DE GRUYTER OPEN

uniform distribution theory

DOI: 10.1515/udt-2017–0003
Unif. Distrib. Theory **12** (2017), no.1, 37–53

p-ADIC VALUATION OF EXPONENTIAL SUMS IN ONE VARIABLE ASSOCIATED TO BINOMIALS

Francis N. Castro — Raúl Figueroa — Puhua Guan

ABSTRACT. In this paper we compute the p-adic valuation of exponential sums associated to binomials $F(X) = aX^{d_1} + bX^{d_2}$ over $\mathbb{F}_p$. In particular, its p-adic valuation is constant for $a, b \in \mathbb{F}_p^*$. As a byproduct of our results, we obtain a lower bound for the sizes of value sets of binomials over $\mathbb{F}_q$.

Communicated by Arne Winterhof

1. Introduction

Exponential sums have been applied in many areas of mathematics and their p-adic valuation is used as a tool to characterize important properties of objects in applied mathematics. Many authors have studied the p-adic valuation of the roots of the L-function associated to the exponential sum. This information is encoded in the Newton polygon of the L-function ([1, 2, 5, 6, 18, 21, 23, 24]). As the value of an exponential sum is equal to the sum of the roots of the associated L-function, any estimate on the roots implies an estimate for the p-adic valuation of the exponential sum. In this paper we study the p-adic valuation of exponential sums associated to polynomials over $\mathbb{F}_p$ when p is odd, i.e., the p-adic valuation of the sum of the roots of the L-function associated to the exponential sum.

In general, there are good estimates for the p-adic valuation of exponential sums ([1, 9, 14, 15, 19]). We are interested in computing the p-adic valuation of exponential sums associated to polynomials in one variable over the prime field $\mathbb{F}_p$. This is a difficult problem in general, therefore, in this paper, we study the p-adic valuation of exponential sums associated to binomials. The p-adic valuation of exponential sums associated to monomials is well known; the next simplest case is exponential sums associated to binomials.

2010 Mathematics Subject Classification: 11T23; 11T06.
Keywords: p-divisibility, exponential sums, value sets.

In this paper we compute the p-adic valuation of families of exponential sums associated to binomials. In particular, the p-adic valuation is computed for exponential sums associated to $F(X) = aX^{d_1} + bX^{d_2}$, when $a, b \in \mathbb{F}_p^*$, and $\max\{d_1, d_2\} \leq \sqrt{p-1}$. In the case when $(d_1 - d_2)$ divides $(p-1)$, we completely characterize the p-adic valuation of exponential sums associated to binomials.

Let $u_p(F)$ be the smallest positive integer k such that $\sum_{x\in\mathbb{F}_q} F(x)^k \neq 0$ in $\mathbb{F}_q (q = p^f)$. If $u_p(F)$ does not exist, define $u_p(F) = \infty$. In [20], W a n, S h i u e, C h e n established the following lower bound for the size of the value set V_F of a polynomial F over a finite field $\mathbb{F}_q$: if $u_p(F) < \infty$, then $|V_F| \geq u_p(F) + 1$. $u_p(F)$ is always finite for the prime field $\mathbb{F}_p$ (see Remark 2.3 in [20]). Recently, M u l l e n, W a n, W a n g generalized this result to polynomials in several variables ([17]). We compute $u_p(aX^{d_1} + bX^{d_2})$ for d_1 and d_2 satisfying some natural conditions. In particular, $u_p(aX^{d_1} + bX^{d_2})$ is computed explicitly when $\max\{d_1, d_2\} \leq \sqrt{p-1}$.

2. Preliminaries

Given j, j_i integers such that $0 \leq j_i < p$ and $j = \sum_{i=0}^{r} j_i p^i$, we define the p-weight of j by $\sigma_p(j) = \sum_{i=0}^{r} j_i$, and $\rho_p(j) = \prod_{i=0}^{r} j_i!$. From now on, we assume that a polynomial $F(X) = \sum_{i=1}^{N} a_i X^{d_i}$ is a nonconstant polynomial of degree less than p. In this paper we consider p to be odd.

Let $\mathbb{Q}_p$ be the p-adic field with ring of integers $\mathbb{Z}_p$. Let $\mathcal{T}$ denote the Teichmüller representatives of $\mathbb{F}_p$ in $\mathbb{Q}_p$. Denote by ξ a primitive p-th root of unity in $\overline{\mathbb{Q}}_p$. Define $\theta = 1 - \xi$ and denote by ν_θ the valuation over θ. Note that $\nu_\theta(p) = p - 1$ and $\nu_p(x) = \frac{\nu_\theta(x)}{p-1}$.

Let $\phi : \mathbb{F}_p \to \mathbb{Q}(\xi)$ be a nontrivial additive character. The exponential sum associated to $F(X) = \sum_{i=1}^{N} a_i X^{d_i}$ is defined as follows

$$S_p(F) = \sum_{x\in\mathbb{F}_p} \phi\big(F(x)\big).$$

Frequently, we denote $S_p(aX^{d_1} + bX^{d_2})$ by $S_p(d_1, d_2)$, where $ab \neq 0$.

Note that if the p-adic valuation of the exponential sum $\sum_{x\in\mathbb{F}_p} \phi(F(x))$ is a real number, then $S_p(F)$ will not be divisible by an arbitrary power of p and therefore $S_p(F) \neq 0$. The next theorem gives a bound for the θ-adic valuation of an exponential sum with respect to θ.

Theorem 2.1 ([15]). *Let $F(X) = \sum_{i=1}^{N} a_i X^{d_i}$, $a_i \neq 0$. If $S_p(F)$ is the exponential sum*

$$S_p(F) = \sum_{x \in \mathbb{F}_p} \phi\big(F(x)\big), \tag{1}$$

then $\nu_\theta\big(S_p(F)\big) \geq \mu_p(d_1, \ldots, d_N)$, where

$$\mu_p(d_1, \ldots, d_N) = \min_{(j_1, \ldots, j_N)} \left(\left\{ \sum_{i=1}^{N} j_i \mid 0 \leq j_i < p \right\} + \epsilon(p-1) \right),$$

for $(j_1, \ldots, j_N)$ a solution to the modular equation

$$d_1 j_1 + d_2 j_2 + \cdots + d_N j_N \equiv 0 \bmod p - 1 \tag{2}$$

and

$$\epsilon = \begin{cases} 1 & \text{if } (j_1, \ldots, j_N) = (0, \ldots, 0), \\ 0, & \text{otherwise.} \end{cases}$$

Following the notation in [15], we expand the exponential sum $S_p(F)$:

$$S_p(F) = \sum_{j_1=0}^{p-1} \cdots \sum_{j_N=0}^{p-1} \left[\prod_{i=1}^{N} c(j_i) \right] \left[\sum_{t \in \mathcal{T}} t^{d_1 j_1 + \cdots + d_N j_N} \right] \left[\prod_{i=1}^{N} a_i'^{j_i} \right], \tag{3}$$

where a_i''s are the Teichmüller representatives of the coefficients a_i of F, and $c(j_i)$ is defined in Lemma 2.3 below. Each solution $(j_1, \cdots, j_N)$ of (2) is associated to a term T in the above sum with

$$\begin{aligned} \nu_\theta(T_{j_1, \ldots, j_N}) &= \nu_\theta \left(\left[\prod_{i=1}^{N} c(j_i) \right] \left[\sum_{t \in \mathcal{T}} t^{d_1 j_1 + \cdots + d_N j_N} \right] \left[\prod_{i=1}^{N} a_i'^{j_i} \right] \right) \\ &= \nu_\theta \left(\left[\prod_{i=1}^{N} c(j_i) \right] \right) + \nu_\theta \left(\left[\sum_{t \in \mathcal{T}} t^{d_1 j_1 + \cdots + d_N j_N} \right] \right) + \nu_\theta \left(\left[\prod_{i=1}^{N} a_i'^{j_i} \right] \right) \\ &= \sum_{i=1}^{N} \sigma_p(j_i) + 0 + 0 = \sum_{i=1}^{N} j_i, \end{aligned} \tag{4}$$

for $(j_1, \ldots, j_N) \neq (0, \ldots, 0)$(see Lemma 2.4).

Sometimes there is not equality in the bound of Theorem 2.1 on the p-adic valuation of $S_p(F)$ because it could happen that there is more than one solution $(j_1, \ldots, j_N)$ providing the minimum value for $\sum_{i=1}^{N} j_i$, for example, when the associated terms are similar some of them could add to produce higher powers of θ dividing the exponential sum. In [7, 8, 10], we computed the p-adic valuation of some exponential sums over finite fields for special polynomials. Our results of this paper generalize and improve the results of [8].

Remark 2.2. In the case that there is a unique $(\mathbf{j}_1, \ldots, \mathbf{j}_N)$ such that $\mu_p(d_1, \ldots, d_N) = \mathbf{j}_1 + \cdots + \mathbf{j}_N$, then

$$\nu_\theta\big(S(F)\big) = \nu_\theta\left(\sum_{\substack{(j_1,\ldots,j_N)\\ d_1j_1+\cdots+d_Nj_N\equiv 0 \bmod p-1}} T_{j_1,\ldots,j_N}\right) = \nu_\theta(T_{\mathbf{j}_1,\ldots,\mathbf{j}_N}))$$

since

$$\nu_\theta(T_{j_1,\ldots,j_N}) > \nu_\theta(T_{\mathbf{j}_1,\ldots,\mathbf{j}_N})$$

for any $(j_1, \ldots, j_N) \neq (\mathbf{j}_1, \ldots, \mathbf{j}_N)$ and $(j_1, \ldots, j_N)$ satisfies (2).

From now on, we call any solution $(j_1, \cdots, j_N)$ of (2) that has $\nu_\theta(T) = \mu_p(d_1, \ldots, d_N)$ of minimum value a *minimal solution*. We need to use the following lemma together with Stickelberger's Theorem([3]) to compute the p-adic valuation.

Lemma 2.3. *There is a unique polynomial* $C(X) = \sum_{j=0}^{p-1} c(j)X^j \in \mathbb{Q}_p(\xi)[X]$ *of degree* $p-1$ *such that*

$$C(t) = \xi^t \qquad \text{for all } t \in \mathcal{T}.$$

Moreover, the coefficients of $C(X)$ *satisfy*

$$\begin{aligned} c(0) &= 1 \\ (p-1)c(p-1) &= -p \\ (p-1)c(j) &= g(j) \qquad \text{for } 0 < j < p-1, \end{aligned} \tag{5}$$

where $g(j)$ *is the Gauss sum,*

$$g(j) = \sum_{t\in\mathcal{T}^*} t^{-j}\xi^t.$$

Theorem 2.4 (Stickelberger [16])**.** *For* $0 \leq j < p-1$,

$$\frac{g(j)\rho_p(j)}{\theta^{\sigma_p(j)}} \equiv -1 \bmod \theta. \tag{6}$$

Now we state some theorems about polynomials that are going to be used in the following sections.

Theorem 2.5 ([12])**.** *The polynomial* $F(X)$ *in one variable over* $\mathbb{F}_q (q = p^f)$ *is a permutation polynomial of* $\mathbb{F}_q$ *if and only if* $S_q(F) = \sum_{x\in\mathbb{F}_q} \phi\big(F(x)\big) = 0$ *for all nontrivial additive characters* ϕ *of* $\mathbb{F}_q$.

Remark 2.6. Theorem 2.5 implies that if $S_q(F) \neq 0$ for at least one nontrivial additive character, then F is not a permutation polynomial of $\mathbb{F}_q$. Using the result of Conway-Jones in [11], we obtain that if $S_p(F) = 0$ for a nontrivial

additive character ϕ of $\mathbb{F}_p$, then F is a permutation of $\mathbb{F}_p$. Note this is only true for the ground field. For example,

$$\sum_{x\in\mathbb{F}_{32}} (-1)^{Tr(x^7+(\alpha+1)x)} = 0, \quad \text{and} \quad |V_F| = 21, \quad \text{where } \alpha^5+\alpha^2+1=0.$$

We extend the definition of $\mu_p(d_1,d_2)$ for field extensions of $\mathbb{F}_p$. Let

$$\mu_q(d_1,d_2) = \min_{\substack{0\le j_1,j_2\le q-1\\ j_1+j_2\neq 0}} \{j_1+j_2 \,|\, d_1j_1+d_2j_2 \equiv 0 \bmod q-1,\ q=p^f\}. \tag{7}$$

The conclusion of Theorem 2.1 is false for $q=p^f>p$ (see [15] for the correct version of the theorem).

Now we state a relation between $u_p(F)$ and $\mu_q(d_1,d_2)$.

Lemma 2.7. *With the above notation $u_p(F)\ge\mu_q(d_1,d_2)$. In the case that equation* (2) *has a unique minimal solution, we have $u_p(F)=\mu_p(d_1,d_2)$.*

Proof. If $u_p(F)$ does not exist, then $u_p(F)\ge\mu_q(d_1,d_2)$. We assume that $u_p(F)<\infty$. We are going to prove the lemma for binomials but the proof is similar for general polynomials. The terms of $(ax^{d_1}+bx^{d_2})^m$ are of the form $\binom{m}{j_1,j_2}a^{j_1}b^{j_2}x^{d_1j_1+d_2j_2}$ with $j_1+j_2=m$. We have that

$$\sum_{x\in\mathbb{F}_q}\binom{m}{j_1,j_2}a^{j_1}b^{j_2}x^{d_1j_1+d_2j_1}=0 \quad \text{if } d_1j_1+d_2j_1\not\equiv 0 \bmod q-1.$$

In the case $d_1j_1+d_2j_1\equiv 0 \bmod q-1$, we have that $\sum_{x\in\mathbb{F}_q} a^{j_1}b^{j_2}x^{d_1j_1+d_2j_1}\neq 0$. Hence $u_p(F)$ has to be greater or equal than $\mu_q(d_1,d_2)$ since $\mu_q(d_1,d_2)$ is the smallest positive integer such that $(ax^{d_1}+bx^{d_2})^{\mu_q(d_1,d_2)}$ contains terms of x with exponent congruent to $0 \bmod q-1$. Now we consider the case when $q=p$ and equation (2) has a unique minimal solution. When we expand $(ax^{d_1}+bx^{d_2})^{\mu_p(d_1,d_2)}$ many terms of x with exponents congruent to $0 \bmod p-1$ could appear and its sum could be equal to zero. In the case that equation (2) has a unique minimal solution, we only have one term congruent to $0 \bmod p-1$. Hence, $\sum_{x\in\mathbb{F}_p}(ax^{d_1}+bx^{d_2})^{\mu_p(d_1,d_2)}\neq 0$. Therefore, $u_p(F)=\mu_p(d_1,d_2)$. □

Remark 2.8. The condition of a unique minimal solution of (7) does not guarantee $u_p(F)=\mu_q(d_1,d_2)$ since the coefficient of x^{q-1} in the expansion of $(ax^{d_1}+bx^{d_2})^{\mu_q(d_1,d_2)}$ could be zero. This can happen when $q=p^f>p$. For example, we have that the modular equation $11j_1+3j_2\equiv 0 \bmod 127$ has a unique minimal solution $(11,2)$. Hence $\mu_{127}(11,2)=13$. We have that $\sum_{x\in\mathbb{F}_{128}}(x^{11}+x^3)^{13}=\sum_{x\in\mathbb{F}_{128}}(x^{111}+x^{103}+x^{79}+x^{71}+x^{47}+x^{39}+x^{16}+x^8)=0$ in $\mathbb{F}_{128}$ since the coefficient of the monomial x^{127} is equal to $\binom{13}{11}=0$ in $\mathbb{F}_{128}$. Actually the value of $u_p(F)=29$.

3. p-adic Valuation of $S_p(d_1, d_2)$

In this section we compute the p-adic valuation of $S_p(d_1, d_2)$ under some natural conditions. In particular, we compute the divisibility of $S_p(d_1, d_2)$ for $\max\{d_1, d_2\} \leq \sqrt{p-1}$. Also, we obtain a lower bound for the value sets of binomials over finite fields.

Now we state an elementary lemma that is going to be used in the following lemma.

Lemma 3.1. *Let $d_1 > d_2$ be positive integers, and $p - 1 \equiv s_1 \bmod d_1$, where s_1 is the smallest non-negative integer satisfying the modular equation. Then $ld_1 \equiv -s_1 \bmod d_2$ is solvable if and only if $\gcd(d_1, d_2)$ divides $p - 1$.*

Proof. We have that $ld_1 \equiv -s_1 \bmod d_2$ is solvable if and only if $\gcd(d_1, d_2)$ divides $-s_1$. But we have $gcd(d_1, d_2)$ divides $-s_1$ if and only if $\gcd(d_1, d_2)$ divides $p - 1$. □

The next elementary lemma computes $\mu_p(d_1, d_2)$ for the modular equation $d_1 i + d_2 j \bmod p - 1$. We did not find a proof of the following lemma, hence we state the lemma and include its proof. The proof of the main theorem of this paper relies on the following elementary result.

Lemma 3.2. *Let $d_1 > d_2$ be positive integers, $\gcd(d_1, d_2)$ divides $p - 1$ and $p - 1 \equiv s_1 \bmod d_1$, where s_1 is the smallest non-negative integer satisfying the modular equation. Let l_1 be a non-negative integer satisfying*

$$l_1 = \min\{l \mid ld_1 \equiv -s_1 \bmod d_2\}. \tag{8}$$

If l_1 satisfies

$$l_1 \leq \left\lfloor \frac{p-1}{d_1} \right\rfloor \quad \text{and} \quad d_1 - d_2 \leq \frac{p-1}{d_1}, \tag{9}$$

then the modular equation

$$d_1 i + d_2 j \equiv 0 \bmod p - 1 \tag{10}$$

has a unique minimal solution given by $(i_1, j_1) = (\lfloor \frac{p-1}{d_1} \rfloor - l_1, \frac{s_1 + l_1 d_1}{d_2})$. Furthermore, $\mu_p(d_1, d_2) = \min\{i + j \mid d_1 i + d_2 j \equiv 0 \bmod p - 1, (i, j) \neq (0, 0)\} = i_1 + j_1$, where

$$i_1 = \left\lfloor \frac{p-1}{d_1} \right\rfloor - l_1 \quad \text{and} \quad j_1 = \frac{s_1 + l_1 d_1}{d_2}. \tag{11}$$

P r o o f. The assumption that $\gcd(d_1, d_2)$ divides $p-1$ and Lemma 3.1 guarantee that l_1 exists, so

$$\begin{aligned} l_1 &= \min\{l \,:\, ld_1 + s_1 \equiv 0 \bmod d_2\} \\ &= \min\left\{l \,:\, ld_1 + \left(p - 1 - \Big\lfloor \frac{p-1}{d_1} \Big\rfloor d_1\right) \equiv 0 \bmod d_2\right\} \\ &= \min\left\{l \,:\, p - 1 + d_1\left(\Big\lfloor \frac{p-1}{d_1} \Big\rfloor - l\right) \equiv 0 \bmod d_2\right\}, \end{aligned}$$

where the minimizations are over nonnegative integers. We can set

$$i_1 = \Big\lfloor \tfrac{p-1}{d_1} \Big\rfloor - l_1,\ j_1 = \tfrac{p-1-i_1 d_1}{d_2} = \tfrac{p-1-d_1\lfloor (p-1)/d_1 \rfloor + d_1 l_1}{d_2} = \tfrac{s_1 + d_1 l_1}{d_2},$$

so as to have $d_1 i_1 + d_2 j_1 = p - 1$. We note that $l_1 < d_2$ since it is the least nonnegative integer satisfying a congruence modulo d_2, and $s_1 < d_1$ for similar reason. Thus

$$j_1 < d_1(l_1 + 1)/d_2 \quad \text{and so} \quad j_1 < d_1. \tag{12}$$

We shall show that $(x, y) = (i_1, j_1)$ is the unique minimizer of $x + y$ among pairs of nonnegative integers satisfying the congruence $d_1 x + d_2 y \equiv 0 \bmod p - 1$. So suppose we have a nonnegative pair (i, j) with $d_1 i + d_2 j = T(p-1)$ for some integer $T \geq 1$ and suppose that $i + j \leq i_1 + j_1$. We shall show that in fact $(i, j) = (i_1, j_1)$.

We note that $d_1(Ti_1) + d_2(Tj_1) = T(p-1)$, and any other i, j with $d_1 i + d_2 j = T(p-1)$ must be of the form $i = Ti_1 + (ud_2/g)$ and $j = Tj_1 - (ud_1/g)$, for some integer u, where $g = \gcd(d_1, d_2)$. So we write our pair (i, j) in this way. Then

$$0 \leq i_1 + j_1 - (i + j) = -(T-1)(i_1 + j_1) + \big(u(d_1 - d_2)/g\big),$$

and thus $(T-1)(i_1 + j_1) \leq u(d_1 - d_2)/g$. On the other hand, the fact that j is nonnegative forces $(u/g) \leq Tj_1/d_1$. Combining these, we obtain

$$(T-1)(i_1 + j_1) \leq Tj_1(d_1 - d_2)/d_1,$$

which means that $Td_1 i_1 + Td_2 j_1 \leq d_1(i_1 + j_1)$, that is, $T(p-1) \leq d_1(i_1 + j_1)$, or equivalently

$$T(p-1) \leq d_1 i_1 + d_2 j_1 + (d_1 - d_2) j_1 = p - 1 + (d_1 - d_2) j_1,$$

so that $(T-1)(p-1) \leq (d_1 - d_2) j_1$. Now we know that $d_1 - d_2 \leq (p-1)/d_1$ from our given assumptions and $j_1 < d_1$ by (12), so we have $(T-1)(p-1) < p-1$, which forces $T = 1$.

Thus $i = i_1 + (ud_2/g)$ and $j = j_1 - (ud_1/g)$ and $d_1 i + d_2 j = d_1 i_1 + d_2 j_1 = p - 1$ and $i + j = i_1 + j_1 - (u(d_1 - d_2)/g)$. Since we have assumed that $i + j \leq i_1 + j_1$, this forces $u \geq 0$. So then $i \geq i_1$ and we can set $l = \lfloor (p-1)/d_1 \rfloor - i$, which is less

than or equal to $l_1 = \lfloor (p-1)/d_1 \rfloor - i_1$. Furthermore, since $d_1 i \leq d_1 i + d_2 j = p-1$, we know that $i \leq \lfloor (p-1)/d_1 \rfloor$. So l is nonnegative. Furthermore

$$p - 1 - d_1 \left(\left\lfloor \frac{p-1}{d_1} \right\rfloor - l \right) = p - 1 - d_1 i_1 = d_2 j \equiv 0 \bmod d_2$$

Thus by the minimality of l_1, we have $l = l_1$, which means $i = i_1$. This implies $u = 0$ and so $j = j_1$. □

Remark 3.3. Lemma 3.2 can be modified to be applied when $\gcd(d_1, d_2) \nmid p-1$. Let $g = \frac{\gcd(d_1,d_2)}{\gcd(d_1,d_2,p-1)}$. Then equation (10) is equivalent to

$$\left(\frac{d_1}{g}\right) i + \left(\frac{d_2}{g}\right) j \equiv 0 \bmod p-1.$$

Note that $\gcd\left(\frac{d_1}{g}, \frac{d_2}{g}\right) \mid (p-1)$. Hence $\mu_p(d_1, d_2) = \mu_p\left(\frac{d_1}{g}, \frac{d_2}{g}\right)$.

Now, we state the main result of this section.

Theorem 3.4. *With the same notation and assumptions as in Lemma 3.2, we have*

(1) $\nu_\theta\big(S_p(d_1, d_2)\big) = \left\lfloor \frac{p-1}{d_1} \right\rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2}$

(2) $p > |V_{aX^{d_1} + bX^{d_2}}| \geq \left\lfloor \frac{p-1}{d_1} \right\rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2} + 1.$

P r o o f. Now we prove the first part of the theorem. Combining Remark 2.2 and the uniqueness of Lemma 3.2, we obtain that the p-adic valuation:

$$\nu_\theta\big(S_p(d_1, d_2)\big) = \mu_p(d_1, d_2).$$

Also Lemma 3.2 implies that $\mu_p(d_1, d_2) = \lfloor \frac{p-1}{d_1} \rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2}$. The second part of the theorem follows substituting

$$\nu_p(d_1, d_2) = \left\lfloor \frac{p-1}{d_1} \right\rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2}$$

in Lemma 2.7 and applying the result of W a n, S h i u e, C h e n [20]. □

Those conditions of the Theorem 3.4 seem artificial but will lead to the calculation of p-adic valuation of exponential sums under natural conditions.

In the following corollary we impose conditions on d_1 and d_2 such that we can apply Theorem 3.4.

Corollary 3.5. *If $d_1 \leq \sqrt{p-1}$ and $\gcd(d_2, d_1) = 1$, then*

$$\nu_\theta\big(S_p(d_1, d_2)\big) = \left\lfloor \frac{p-1}{d_1} \right\rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2}$$

and

$$p > |V_{aX^{d_1}+bX^{d_2}}| \geq \left\lfloor \frac{p-1}{d_1} \right\rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2} + 1.$$

P r o o f. The condition $d_1 \leq \sqrt{p-1}$ implies that $l_1 \leq \lfloor \frac{p-1}{d_1} \rfloor$ and $d_1 - d_2 \leq \frac{p-1}{d_1}$. If $\gcd(d_2, d_1) = 1$, then there exists l_1 in Lemma 3.2. Hence applying Lemma we obtain desired result. □

Example 3.6. Let $p = 619$, $d_1 = 27$, $d_2 = 23$. The conditions of Theorem 3.4 are satisfied since $\lfloor \frac{618}{27} \rfloor = 22$, $s_1 = 24$, $j_1 = 24$, $l_1 = 17$ and $17 < 22$, $22 > 4 = 27 - 23$. In this case, we have that $\nu_\theta(S_{619}(27, 23)) = 22 - 17 + 21 = 26$ and $|V_{X^{27}+bX^{23}}| \geq 27$. Corollary 2.5 in [20] implies that $|V_{X^{27}+bX^{23}}| \geq 24$.

Remark 3.7. Theorem 3.4 can be modified to compute the p-adic valuation when $\gcd(d_1, d_2) \nmid p - 1$ using Remark 3.3.

Example 3.8. We want to compute the p-adic valuation of the exponential sum $S_{67}(35, 5)$ for $p = 67$. Note that $5 \nmid 66$. Using Remark 3.3, the modular equation associated to $S_{67}(35, 5)$ is $7i + j \bmod 66$. Now applying Lemma 3.2, we obtain that $\nu_\theta(S_{67}(35, 5)) = 12$.

Now, we apply Lemma 3.2 to give a lower bound to the value sets of binomials over $\mathbb{F}_q$.

Theorem 3.9. *With the same notation and assumptions as in Lemma 3.2, we have*

$$|V_{aX^{d_1}+bX^{d_2}}| \geq u_p(F) + 1 \geq \left\lfloor \frac{q-1}{d_1} \right\rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2} + 1,$$

whenever $u_p(F) < \infty$.

P r o o f. Lemma 3.2 is true substituting $p-1$ by $q-1$. Hence $u_p(F) \geq \nu_p(d_1, d_2) = \lfloor \frac{q-1}{d_1} \rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2}$ by Lemma 2.7. Applying the result of W a n, S h i u e, C h e n ([20]), we obtain $|V_{aX^{d_1}+bX^{d_2}}| \geq u_p(F)+1 \geq \lfloor \frac{q-1}{d_1} \rfloor + \frac{s_1 + l_1(d_1 - d_2)}{d_2} + 1$. □

Example 3.10. Consider the polynomial $F(X) = X^{11} + aX$ over $\mathbb{F}_{128}$. Using Theorem 3.9, we have that $|V_F| \geq 18$.

Remark 3.11. In [5], B l a c h e, F é r a r d, Z h u state the following conjecture: Let $\epsilon > 0$ and $F(X)$ be a polynomial of degree d over the rational numbers. If $\nu_p(S_p(F(X)) > \frac{1}{d} + \epsilon$ for infinitely many primes p, then $F(X) = P\big(D_n(x, c)\big)$ for some polynomial $P(X)$ over the rational numbers and a global Dickson polynomial D_n of degree $n > 0$. Corollary 3.5 implies

$$\lim_{p \to \infty} \frac{\nu_\theta\left(S_p(aX^{d_1} + bX^{d_2})\right)}{p-1} = \frac{1}{d_1},$$

whenever $\gcd(d_1, d_2) = 1$. For the case when $\gcd(d_2, d_1) > 1$, we need to use Remarks 3.3 and 3.7.

Remark 3.12. In [13], Katz used p-adic divisibility to obtain restrictions on families of exponential sums with three values.

Now we state a conjecture.

Conjecture. Let $s = \gcd(d_1 - d_2, p-1)$. If $s \leq \sqrt{p-1}$, then the modular equation (10) has a unique minimal solution.

The following Corollary follows from Theorem 3.4 for $d_2 = 2$.

Corollary 3.13. *Let $d_1 > 1$ be a positive integer and $p - 1 = \lfloor \frac{p-1}{d_1} \rfloor d_1 + s_1$ with $0 \leq s_1 < d_1$.*

(1) *If s_1 is even and $\frac{p-1}{d_1} > d_1 - 2$, then $\nu_\theta(S_p(d_1, 2)) = \lfloor \frac{p-1}{d_1} \rfloor + \frac{s_1}{2}$, and $p > |V_{aX^{d_1}+bX^2}| \geq \lfloor \frac{p-1}{d_1} \rfloor + \frac{s_1}{2} + 1$.*

(2) *If $d_1 s_1$ is odd and $\frac{p-1}{d_1} > d_1 - 2$, then*

$$\nu_\theta(S_p(d_1, 2)) = \left\lfloor \frac{p-1}{d_1} \right\rfloor - 1 + \frac{s_1 + d_1}{2},$$

and

$$p > |V_{aX^{d_1}+bX^2}| \geq \left\lfloor \frac{p-1}{d_1} \right\rfloor + \frac{s_1 + d_1}{2}.$$

Proof. The corollary follows considering all the congruent classes modulo $d_2 = 2$ and noting that $l_1 \leq 1$ in the case of $d_2 = 2$. □

Now we are going to improve Theorem 3.4 when

$$d_2 \mid s_1 \quad \text{and} \quad p - 1 = \left\lfloor \frac{p-1}{d_1} \right\rfloor d_1 + s_1, \quad 0 \leq s_1 \leq d_1 - 1.$$

Theorem 3.14. *Let $d_1 > 2$ be a positive integer. Let*

$$F(X) = aX^{d_1} + bX^{d_2} (ab \neq 0) \quad \textit{be a polynomial over } \mathbb{F}_p$$

and

$$p - 1 = \left\lfloor \frac{p-1}{d_1} \right\rfloor d_1 + s_1, \qquad \textit{where} \quad 0 \leq s_1 \leq d_1 - 1.$$

a. *If $s_1 \leq \lfloor \frac{p-1}{d_1} \rfloor$, then*

$$\nu_\theta\big(S_p(X^{d_1} + bX)\big) = \left\lfloor \frac{p-1}{d_1} \right\rfloor + s_1,$$

$$\textit{in particular, } p > V_F \geq \left\lfloor \frac{p-1}{d_1} \right\rfloor + s_1 + 1.$$

b. *If* $d_2 \mid s_1$ *and* $(p-1) \geq (d_1-d_2)^2$, *then*

$$\nu_\theta\big(S_p(X^{d_1}+bX^{d_2})\big) = \left\lfloor \frac{p-1}{d_1} \right\rfloor + \frac{s_1}{d_2},$$
$$\textit{in particular, } p > V_F \geq \left\lfloor \frac{p-1}{d_1} \right\rfloor + \frac{s_1}{d_2} + 1.$$

P r o o f. If $d_1 \mid p-1$, then $\nu_\theta\big(S_p(X^{d_1}+aX)\big) = \frac{p-1}{d_1}$. From now on, suppose that $d_1 \nmid (p-1)$. We have $p-1 = d_1\lfloor \frac{p-1}{d_1} \rfloor + s_1$ and $d_1 i_1 + j_1 = c(p-1)$ for some integer $c > 1$. Suppose that $i_1 + j_1 \leq \lfloor \frac{p-1}{d_1} \rfloor + s_1$. We have that

$$d_1 i_1 + j_1 + (d_1-1)j_1 \leq d_1 \left\lfloor \frac{p-1}{d_1} \right\rfloor + s_1 + (d_1-1)s_1 \Longleftrightarrow$$
$$(c-1)(p-1) + (d_1-1)j_1 \leq (d_1-1)s_1 \leq (d_1-1)\left\lfloor \frac{p-1}{d_1} \right\rfloor < p-1.$$

This is a contradiction, part **a** holds.

Now we are going to prove part **b**. If $d_1 \mid (p-1)$, then the theorem holds. From now on, we assume that $d_1 \nmid (p-1)$. Suppose that $i_1 + j_1 \leq \lfloor \frac{p-1}{d_1} \rfloor + \frac{s_1}{d_2}$, where $d_1 i_1 + d_2 j_1 = c(p-1), \lfloor \frac{p-1}{d_1} \rfloor d_1 + d_2(\frac{s_1}{d_2}) = p-1$ for $c > 1$. This implies that

$$d_1 i_1 + d_2 j_1 + (d_1-d_2)j_1 \leq d_1 \left\lfloor \frac{p-1}{d_1} \right\rfloor + s_1 + (d_1-d_2)\left(\frac{s_1}{d_2}\right).$$

The last inequality can be written as follows:

$$c(p-1) + (d_1-d_2)j_1 \geq p-1 + (d_1-d_2)\frac{s_1}{d_2} \Longleftrightarrow$$
$$(c-1)(p-1) \leq \left(\frac{s_1}{d_2} - j_1\right)(d_1-d_2). \quad (13)$$

Therefore $\frac{s_1}{d_2} > j_1$. We have $i_1 > \lfloor \frac{p-1}{d_1} \rfloor$ since $i_1 \geq (c-1)(\frac{p-1}{d_1})$. Then

$$c(p-1) = (d_1-d_2)i_1 + d_2(i_1+j_1) \leq (d_1-d_2)i_1 + d_2\left(\left\lfloor \frac{p-1}{d} \right\rfloor + \frac{s_1}{d_2}\right)$$
$$= (d_1-d_2)i_1 + (p-1) - (d_1-d_2)\left\lfloor \frac{p-1}{d_1} \right\rfloor,$$
$$p-1 \leq (c-1)(p-1) \leq (d_1-d_2)\left(i_1 - \left\lfloor \frac{p-1}{d_1} \right\rfloor\right) \leq (d_1-d_2)\left(\frac{s_1}{d_2} - j_1\right)$$
$$\leq (d_1-d_2)\left(\frac{d_1-1}{d_2} - 1\right) \leq (d_1-d_2)\left(\frac{d_1-1-d_2}{d_2}\right)$$
$$< (d_1-d_2)^2, \qquad \text{for } j_1 \geq 1.$$

This is a contradiction, i.e., $(p-1) < (d_1-d_2)^2$. If $j_1 = 0$, then

$$(p-1) \leq (c-1)(p-1) \leq (d_1-d_2)\left(\frac{s_1}{d_2}\right). \tag{14}$$

We have two cases:

- if $s_1 = d_2$, then $(p-1) \leq (d_1-d_2) \leq (d_1-d_2)^2$. This is a contradiction since $d_1 - d_2 < p-1$.
- if $1 < d_2 < s_1$, then

$$\begin{aligned} d_2+1 < d_1 &\to d_2^2 - 1 < d_1 d_2 - d_1 \\ &\to d_1 - 1 < d_1 d_2 - d_2^2 \\ &\to \frac{d_1-1}{d_2} < d_1 - d_2 \\ &\to \frac{s_1}{d_2} \leq \frac{d_1-1}{d_2} < d_1 - d_2 \\ &\to (d_1-d_2)\frac{s_1}{d_2} < (d_1-d_2)^2 \\ &\to (p-1) \leq (d_1-d_2)\frac{s_1}{d_2} < (d_1-d_2)^2. \end{aligned}$$

This is a contradiction. If $d_2 = 1$, then (14) gives the desired contradiction. □

4. Divisibility of $S_p(aX^{d_1} + bX^{d_2})$ when $(d_1 - d_2) \mid (p-1)$

In this section, we estimate the p-adic valuation of exponential sums of type $S_p(d_1, d_2)$, where $d_1 - d_2$ divides $p-1$. This result is an improvement to the results of Section 3 when $d_1 - d_2$ divides $p-1$. In particular, we compute the p-adic valuation of $S_p(d_1, d_2)$ when $\frac{d_2(d_1-d_2)}{p-1}$ and $\frac{d_1(d_1-d_2)}{p-1}$ satisfy certain conditions. We apply our calculation of $\mu_p(d_1, d_2)$ to the value sets of these binomials.

Our results of this section allow us to determine families of polynomials that do not permute $\mathbb{F}_p$. In particular, we obtain that if $d_1 - 1$ divides $p-1$ and $F(X) = X^{d_1} + bX$ permutes $\mathbb{F}_p$, then $d_1 \geq \sqrt{2(p-1)}$. This is an improvement to the known results in this special case(see [4]).

Lemma 4.1. *Let $d_1 > d_2$ be positive integers satisfying $\gcd(d_1, d_2) = 1$ and $(d_1 - d_2) \mid (p-1)$. Let $\boldsymbol{\nu} = (p-1)/(d_1-d_2)$. Let $n_0 \geq 1$ be the smallest integer for which there exists an integer $c > 0$ such that*

$$\frac{n_0 d_2}{\boldsymbol{\nu}} \leq c \leq \frac{n_0 d_1}{\boldsymbol{\nu}}. \tag{15}$$

Then for the modular equation $d_1 i + d_2 j \equiv 0 \bmod p-1$*, we have that*:

(1) *for each* $c > 0$ *satisfying* (15)*, the pair* (i,j) *with* $i = c\boldsymbol{\nu} - n_0 d_2$*,* $j = n_0 d_1 - c\boldsymbol{\nu}$*, is a solution of the modular equation and the sum* $i + j = n_0(d_1 - d_2)$ *is the minimal sum.*

(2) *If* $d_1 > \boldsymbol{\nu}$ *and* $d_2/\boldsymbol{\nu} \leq \lfloor d_1/\boldsymbol{\nu} \rfloor - 1$*, then the modular equation has more than one solution with minimal sum.*

(3) *If* $d_1 \leq \boldsymbol{\nu}$ *or if* $d_1 > \boldsymbol{\nu}$ *and* $d_2/\boldsymbol{\nu} > \lfloor d_1/\boldsymbol{\nu} \rfloor - 1$*, then there is a unique pair satisfying the modular equation with minimal sum.*

P r o o f. Let (i,j) be any solution of the modular equation $d_1 i + d_2 j \equiv 0 \bmod p-1$, with $i,j \geq 0$, $(i,j) \neq (0,0)$. Let $S = i + j$ and $d = d_1 - d_2$. Then $(S-j)d_1 + jd_2 = c'(p-1) = c'd\boldsymbol{\nu}$, for some integer $c' > 0$. From here, $Sd_1 = (c'\boldsymbol{\nu} + j)d$ and $S = ((c'\boldsymbol{\nu} + j)/d_1)d$ with $(c'\boldsymbol{\nu} + j)/d_1$ an integer, since $\gcd(d_1, d) = 1$. Likewise $S = ((c'\boldsymbol{\nu} - i)/d_2)d$. Let n_0 and c as in the statement of this lemma. Let $i' = c\boldsymbol{\nu} - n_0 d_2$ and $j' = n_0 d_1 - c\boldsymbol{\nu}$. Then $i' \geq 0$, $j' \geq 0$ and $i' \neq 0$ or $j' \neq 0$ since $d_1 \neq d_2$. Clearly (i', j') is a solution of the modular equation and $i' + j' = n_0 d$ is the minimal sum.

For the second point, assume $d_1 > \boldsymbol{\nu}$. Let $d_1 = q\boldsymbol{\nu} + r$ with q, r integers and $0 \leq r < \boldsymbol{\nu}$. When $d_2/\boldsymbol{\nu} \leq q-1$, we have $d_1/\boldsymbol{\nu} \geq q > q-1 \geq d_2/\boldsymbol{\nu}$ so $n_0 = 1$ and $c = q$ and $c = q-1$ satisfy equation (15).

For the third point, assume $d_1 \leq \boldsymbol{\nu}$. If $d_1 = \boldsymbol{\nu}$, then $d_1/\boldsymbol{\nu} = 1 > d_2/\boldsymbol{\nu}$, so $c = 1$ and $n_0 = 1$. When $d_1 < \boldsymbol{\nu}$, we have that $\boldsymbol{\nu} = qd_1 + r$, with q, r integers, $0 \leq r < d_1$, and $(q+1)d_1 < 2\boldsymbol{\nu}$. If $(q+1)d_2 \leq \boldsymbol{\nu}$, then $(q+1)d_2/\boldsymbol{\nu} \leq 1 < (q+1)d_1/\boldsymbol{\nu}$ so $n_0 = q+1$ and there is a unique $c = 1$.

In the case that $(q+1)d_2 > \boldsymbol{\nu}$, we have $1 < (q+1)d_2/\boldsymbol{\nu} < (q+1)d_1/\boldsymbol{\nu} < 2$. Let m be the minimal positive integer for which there exists an integer f such that $f < md_2/\boldsymbol{\nu} < md_1/\boldsymbol{\nu} < f+1$ and $(m+1)d_2/\boldsymbol{\nu}$ and $(m+1)d_1/\boldsymbol{\nu}$ do not belong to the same open interval $(g, g+1)$ for all integer $g \geq 0$. Since $f < (m+1)d_2/\boldsymbol{\nu} < (m+1)d_1/\boldsymbol{\nu} = md_1/\boldsymbol{\nu} + d_1/\boldsymbol{\nu} < f+2$ and the assumption on m, we have that $f+1 = (m+1)d_2/\boldsymbol{\nu}$ or $f+1 = (m+1)d_1/\boldsymbol{\nu}$ or $(m+1)d_2/\boldsymbol{\nu} < f+1 < (m+1)d_1/\boldsymbol{\nu}$. In any of these cases $n_0 = m+1$ and only $c = f+1$ satisfies (15).

Assume now $d_1 > \boldsymbol{\nu}$ and $d_2/\boldsymbol{\nu} > q-1$, where $q = \lfloor d_1/\boldsymbol{\nu} \rfloor$. In the case that $d_1/\boldsymbol{\nu} \geq q > d_2/\boldsymbol{\nu} > q-1$, we have that $n_0 = 1$ and $c = q$ is the unique integer satisfying (15). The same occurs when $d_2/\boldsymbol{\nu} = q$ (so $d_1/\boldsymbol{\nu} > q = d_2/\boldsymbol{\nu}$). For the other case $q+1 > d_1/\boldsymbol{\nu} > d_2/\boldsymbol{\nu} > q$, let m be the minimal positive integer for which there exists an integer f such that $f < md_2/\boldsymbol{\nu} < md_1/\boldsymbol{\nu} < f+1$ and $(m+1)d_1/\boldsymbol{\nu}$ and $(m+1)d_2/\boldsymbol{\nu}$ do not belong to the same open interval $(g, g+1)$ for all integer $g > 0$. Then $(m+1)d_2/\boldsymbol{\nu} = md_2/\boldsymbol{\nu} + d_2/\boldsymbol{\nu} > f+q$ and

$(m+1)d_1/\boldsymbol{\nu} < f+1+q+1$ and by the assumption on m, we have $n_0 = m+1$ and $c = f+q+1$ is the unique integer that satisfies (15). □

Remark 4.2. Lemma 4.1 can be modified to compute $\mu_p(d_1,d_2) = n_0(d_1-d_2)$ when $\gcd(d_1,d_2) > 1$ and $(d_1-d_2) \mid (p-1)$. If $\gcd(d_1,d_2) = g > 1$, then we need to apply Lemma 4.1 to the modular equation

$$d_1' i + d_2' j \equiv 0 \bmod \frac{p-1}{\gcd(g,p-1)}, \quad \text{where } d_1 = gd_1' \quad \text{and} \quad d_2 = gd_2'.$$

Now we state the main result of this section that follows immediately from Lemma 4.1.

Theorem 4.3. *With the same notation and assumptions as in Lemma 4.1, we have*:

(1) $\nu_\theta(S_p(F)) \geq n_0(d_1-d_2)$ *and* $|V_F| \geq n_0(d_1-d_2)+1$.
(2) *If* $d_1 \leq \boldsymbol{\nu}$ *or if* $d_1 > \boldsymbol{\nu}$ *and* $d_2/\boldsymbol{\nu} > \lfloor d_1/\boldsymbol{\nu} \rfloor - 1$, *then*:
   - $\nu_\theta(S_p(F)) = n_0(d_1-d_2)$.
   - F *is not a permutation polynomial of* $\mathbb{F}_p$.

Now we apply Theorem 4.3 to families of polynomials.

Example 4.4. Various examples:

- Let $F(X) = X^{49} + bX^{15}$ be a polynomial over $\mathbb{F}_{919}$. In this case $d_1 - d_2 = 34$ and $\boldsymbol{\nu} = 27$. Applying Theorem 4.3, equation (10) has a unique minimal solution. Hence, $\nu_\theta(S_{919}(F)) = 34$ and $p > V_F \geq 35$. Note that Theorem 1.7 in [4] does not give any information since $1122 = 34 \times 33 > 918$.
- Let $F(X) = X^{p-2} + bX^{p-3}$ be a polynomial over $\mathbb{F}_p$. In this case $d_1 - d_2 = 1$ and $\boldsymbol{\nu} = p-1$. Theorem 4.3 implies that $\nu_2(S(p-2,p-3)) = \frac{p-1}{2}$ and $|V_F| = \frac{p+1}{2}$. Using the Cauchy-Davenport Theorem, we obtain that any $\alpha \in \mathbb{F}_p$ can be written as follows: $x^{p-2} + y^{p-2} + a(x^{p-3} + y^{p-3}) = \alpha$. We have that the Waring number of F is 2 since F is not a permutation polynomial of $\mathbb{F}_p$ ([22]).
- Let $F(X) = X^{p-3} + bX^{p-4}$ be a polynomial over $\mathbb{F}_p$. In this case $d_1 - d_2 = 1$ and

$$n_0 = \begin{cases} \frac{p-1}{3} & p \equiv 1 \bmod 3\,, \\ \frac{p+1}{3} & p \equiv 2 \bmod 3\,. \end{cases}$$

Theorem 4.3 implies that

$$\nu_2\big(S(p-3,p-4)\big) = \frac{p-\delta}{3} \quad \text{and} \quad |V_F| \geq \frac{p+3-\delta}{3}, \quad \text{where } \delta \in \{-1,1\}.$$

The following corollary is an improvement to Corollary 2.5 of [4] whenever $(d_1 - 1)$ divides $(p - 1)$.

Corollary 4.5. *Let $F(X) = aX^{d_1} + bX$ be a binomial over $\mathbb{F}_p$, so $d_2 = 1$, where $ab \neq 0$. Suppose d_1 is an integer satisfying $d_1 > 2$ and $(d_1 - 1)$ divides $(p - 1)$. Let $\boldsymbol{\nu} = (p-1)/(d_1-1) = \lfloor \frac{\boldsymbol{\nu}}{d_1} \rfloor d_1 + s_1, 0 \leq s_1 < d_1$. Then*

(1) $\nu_\theta\big(S_p(F)\big) = \big(\lfloor \frac{\boldsymbol{\nu}}{d_1} \rfloor + 1\big)(d_1 - 1)$, *whenever* $d_1 < \sqrt{2(p-1)}$.

(2) $p > |V_F| \geq \big(\lfloor \frac{\boldsymbol{\nu}}{d_1} \rfloor + 1\big)(d_1 - 1) + 1$, *whenever* $d_1 < \sqrt{2(p-1)}$.

(3) *If $F(X)$ permutes $\mathbb{F}_p$, then* $d_1 \geq \sqrt{2(p-1)}$.

P r o o f. The proof of Corollary 4.5 follows from Theorem 4.3 considering the cases $\boldsymbol{\nu} > d_1$ and $\boldsymbol{\nu} \leq d_1$. Note that the hypothesis $d_1 < \sqrt{2(p-1)}$ of the corollary implies that $d_1 < 2\boldsymbol{\nu}$. □

Remark 4.6. The modular equation associated to the polynomial $F(X) = aX^{d_1} + bX$ defined in Corollary 4.5 has a unique minimal solution. This is not true for $d_1 - 1 < \sqrt{2(p-1)}$. Taking $p = 67$ and $d_1 = 12$, we have that the modular equation $12i + j \equiv 0 \bmod 66$ has two minimal solutions: $(5, 6), (11, 0)$. Note that $12 - 1 = 11 < \sqrt{2(p-1)} = \sqrt{132} \approx 11.49$.

Example 4.7. Let $F(X) = X^{15} + bX$ be a polynomial over $\mathbb{F}_{127}$. In this case $\sqrt{2(126)} \approx 15.87$. Corollary 4.5 implies $\nu_\theta(S_{127}(F)) = 14$ and F is not a permutation polynomial of $\mathbb{F}_{127}$.

Acknowledgments. The authors thank the referee for careful reading the paper as well as many helpful comments and corrections. Also, we are grateful to the referee for providing a shorter and more elegant proof of Lemma 3.2 than the original proof.

REFERENCES

[1] ADOLPHSON, A.—SPERBER, S.: *p-adic Estimates for Exponential Sums and the Theorem of Chevalley-Warning*, Ann. Sci. Ecole Norm. Sup., **20** (1987), 545–556.

[2] ADOLPHSON, A.—SPERBER, S.: *Exponential Sums Nondegenerate Relative to a Lattice*, Algebra Number Theory **8**(2009), 881–906.

[3] AX, J.: *Zeros of Polynomials over Finite Fields*, Am. J. of Math., **86**(1964), 255–261.

[4] AYAD, M.—BELGHABA, K.—KIHEL, O.: *On Permutations Binomials over Finite Fields*, Bull. Aust. Math. Soc., **89**(2014), 116–124.

[5] BLACHE, R.— FÉRARD, E.—ZHU, H. J.: *Hodge-Stickelberger for L-functions of Exponential Sums of $P(x^s)$*, Math. Res. **15**(2008), 1053–1071.

[6] BLACHE, R.: *Valuation of Exponential Sums and the Generic First Slope for Artin-Schreier Curves*, J. Number Theory **132**(2012), 2336–2352.

[7] CASTRO, F.—RUBIO, I.—VEGA, J.: *Divisibility of Exponential Sums and Solvability of Certain Equations over Finite Fields*, The Quart. J. Math., **60**(2008), 169–181.

[8] CASTRO, F.—FIGUEROA, R.—MEDINA, L.: *Exact divisibility of exponential sums and some consequences*, Contemp. Math. **579**(2012), 55–66.

[9] CASTRO, F.—CASTRO-VELEZ, F.: *Improvement to Moreno-Moreno's theorems*, Finite Fields Appl.**18**(2012), 1207–1216.

[10] CASTRO, F.—RUBIO, I.: *Exact p-divisibility of exponential sums via the covering method*, Proc. Amer. Math. Soc. **143** (2015), 1043–1056.

[11] CONWAY J. H.—JONES, A. J.: *Trigonometric Diophantine Equations(On vanishing sums of roots of unity)*, Acta Arith. **XXX**(1976), 229–240.

[12] LIDL, R.—NIEDERREITER, H.: *Finite Fields*, Encyclopedia of Mathematics and its Applications Vol. 20, Cambridge University Press, Cambridge 1997.

[13] KATZ, D.: *Divisibility of Weil Sums of Binomials*, Proc. Amer. Math. Soc. **143**(2015), 4623–4632.

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

[15] MORENO, O.—SHUM, K.—CASTRO, F. N.—KUMAR, P. V.: *Tight Bounds for Chevalley-Warning-Ax Type Estimates, with Improved Applications*, Proc. Lond. Math. Soc. **88**(2004), 545–564.

[16] MORENO, C. J.: *Algebraic Curves Over Finite Fields*, Cambridge University Press, Cambridge 1991.

[17] MULLEN, G.—WAN, D.—WANG, Q.: *Value Sets of Polynomials Maps over Finite Fields*, Quart. J. Math. **64**(2013) 1191–1196.

[18] SCHOLTEN, S.—ZHU, H. J.: *The First Case of Wan's Conjecture*, Finite Fields Appl. **8**(2002), 414–419.

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

[20] WAN, D.—JAU-SHYONG SHIUE, P.— CHEN, C. S.: *Value Sets of Polynomials over Finite Fields*, Proc. Amer. Math. Soc. **119**(1993), 711–717.

[21] YANG, R.: *Newton Polygons of L-functions of polynomials of the form $x^d + \lambda x$*, Finite Fields Appl. **9**(2003), 59–88.

[22] WINTERHOF, A.: *On Waring's Problem in Finite Fields*, Acta Arith. **LXXXVII.2** (1998), 171–177.

[23] ZHU, H. J.: *p-adic Variation of L functions of One Variable Exponential Sums*, J. Reine Angew. Math. **572**(2004), 219–233.

[24] ZHU, H. J.: *Asymptotic Variation of L functions of One Variable Exponential Sums I*, Amer. J. Math. **125**(2003), 669–690.

Received July 8, 2015
Accepted December 16, 2015

Francis N. Castro
Raúl Figueroa
Puhua Guan
Department of Mathematics
University of Puerto Rico
Río Piedras
P. O.Box 70377
Puerto Rico 00936–8377
U.S.A
E-mail: franciscastr@gmail.com
junioyjulio@gmail.com
pguan31@gmail.com