{e_n}) = \prod_{i=1}^n S_1(x^{e_i})$ is non-zero only when $e_i = q-1$ for each i, but the term $S_n(x_1^{q-1} \cdots x_n^{q-1})$ does not contribute to $S_n(F)$. $\square$

4. Optimality of the condition $q - 1 \notin \Delta(f_1, ..., f_r)$.

Using the theory of elliptic curves, let us provide an example showing that the condition $q - 1 \notin \Delta(f_1, ..., f_r)$ in Theorem 3.1 is optimal in some cases.

Let p be a prime and let $f_p = x_1^3 - x_2^2 x_3 + x_3^3 \in \mathbb{F}_p[x_1, x_2, x_3]$. Let $V_p \subseteq \mathbb{P}^2(\mathbb{F}_p)$ be the set of zeros of f_p over $\mathbb{F}_p$ in the projective plane. We have $\mathrm{supp}(f_p) = \{(3,0,0), (0,2,1), (0,0,3)\}$ and $\Delta(f_p) = 6\mathbb{N}$. Theorem 3.1 ensures that $\#V_p \equiv 1 \bmod p$ for each prime p with $6 \nmid p - 1$, that is, for $p = 3$ and $p \equiv 2 \bmod 3$ (cf. Remark 3.2). We claim that for all primes $p \equiv 1 \bmod 3$ we actually have $\#V_p \not\equiv 1 \bmod p$.

For $p \geq 5$ the equation $f_p = 0$ defines an elliptic curve E_p over $\mathbb{F}_p$. Let $a_p = p + 1 - \#V_p$ as usual. Note that E_p is the reduction modulo p of the CM elliptic curve E with affine equation $y^2 = x^3 + 1$ over $\mathbb{Q}$, for which it is known that $a_p = 0$ if $p \equiv 2 \bmod 3$ and $a_p \neq 0$ for all primes $p \equiv 1 \bmod 3$

(see below). In the latter case, by Hasse's bound we see that in fact $p \nmid a_p$, for otherwise a_p would be a non-zero integer divisible by p with $|a_p| < 2\sqrt{p}$.

Therefore, for all primes $p \equiv 1 \bmod 3$ we have $\#V_p \not\equiv 1 \bmod p$, as claimed.

The fact that $a_p \neq 0$ for all primes $p \equiv 1 \bmod 3$ follows from a more precise classical result going back to Gauss and Jacobi: Every prime $p \equiv 1 \bmod 3$ can be written as $p = A_p^2 + 3B_p^2$ with A_p, B_p integers satisfying $a_p = 2A_p$. More generally, see Theorem 4 in Ch. 18 of [10].

5. Some special cases

Corollary 5.1. *Let $n \geq 2$. Let $f_1, ..., f_r \in k[x_1, ..., x_n]$ be polynomials of degrees $d_j = \deg(f_j) \geq 1$ for each $1 \leq j \leq r$, such that $d_1 + ... + d_r = n$. Let Z be the set of common zeros of these polynomials in k^n. Suppose that at least one of the following conditions holds:*

(i) *The convex hull of $\mathrm{supp}(f_1, ..., f_r)$ in $\mathbb{R}^n$ does not contain a vector of the form $(\lambda, ..., \lambda)$ for $\lambda \in \mathbb{R}_{>0}$.*

(ii) *For each $1 \leq j \leq r$ we have $\widehat{f_j} = a_j x_1^{d_j} + h_j$ for certain $a_j \in k$ and $h_j \in k[x_2, ..., x_n]$, and moreover $\delta = \gcd(d_1, ..., d_r)$ does not divide $q - 1$.*

(iii) *$q \leq \mu(f_1, ..., f_r)$.*

Then $\#Z \equiv 0 \bmod p$.

Proof. This is a direct consequence of Theorem 3.1 and the Examples 2.1, 2.2, and 2.3. □

Remark 5.2. If (i) holds in Corollary 5.1 with $r = 1$, then we obtain a result of Adolphson and Sperber (cf. the discussion after Corollary 2.9 in [1]).

Remark 5.3. The condition $\widehat{f_j} = a_j x_1^{d_j} + h_j$ in (ii) of Corollary 5.1 agrees with Cao's notion of isolated variable in [4].

Remark 5.4. The condition $\delta \nmid q - 1$ in (ii) of Corollary 5.1 cannot be completely dropped. Indeed, consider $q = p \equiv -1 \bmod 4$ and $f = x_1^2 + x_2^2 \in \mathbb{F}_p[x_1, x_2]$. Then $\delta = 2$ divides $p - 1$, while $\#Z = 1$. See also the example in Section 4 taking $\delta = 3$.

Remark 5.5. In general, the inequality $q \leq \mu = \mu(f_1, ..., f_r)$ in (iii) of Corollary 5.1 cannot be relaxed. For instance, consider $q = p = 3$ and $f = x_1^2 + x_2^2 \in \mathbb{F}_p[x_1, x_2]$ as in the previous remark. In this case $\mu = 2$ and $q = 3$, so that $q = \mu + 1$, while $\#Z = 1$.

6. Acknowledgments

This research was supported by ANID (ex CONICYT) FONDECYT Regular grant 1190442 from Chile.

References

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

[2] J. Ax, *Zeros of polynomials over finite fields.* Amer. J. Math. 86 (1964), p. 255-261.

[3] D. Brink, *Chevalley's theorem with restricted variables.* Combinatorica 31 (2011), 127-130.

[4] W. Cao, *A partial improvement of the Ax-Katz theorem.* J. Number Theory 132 (2012), no. 4, 485-494.

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

[6] P. Clark, T. Genao, F. Saia, *Chevalley-Warning at the boundary.* Expositiones Mathematicae. Available online 25 May 2021.

[7] H. Esnault, *Varieties over a finite field with trivial Chow group of 0-cycles have a rational point.* Invent. Math. 151 (2003), 187-191.

[8] R. Hartshorne, *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[9] D. R. Heath-Brown, *On Chevalley-Warning theorems.* Uspekhi Mat. Nauk 66 (2011), 223-232; translation in: Russian Math. Surveys 66 (2011), 427-436.

[10] K. Ireland, M. Rosen, *A classical introduction to modern number theory.* Second Edition, Grad. Texts in Math. 84, Springer, New York, 1990.

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

[12] O. Moreno, C. Moreno, *Improvements of the Chevalley-Warning and the Ax-Katz theorems.* Amer. J. Math. 117 (1995), no. 1, 241-244.

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

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile

Email address, H. Pasten: hpasten@gmail.com