A SIMULTANEOUS GENERALIZATION OF THE THEOREMS OF CHEVALLEY-WARNING AND MORLAYE

PETE L. CLARK

Abstract. Inspired by recent work of I. Baoulina, we give a simultaneous generalization of the theorems of Chevalley-Warning and Morlaye.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of order $q = p^f$.

Our point of departure is this recent result, established using a Coefficient Formula of Schauz [Sc08a].

Theorem 1.1. *(Restricted Variable Chevalley-Warning* [Cl14]*)*
Let $P_1, \ldots, P_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be polynomials. For $1 \leq i \leq n$, let $\varnothing \neq X_i \subseteq \mathbb{F}_q$, and let $\varphi_i(t) = \prod_{x_i \in X_i}(t - x_i) \in \mathbb{F}_q[t]$. Put $X \coloneqq \prod_{i=1}^n X_i$. We suppose:

$$(q-1)\sum_{j=1}^r \deg(P_j) < \sum_{i=1}^n (\#X_i - 1)\,. \tag{1}$$

Put $V_X = \{x \in X \mid P_1(x) = \ldots = P_r(x) = 0\}$. Then we have:

$$\sum_{x \in V_X} \frac{1}{\prod_{i=1}^n \varphi_i'(x_i)} = 0 \in \mathbb{F}_q. \tag{2}$$

Remark 1.2. *a) It follows from (2) that $\#V_X \neq 1$. This is the Restricted Variable Chevalley Theorem of Schauz* [Sc08a] *and Brink* [Br11].
b) Take $X_i = \mathbb{F}_q$ for all i, and suppose (1) holds, i.e., $\sum_{j=1}^r \deg(P_j) < n$. Then for all i we have $\varphi_i(t) = t^q - t$ and $\varphi_i'(t) = -1$, so $\sum_{x \in V_x}(-1)^n = 0 \in \mathbb{F}_q$. Thus $p \mid \#\{x \in \mathbb{F}_q^n \mid P_1(x) = \ldots = P_r(x) = 0\}$: Chevalley-Warning [Ch35], [Wa35].

In this note we will use Theorem 1.1 to deduce the following result.

Theorem 1.3. *For $1 \leq i \leq n$, let $m_i \in \mathbb{Z}^+$ and put $d_i = \gcd(m_i, q-1)$. Let $P_1, \ldots, P_r \in \mathbb{F}_q[t_1, \ldots, t_n]$. We suppose:*

$$\sum_{j=1}^r \deg(P_j) < \sum_{i=1}^n \frac{1}{d_i}. \tag{3}$$

Then $p \mid \#\{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid P_1(x_1^{m_1}, \ldots, x_n^{m_n}) = \ldots = P_r(x_1^{m_1}, \ldots, x_n^{m_n}) = 0\}$.

The proof of Theorem 1.3 inspired by work of Baoulina [Ba17], which restricts variables to the *value sets* $f_1(\mathbb{F}_q), \ldots, f_n(\mathbb{F}_q)$ of polynomials $f_1, \ldots, f_n \in \mathbb{F}_q[t]$.

Taking $m_i = 1$ for all i in Theorem 1.3 recovers Chevalley-Warning. Taking $r = 1$ and P_1 linear recovers the following result.

Theorem 1.4. *(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 $a_1, \ldots, a_n, b \in \mathbb{F}_q$. Suppose that*

$$\sum_{i=1}^n \frac{1}{d_i} > 1. \tag{4}$$

Then $p \mid \mathbf{z} := \#\{x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid a_1 x_1^{m_1} + \ldots + a_n x_n^{m_n} = b\}$.

Remark 1.5. *It is easy to see that*

$$\#\{x \in \mathbb{F}_q^n \mid a_1 x_1^{m_1} + \ldots + a_n x_n^{m_n} = b\} = \#\{x \in \mathbb{F}_q^n \mid a_1 x_1^{d_1} + \ldots + a_n x_n^{d_n} = b\}.$$

So in Theorem 1.4 we may assume that $m_i = d_i$ for all i. If moreover $d_1 = \ldots = d_n$, then (4) simplifies to $n > \deg(a_1 t_1^{d_1} + \ldots + a_n t_n^{d_n} - b)$, a case of Chevalley-Warning. This does not apply to the general case: consider e.g. $t_1^2 + t_2^3 + t_3^5 = -1$.

Acknowledgments: Thanks to I. Baoulina, A. Bishnoi, G. Ottinger, P. Pollack and J.R. Schmitt for helpful conversations.

2. Proof of the Main Theorem

We begin with the following special case of Theorem 1.1.

Proposition 2.1. *Let $f_1, \ldots, f_n \in \mathbb{F}_q[t]$ and $P_1, \ldots, P_r \in \mathbb{F}_q[t_1, \ldots, t_n]$. For $1 \leq i \leq n$, put $X_i = f_i(\mathbb{F}_q)$ and $V_X = \{x \in X \mid P_1(x) = \ldots = P_r(x) = 0\}$. We suppose*

$$(q-1)\sum_{j=1}^r \deg(P_j) < \sum_{i=1}^n (\#X_i - 1). \tag{5}$$

a) We have $\sum_{x \in V_X} \frac{1}{\prod_{i=1}^n \varphi_i'(x)} = 0 \in \mathbb{F}_q$.
b) If there is $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ such that

$$P_1(f_1(x_1), \ldots, f_n(x_n)) = \ldots = P_r(f_1(x_1), \ldots, f_n(x_n)) = 0,$$

there is $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ with $(f_1(x_1), \ldots, f_n(x_n)) \neq (f_1(y_1), \ldots, f_n(y_n))$ and $P_1(f_1(y_1), \ldots, f_n(y_n)) = \ldots = P_r(f_1(y_1), \ldots, f_n(y_n)) = 0$.

Remark 2.2. *a) Proposition 2.1b) is a recent result of Baoulina* [Ba17, Cor. 2].
b) Baoulina remarks that for $f \in \mathbb{F}_q[t]$ of positive degree, we have

$$\#f(\mathbb{F}_q) \geq \left\lfloor \frac{q-1}{\deg f} \right\rfloor + 1$$

and thus (when $\deg(f_i) \geq 1$ for all i) the following condition implies (5):

$$(q-1)\sum_{j=1}^r \deg(P_j) < \sum_{i=1}^n \left\lfloor \frac{q-1}{\deg(f_i)} \right\rfloor.$$

Now for $1 \leq i \leq n$, let $m_i \in \mathbb{Z}^+$, put

$$d_i := \gcd(q-1, m_i), \quad f_i(t) := t^{m_i}, \quad X_i := f_i(\mathbb{F}_q).$$

Then $X_i = \{x^{m_i} \mid x \in \mathbb{F}_q\} = \{x^{d_i} \mid x \in \mathbb{F}_q\}$, so $\#X_i = \frac{q-1}{d_i} + 1$.

Lemma 2.3. *Let $d \mid q-1$, let $X = \{x^d \mid x \in \mathbb{F}_q\}$ be the set of dth powers in $\mathbb{F}_q$, and let $\varphi(t) = \prod_{x \in X}(t-x)$. Then:*
a) We have $\varphi'(0) = -1$.
b) For all $x \in X \setminus \{0\}$, we have $\varphi'(x) = \frac{-1}{d}$.

Proof. Since $\varphi(t) = \prod_{x\in X}(t-x)$, we have

$$\varphi'(t) = \sum_{x\in X}\prod_{y\in X\setminus\{x\}}(t-y).$$

a) Thus $\varphi'(0) = \prod_{x\in X\setminus\{0\}}(-x) = (-1)^{\frac{q-1}{d}}\prod_{x\in X\setminus\{0\}}x$. Since $\prod_{x\in X\setminus\{0\}}x$ is the product over all elements of a cyclic group of order $\frac{q-1}{d}$, it is -1 if $\frac{q-1}{d}$ is even and 1 if $\frac{q-1}{d}$ is odd. The result follows.
b) Let $x\in X\setminus\{0\}$. Let ζ be a primitive $\frac{q-1}{d}$th root of unity in $\mathbb{F}_q$, so ζ generates the subgroup $X\setminus\{0\}$ and in particular $x=\zeta^a$ for some $1\le a\le\frac{q-1}{d}$. Then

$$\varphi'(x) = \prod_{y\in X\setminus\{x\}}(x-y) = \zeta^a\prod_b(\zeta^a-\zeta^b),$$

where b runs from 1 to $\frac{q-1}{d}$ with a omitted. Thus

$$\varphi'(x) = (\zeta^a)^{\frac{q-1}{d}}\prod_b(1-\zeta^{b-a}) = \prod_{c=1}^{\frac{q-1}{d}-1}(1-\zeta^c).$$

But

$$\prod_{c=1}^{\frac{q-1}{d}-1}(X-\zeta^c) = \frac{X^{(q-1)/d}-1}{X-1} = 1+X+\ldots+X^{(q-1)/d-1},$$

and evaluating at $X=1$ gives $\varphi'(x) = \frac{q-1}{d} = \frac{-1}{d}\in\mathbb{F}_q$. □

Now we give the proof of Theorem 1.3. Put

$$S \coloneqq \{(x_1,\ldots,x_n)\in\mathbb{F}_q^n \mid P_1(x_1^{m_1},\ldots,x_n^{m_n}) = \ldots = P_r(x_1^{m_1},\ldots,x_n^{m_n}) = 0\}.$$

For $1\le i\le n$ and $x_i\in X_i = \{x^{d_i}\mid x\in\mathbb{F}_q\}$, put

$$e_i(x_i) = \begin{cases} 1 & x_i = 0 \\ d_i & x_i\neq 0 \end{cases},$$

and for $x=(x_1,\ldots,x_n)\in X=\prod_{i=1}^n X_i$, put

$$e(x) = \prod_{i=1}^n e_i(x_i).$$

For each $x_i\in X_i$, there are $e_i(x_i)$ elements y of $\mathbb{F}_q$ such that $y^{m_i}=x_i$ and thus each $(x_1,\ldots,x_n)\in V_X$ corresponds to $e(x)$ elements $(y_1,\ldots,y_n)\in S$ such that $(y_1^{m_1},\ldots,y_n^{m_n}) = (x_1,\ldots,x_n)$. Applying Proposition 2.1a) and Lemma 2.3, we get

$$0 = \sum_{x\in V_X}\frac{1}{\prod_{i=1}^n\varphi_i'(x_i)} = \sum_{y\in S}\frac{1}{e(y_1^{m_1},\ldots,y_n^{m_n})}\frac{1}{\prod_{i=1}^n\varphi_i'(y_i^{m_i})}$$

$$= \sum_{y\in S}\frac{1}{\prod_{i=1}^n e_i(y_i^{m_i})\varphi_i'(y_i^{m_i})} = \sum_{y\in S}(-1)^n.$$

It follows that $p\mid \#S$, completing the proof of Theorem 1.3.

3. Final Remarks

In the setting of Chevalley-Warning, Warning [Wa35] also proved: if $V_{\mathbb{F}_q^n} \neq \varnothing$ then

$$\#V_{\mathbb{F}_q^n} \geq q^{n-\sum_{j=1}^r \deg(P_j)}.$$

These two results raise the following questions:

(Q1) Do we always have $q \mid \#V_{\mathbb{F}_q^n}$?
(Q2) For fixed $\deg(P_1), \ldots, \deg(P_r)$, what is the largest power of p that always divides $\#V_{\mathbb{F}_q^n}$?

Ax [Ax64] answered (Q1) (affirmatively) and answered (Q2) when $r = 1$. Katz answered (Q2) in the general case.

In the setting of Theorem 1.4 – i.e., one diagonal equation – higher p-adic divisibilities were shown by Joly [Jo71] in certain cases. (Joly also showed Theorem 1.4 in certain cases, including when $q = p$.) Joly conjectured that (Q1) has an affirmative answer here as well, i.e., that $q \mid \mathbf{z}$ in all cases. This was proved by Wan [Wa88], and his result also addresses (Q2).

Theorem 3.1. *(Wan) In Theorem 1.4, if $\sum_{i=1}^n \frac{1}{d_i} > b \geq 1$, then $q^b \mid \mathbf{z}$.*

We ask (Q1) and (Q2) in the setting of Theorem 1.3. To answer them it would be useful to have a "Restricted Variable Ax-Katz Theorem." I find the idea of this intriguing, but to be sure, I do not even have a conjectural statement.

References

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

[Ba17] I. Baoulina, *On a theorem of Morlaye and Joly and its generalization*. `https://arxiv.org/pdf/1707.00353.pdf`.

[Br11] D. Brink, *Chevalley's theorem with restricted variables*. Combinatorica 31 (2011), 127–130.

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

[Cl14] P.L. Clark, *The Combinatorial Nullstellensätze Revisited*. Electronic Journal of Combinatorics. Volume 21, Issue 4 (2014). Paper #P4.15

[Jo71] J.-R. Joly, *Nombre de solutions de certaines équations diagonales sur un corps fini*. C. R. Acad. Sci. Paris Sér. A-B 272 (1971), A1549-A1552.

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

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

[Sc08a] U. Schauz, *Algebraically solvable problems: describing polynomials as equivalent to explicit solutions*. Electron. J. Combin. 15 (2008), no. 1, Research Paper 10, 35 pp.

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

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