# AN IMPROVEMENT TO CHEVALLEY'S THEOREM WITH RESTRICTED VARIABLES

FRANCIS N. CASTRO, OSCAR E. GONZÁLEZ, AND LUIS A. MEDINA

Abstract. Recently Schauz and Brink independently extended Chevalley's theorem to polynomials with restricted variables. In this note we give an improvement to Schauz-Brink's theorem via the ground field method. The improvement is significant in the cases where the degree of the polynomial is large compared to the weight of the degree of the polynomial.

## 1. Introduction

Chevalley's 1935 theorem [Che35] settled a conjecture of Artin that finite fields are quasi-algebraically closed. This was done by proving that a set of polynomials $F_j(X_1, \ldots, X_n)$ without constant terms over a finite field $\mathbb{F}_q$ has a nontrivial common zero $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$ if the number of variables $n$ exceeds the sum of total degrees. In general, the determination of the solvability of a system of polynomials equations over subsets of finite fields is a hard problem. Many improvements of Chevalley's theorem have been given throughout the years, most notably by Warning [War35], Ax [Ax64] and Katz [Kat71]. See also [AS87, MSCK04, CCV12]. In this note we improve Schauz-Brink's result for certain types of subsets of finite fields.

Recently Schauz [Sch08] and Brink [Bri11] gave an extension of Chevalley's theorem to polynomials with variables belonging to arbitrary non-empty subsets of a finite field using Alon's Nullstellensatz. Here we apply the ground field method to this result. The improvements are sizable when the degree of the polynomials is large compared to the weight of the degree, as is illustrated in Example 8. (The $k$-ary weight $w_k(n)$ of an integer $n$ is the sum of the digits of $n$, when $n$ is written in base $k$.) Our result is the following:

**Theorem 1.** *Let $q = p^f$ and $q' = p^e$ where $e \mid f$. Consider polynomials $F_1(X_1, \ldots, X_n), \ldots, F_t(X_1, \ldots, X_n)$ over a finite field $\mathbb{F}_q$. Let $A_{ih} \subset \mathbb{F}_{q'}$ for $i = 1, \ldots, n$ and $h = 1, \ldots, \frac{f}{e}$ and*

$$A_i = \{\sum_{h=1}^{f/e} a_{ih}\alpha_h \,|\, a_{ih} \in A_{ih} \ \text{ and } \{\alpha_h\} \ \text{ is a basis of } \mathbb{F}_q \text{ over } \mathbb{F}_{q'}\},$$

*for $i = 1, \ldots, n$. Suppose that*

$$\sum_{i=1}^{n}\sum_{h=1}^{f/e}(|A_{ih}| - 1) > \frac{f(q'-1)}{e}\sum_{j=1}^{t} w_{q'}(F_j).$$

*Then the solution set $V = \{\mathbf{a} \in \prod_{i=1}^n A_i \,|\, F_j(\mathbf{a}) = 0 \ \forall j\}$ with variables restricted to the $A_i$'s is not a singleton.*

*Date*: March 11, 2019.

2010 *Mathematics Subject Classification.* 11T06.

*Key words and phrases.* Solvability of systems of polynomials over finite fields; Chevalley's theorem.

## 2. Preliminaries

**Definition 2.** *Let $q$, $n$ be natural numbers with $q > 1$. The $q$-weight of $n$, denoted by $\sigma_q(n)$, is the sum of the digits of $n$ in base $q$, i.e., if $n = a_0 + a_1 q + \cdots + a_r q^r$ with $a_i \in \{0, 1, \ldots, q-1\}$, then $\sigma_q(n) = \sum_{\ell=0}^{r} a_\ell$.*

**Example 3.** *We have $\sigma_2(23) = 4$, since $23 = 1 + 2 + 2^2 + 2^4$; $\sigma_6(23) = 8$ since $23 = 5 + 6 \cdot 3$.*

**Definition 4.** *Let $F(X_1, \ldots, X_n) = \sum_{\ell=1}^{r} a_\ell X_1^{e_{1\ell}} \cdots X_n^{e_{n\ell}}$ be a polynomial over $\mathbb{F}_q = \mathbb{F}_{p^f}$ with $a_l \neq 0$. The $q$-weight degree of $f$ is defined by $w_q(f) = \max_\ell \sum_{j=1}^{n} \sigma_q(e_{j\ell})$.*

**Example 5.** *Let $F(X_1, \ldots, X_n) = X_1^{2q+1} + \cdots + X_n^{2q+1}$ be a polynomial over $\mathbb{F}_{q^f}$ . Then $w_q(F) = 2$ if $q = 2$ and $w_q(F) = 3$ otherwise.*

In [Sch08, Corollary 3.5] and [Bri11, Theorem 1] a version of Chevalley's theorem with restricted variables was presented. We now state the Schauz-Brink theorem.

**Theorem 6** (Schauz-Brink)**.** *Consider polynomials $F_1(X_1, \ldots, X_n), \ldots, F_t(X_1, \ldots, X_n)$ over a finite field $\mathbb{F}_q$. Suppose that $A_1, ..., A_n$ are non-empty subsets of $\mathbb{F}_q$ such that*

$$\sum_{i=1}^{n} (|A_i| - 1) > (q-1) \sum_{j=1}^{t} \deg(F_j).$$

*Then the solution set $V = \{\mathbf{a} \in \prod_{i=1}^{n} A_i \mid F_j(\mathbf{a}) = 0 \ \forall j\}$ with the variables restricted to the $A_i$'s is not a singleton.*

The following lemma will be used in the proof of Theorem 1.

**Lemma 7.** *Let $\{F_j\}_{j=1,\ldots,t}$ be a system of $t$ polynomials in the $n$ variables $X_1, \ldots, X_n$ defined over $\mathbb{F}_q = \mathbb{F}_{p^f}$ and let $q' = p^e$ where $e \mid f$. Let $\alpha_1, \ldots, \alpha_{f/e}$ be a basis for $\mathbb{F}_q$ over $\mathbb{F}_{q'}$. Let $N(\{F_j\}, \mathbb{F}_q)$ be the number of solutions of the system $F_j = 0 \ \forall j$ over $\mathbb{F}_q$. Then there exists a system $\{G_{jh}\}_{\substack{j=1,\ldots,t \\ h=1,\ldots,f/e}}$ of $\frac{tf}{e}$ polynomials in $\frac{nf}{e}$ variables over the field $\mathbb{F}_{q'} = \mathbb{F}_{p^e}$ given by $F_j(X_1, \ldots, X_n) = \sum_{h=1}^{f/e} G_{jh}(Y_{11}, Y_{12}, \ldots, Y_{1\frac{f}{e}}, \ldots, Y_{n1}, Y_{n2}, \ldots, Y_{n\frac{f}{e}}) \alpha_h$, where $X_i = \sum_{h=1}^{f/e} Y_{ih} \alpha_h$. The system $\{G_{jh}\}_{\substack{j=1,\ldots,t \\ h=1,\ldots,f/e}}$ is such that $N(\{F_j\}, \mathbb{F}_q) = N(\{G_{jh}\}, \mathbb{F}_{q'})$, where $N(\{G_{jh}\}, \mathbb{F}_{q'})$ is the number of solutions of the system of polynomials $G_{jh} = 0 \ \forall j, h$ over $\mathbb{F}_{q'}$. Furthermore, $\deg(G_{jh}) \leq w_{q'}(F_j)$.*

*Proof.* In Lemma 1 of [MM95], replace the prime field by $\mathbb{F}_{q'}$. □

We now give an example to illustrate how this lemma can be applied to Schauz-Brink's theorem.

**Example 8.** *Let $p \equiv 3 \bmod 4$. Then $x^2 + 1$ is irreducible over $\mathbb{F}_p$ and we have that $1, \alpha$ is a basis for $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, where $\alpha^2 = -1$. Let $A_i = \{a_{i1} + a_{i2}\alpha : a_{ih} \in A_{ih} \subset \mathbb{F}_p$ and $|A_{ih}| \geq 1, h = 1, 2\}$ for $i = 1, \ldots, n$. Consider the following system polynomial equations*

$$\begin{aligned} X_1 + \cdots + X_n &= 0 \\ X_1^{2p+1} + \cdots + X_n^{2p+1} &= 0. \end{aligned} \tag{1}$$

*If $X_i \in A_i$, then $X_i = a_{i1} + a_{i2}\alpha$. We have that*

$$\begin{aligned} X_i^{2p+1} = (a_{i1} + a_{i2}\alpha)^{2p+1} &= (a_{i1} + a_{i2}\alpha)(a_{i1} + a_{i2}\alpha)^{2p} \\ &= (a_{i1} + a_{i2}\alpha)(a_{i1} - a_{i2}\alpha)^{2} \\ &= (a_{i1} + a_{i2}\alpha)(a_{i1}^2 - a_{i2}^2 - 2a_{i1}a_{i2}\alpha) \\ &= a_{i1}^3 + a_{i1}a_{i2}^2 + (-a_{i2}^3 - a_{i1}^2 a_{i2})\alpha. \end{aligned}$$

*Therefore system (1) is equivalent to*

$$\sum_{i=1}^{n} X_i = \sum_{i=1}^{n} a_{i1} + a_{i2}\alpha = 0$$

$$\sum_{i=}^{n} X_i^{2p+1} = \sum_{i=1}^{n} \left[a_{i1}^3 + a_{i1}a_{i2}^2 + (-a_{i2}^3 - a_{i1}^2 a_{i2})\alpha\right] = 0.$$

*Because $1, \alpha$ are a basis and hence linearly independent, the number of solutions of system (1) over $A_1 \times \cdots \times A_n$ is equal to the number of solutions of*

$$\begin{aligned} G_1 &= \sum_{i=1}^{n} a_{i1} = 0 \\ G_2 &= \sum_{i=1}^{n} a_{i2} = 0 \\ G_3 &= \sum_{i=1}^{n} \left(a_{i1}^3 + a_{i1}a_{i2}^2\right) = 0 \\ G_4 &= \sum_{i=1}^{n} \left(-a_{i2}^3 - a_{i1}^2 a_{i2}\right) = 0 \end{aligned} \tag{2}$$

*over $(A_{11} \times A_{12}) \times \cdots \times (A_{n1} \times A_{n2})$. Using Theorem 6, we have that system (2) will have a nontrivial solution if*

$$\sum_i \sum_j (|A_{ij}| - 1) > \sum_{t=1}^{4} \deg(G_t)(p-1) = 8(p-1).$$

*If $|A_{ij}| = 2$, we will need $n \geq 4(p-1)+1$ to guarantee a nontrivial solution. Using Theorem 6 directly on (1), we would need $n > \frac{2(p^2-1)(p+1)}{3}$. In particular if $p = 103$ we need 409 variables to guarantee a nontrivial solution versus the $n = 735489$ given by direct application of Theorem 6.*

## 3. Proof of Theorem 1

*Proof of Theorem 1.* Consider the polynomials $F_1(X_1, \ldots, X_n), \ldots, F_t(X_1, \ldots, X_n)$ over $\mathbb{F}_q$. Choose a basis $\{\alpha_h\}$ for $\mathbb{F}_q$ over $\mathbb{F}_{q'}$. By Lemma 7, a system of $\frac{tf}{e}$ polynomials in $\frac{nf}{e}$ variables defined over the field $\mathbb{F}_{q'}$ with the number of solutions equal to $N(\{F_j\}, \mathbb{F}_q)$ can be constructed using $\{\alpha_h\}$. This system is given by

$$F_j(X_1, \ldots, X_n) = \sum_{h=1}^{f/e} G_{jh}(Y_{11}, Y_{12}, \ldots, Y_{1\frac{f}{e}}, \ldots, Y_{n1}, Y_{n2}, \ldots, Y_{n\frac{f}{e}})\alpha_h,$$

where $X_i = \sum_{h=1}^{f/e} Y_{ih}\alpha_h$.

Let $B_{(i-1)\frac{f}{e}+h} = A_{ih}$ for $h = 1, \dots, \frac{f}{e}$. Since $\sum_{i=1}^{n}\sum_{h=1}^{f/e}(|A_{ih}|-1) > \frac{f(q'-1)}{e}\sum_{j=1}^{t} w_{q'}(F_j)$ we have that

$$\sum_{\ell=1}^{nf/e}(|B_\ell|-1) > \frac{f(q'-1)}{e}\sum_{j=1}^{t} w_{q'}(F_j).$$

By Lemma 7, $\deg(G_{jh}) \le w_{q'}(F_j)$ for $h = 1, \dots, f/e$. Therefore,

$$(q'-1)\sum_{j=1}^{t}\sum_{h=1}^{f/e}\deg(G_{jh}) \le \frac{f(q'-1)}{e}\sum_{j=1}^{t} w_{q'}(F_j),$$

and we obtain

$$\sum_{\ell=1}^{nf/e}(|B_\ell|-1) > (q'-1)\sum_{j=1}^{t}\sum_{h=1}^{f/e}\deg(G_{jh}).$$

Applying Theorem 6 to the system $\{G_{jh}\}_{\substack{j=1,\dots,t\\ h=1,\dots,f/e}}$ we get that the solution set

$$\{\mathbf{b} \in \prod_{\ell=1}^{nf/e} B_\ell \mid G_{jh}(\mathbf{b}) = 0 \ \forall j,h\}$$

with the variables restricted to the $B_\ell$'s is not a singleton and the result follows. □

## 4. Related results

**Example 9.** *Consider the equation $F(X_1,\dots,X_n) = X_1^7 + \cdots + X_n^7 + G(X_1,\dots,X_n)$ over $\mathbb{F}_{2^7}$, where $w_2(G) < 3$ and $G(0,\dots,0) = 0$. Suppose that $A_i = \{\sum_{h=1}^{7} a_{ih}\alpha_h \mid a_{ih} \in A_{ih} \subseteq \{0,1\}\}$, where $|A_{ih}| \ge 1$ and $|A_i| = |A_{i1}||A_{i2}|\cdots|A_{i7}| = 2^4$ for $i = 1,\dots,n$. Suppose $(0,\dots,0) \in \prod A_i$. We have $\sum_{i=1}^{n}\sum_{h=1}^{7}(|A_{ih}|-1) = \sum_{i=1}^{n} 4 = 4n$. Now for $n \ge 6$ we have $4n > 7\cdot 3 = 21$. Hence $F$ has a nontrivial solution for $n \ge 6$. Using Theorem 6 directly, we would need $n \ge 60$ to guarantee a nontrivial solution.*

We now give a corollary for the case when $A_{ih} = \{0,1\}$.

**Corollary 10.** *Consider the polynomial $F(X_1,\dots,X_n)$ over $\mathbb{F}_{p^f}$. Suppose that*

$$A_i = \{\sum_{h=1}^{f} a_{ih}\alpha_h \mid a_{ih} \in A_{ih} = \{0,1\}\},$$

*for $i = 1,\dots,n$ and that $\{\alpha_h\}$ is a basis of $\mathbb{F}_{p^f}$ over $\mathbb{F}_p$. Then the solution set $V = \{\mathbf{a} \in \prod_{i=1}^{n} A_i \mid F(\mathbf{a}) = 0\}$ with variables restricted to the $A_i$'s is not a singleton whenever $n > (p-1)w_p(F)$.*

*Proof.* Consider the polynomial $F(X_1,\dots,X_n)$ over $\mathbb{F}_{p^f}$. We have that $A_i = \{\sum_{h=1}^{f} a_{ih}\alpha_h \mid a_{ih} \in A_{ih} = \{0,1\}\}$, for $i = 1,\dots,n$. Applying Theorem 1 we require $\sum_{i=1}^{n}\sum_{h=1}^{f}(|A_{ih}|-1) = \sum_{i=1}^{n} f = nf > f(p-1)w_p(F)$. Hence $V$ is not a singleton for $n > (p-1)w_p(F)$. □

**Corollary 11.** *Let $q = p^f$ and $q' = p^e$ with $e \mid f$. Let $A_i$ be a nonempty subset of $\mathbb{F}_{q'}$ for $i = 1 \ldots, n$ and $F_1(X_1, \ldots, X_n), \ldots, F_t(X_1, \ldots, X_n)$ be polynomials over $\mathbb{F}_q$. Then $V = \{\mathbf{a} \in \prod_{i=1}^n A_i \mid F_j(\mathbf{a}) = 0\ \forall j\}$ is not a singleton whenever*

$$\sum_{i=1}^n (|A_i| - 1) > \frac{f(q'-1)}{e} \sum_{j=1}^t w_{q'}(F_j).$$

*Proof.* In Theorem 1 take $A_{ih} = \{0\}$ for $h > 1$ and choose $\alpha_1 = 1$. Then $A_{i1} = A_i$. Since $|A_{ih}| - 1 = 0$ for $h > 1$, the result follows. □

## 5. Acknowledgements

We thank the anonymous referees for very useful suggestions and corrections. The second author was partially supported by a GAANN fellowship (#P200A150319, Department of Education) and by the Alfred P. Sloan Foundation's MPHD Program, awarded in 2017.

## References

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

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

[Bri11] David Brink. Chevalley's theorem with restricted variables. *Combinatorica*, 31(1):127–130, 2011.

[CCV12] F. Castro and F. N. Castro-Velez. Improvement to Moreno-Moreno's theorems. *Finite Fields Appl.*, 18(6):1207–1216, 2012.

[Che35] C. Chevalley. Démonstration d'une hypothèse de M. Artin. *Abh. Math. Sem. Univ. Hamburg*, 11(1):73–75, 1935.

[Kat71] Nicholas M. Katz. On a theorem of Ax. *Amer. J. Math.*, 93:485–499, 1971.

[MM95] O. Moreno and C. J. Moreno. Improvements of the Chevalley-Warning and the Ax-Katz theorems. *Amer. J. Math.*, 117(1):241–244, 1995.

[MSCK04] Oscar Moreno, Kenneth W. Shum, Francis N. Castro, and P. Vijay Kumar. Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications. *Proc. London Math. Soc. (3)*, 88(3):545–564, 2004.

[Sch08] Uwe Schauz. Algebraically solvable problems: describing polynomials as equivalent to explicit solutions. *Electron. J. Combin.*, 15(1):Research Paper 10, 35, 2008.

[War35] Ewald Warning. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. *Abh. Math. Sem. Univ. Hamburg*, 11(1):76–83, 1935.

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
*E-mail address*: franciscastr@gmail.com

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61801
*E-mail address*: oscareg2@illinois.edu

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
*E-mail address*: luis.medina17@upr.edu