Communications
in
Mathematical
Research
**33**(4)(2017), 359–362

# On the Lower Bound of the Divisibility of Exponential Sums in Binomial Case

Liu Xiao-gang
(*School of Computer Science and Technology, Nanjing Tech University, Nanjing, 211800*)

Communicated by Du Xian-kun

**Abstract:** In this article, we analyze the lower bound of the divisibility of families of exponential sums for binomials over prime field. An upper bound is given for the lower bound, and, it is related to permutation polynomials.
**Key words:** exponential sum, finite field, binomial, permutation polynomial
**2010 MR subject classification:** 11L07, 12E30
**Document code:** A
**Article ID:** 1674-5647(2017)04-0359-04
**DOI:** 10.13447/j.1674-5647.2017.04.08

## 1 Introduction

Exponential sums and their divisibility have been applied to characterize important properties of objects in applied mathematics. There are many estimates for the divisibility of exponential sums (see [1]–[5]). It is difficult in general. The exact divisibility of families of exponential sums associated to binomials $F(X) = aX^{d_1} + bX^{d_2}$, is computed under some natural conditions when $a, b \in \mathbb{F}_p^*$ (see [2]). The result is applied to the solutions of equations, to the study of Waring problem over finite fields, and to the determination of permutation polynomials.

Let $F(X)$ be a two terms of polynomial in one variable over prime field $\mathbb{F}_p$. The following bound for the valuation (divisibility) of an exponential sum can be thought of as a particular case of Theorem 8 in [4].

**Theorem 1.1** *Let $F(X) = aX^{d_1} + bX^{d_2}$ with $a, b \in \mathbb{F}_p^*$, $1 \le d_1 \ne d_2 \le p-2$. If $S_p(F)$ is the exponential sum $\sum\limits_{X\in\mathbb{F}_p} \phi(F(X))$, then $\nu_\theta(S_p(F)) \ge \mu_p(d_1,\ d_2)$, where*

$$\mu_p(d_1,\ d_2) = \min_{(i,j)}\{i + j \mid 0 \le i, j < p\}, \qquad (i,\ j) \ne (0,\ 0)$$

**Received date:** Aug. 22, 2016.
**Foundation item:** The NSF (61502230) of China.
**E-mail address:** liuxg0201@163.com (Liu X G).

*is a solution of the modular equation*

$$d_1 i + d_2 j \equiv 0 \bmod p-1.$$

**Remark 1.1** Let $\mathbb{Q}_p$ be the $p$-adic field and $\xi$ be a primitive $p$-th root of unity in $\overline{\mathbb{Q}}_p$. Define $\theta = 1-\xi$ and denote by $\nu_\theta$ the valuation over $\theta$. Note that $\nu_\theta(p) = p-1$ and $\nu_p(x) = \dfrac{\nu_\theta(x)}{p-1}$. Let $\phi : \mathbb{F}_p \to \mathbb{Q}(\xi)$ be the nontrivial additive character defined by $\phi(a) = \xi^a$ for $a \in \mathbb{F}_p$. The exponential sum associated to $F(X)$ is defined as $S_p(F) = \sum\limits_{X\in\mathbb{F}_p} \phi(F(X))$.

In the next section, Theorem 2.1 is presented on the lower bound in Theorem 1.1, which is less than half of $p$. To this end, the domain $[0,\ 1)$ is splitted into infinitely many segments, which are used for different range of integers. In this process, we can make a success in our analysis for every step, which is not enough for the whole. But finally, with the splitting parts changing and interacting with each other, we can make it complete. Though not much long and complicated, the important idea in our work is to note the effect of those seemingly nonsignificant interactions between different segments.

## 2 Main Result

**Theorem 2.1** *Let $1 \le d_1 \ne d_2 \le p-2$ be positive integers and let $p \ge 5$ be a prime. Then*

$$\mu_p(d_1,\ d_2) \le \frac{p-1}{2}. \tag{2.1}$$

*Proof.* First, consider the case when $d_1$, $d_2$ are odd numbers, and

$$\gcd(d_1,\ p-1) = \gcd(d_2,\ p-1) = 1,$$

where gcd denotes the greatest common divisor of two or more integers.

Let $i = 1$. Then $d_1 i + d_2 j = d_1 + d_2 j$. If it is zero modular $p-1$, then $j \ne p-1$; if $j = p-2$, then $d_1 + d_2 j = d_1 + d_2(p-2) = d_1 + d_2(p-1) - d_2$ is not equal to zero modular $p-1$. Also, $j \ne 0$. Note that such a $j$ must exist since $\gcd(d_2,\ p-1) = 1$. So,

$$1 \le j \le p-3. \tag{2.2}$$

If $j > \dfrac{p-1}{2}$, then we consider the following sets

$$\left[1-\frac{1}{2^{k-1}},\ 1-\frac{1}{2^k}\right), \qquad k = 1, 2, 3, \cdots$$

We can find that the union of the sets is $[0,\ 1)$. Assume that $j = \alpha_{k-1}(p-1)$ and $\alpha_{k-1} \in \left[1-\dfrac{1}{2^{k-1}},\ 1-\dfrac{1}{2^k}\right)$. Then

$$1-\frac{1}{2^{k-1}} \le \alpha_{k-1},$$

which implies that by (2.2)

$$\left(1-\frac{1}{2^{k-1}}\right)(p-1) \le p-3,$$