Finite Fields and Their Applications 41 (2016) 113–131

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Special values of Kloosterman sums and binomial bent functions

Chunming Tang[a,*], Yanfeng Qi[b]

[a] *School of Mathematics and Information, China West Normal University, Nanchong, Sichuan, 637002, China*
[b] *School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China*

ARTICLE INFO

Article history:
Received 1 April 2014
Received in revised form 10 May 2016
Accepted 11 June 2016
Communicated by Stephen D. Cohen

MSC:
06E75
94A60
11T23

Keywords:
Regular bent function
Walsh transform
Kloosterman sums
π-adic expansion
Cyclotomic fields

ABSTRACT

Let $p \geq 7$ and $q = p^m$. $K_q(a) = \sum_{x\in\mathbb{F}_{p^m}} \zeta^{\mathrm{Tr}_1^m(x^{p^m-2}+ax)}$ is the Kloosterman sum of a on $\mathbb{F}_{p^m}$, where $\zeta = e^{\frac{2\pi\sqrt{-1}}{p}}$. The value $1 - \frac{2}{\zeta+\zeta^{-1}}$ of $K_q(a)$ and its conjugate have close relationship with a class of binomial functions with Dillon exponent. This paper first presents some necessary conditions for a such that $K_q(a) = 1 - \frac{2}{\zeta+\zeta^{-1}}$. Further, we prove that if $p = 11$, for any a, $K_q(a) \neq 1 - \frac{2}{\zeta+\zeta^{-1}}$. And for $p \geq 13$, if $a \in \mathbb{F}_{p^s}$ and $s = \gcd(2, m)$, $K_q(a) \neq 1 - \frac{2}{\zeta+\zeta^{-1}}$. In application, these results explain that some class of binomial regular bent functions does not exist.

* Corresponding author.
E-mail address: tangchunmingmath@163.com (C. Tang).

http://dx.doi.org/10.1016/j.ffa.2016.06.001

1. Introduction

Let $q = p^m$ and $\mathbb{F}_q$ be a finite field with q elements, where p is a prime and m is a positive integer. The Kloosterman sum of a on $\mathbb{F}_q$ is

$$K_q(a) = 1 + \sum_{x \in \mathbb{F}_q^*} \zeta^{\mathrm{Tr}_1^m(\frac{1}{x}+ax)}, a \in \mathbb{F}_q,$$

where Tr_1^m is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $\zeta = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity. Kloosterman sums are related to the construction of some Dillon type bent functions.

Let $n = 2m$. When $p = 2$, Dillon [2] proved that monomial function $\mathrm{Tr}_1^n(ax^{t(q-1)})$ ($a \in \mathbb{F}_{p^n}^*$, $\gcd(t, q+1) = 1$) is bent if and only if $K_q(a^{q+1}) = 0$, i.e., a^{q+1} is the zero point of Kloosterman sum K_q. Helleseth and Kholosha [8] generalized Dillon's results for $p > 2$. When $p = 2, 3$, there exist many zero points of Kloosterman sums [10,13]. Kononen et al. [12] proved the fact that the Kloosterman sum $K_q(\alpha)$ does not take the value zero for $p > 3$. Moisio [15] proved that any zero point of Kloosterman sums does not belong to a proper subfield of $\mathbb{F}_q$.

When $p \geq 3$, the binomial function $\mathrm{Tr}_1^n(ax^{t(q-1)}) + bx^{\frac{p^n-1}{2}}$ ($a \in \mathbb{F}_{p^n}^*$) is studied by Jia et al. [9] and Zheng et al. [21], where $b \in \mathbb{F}_p$ and $\gcd(t, q+1) = 1$. This function is bent if and only if $K_q(a) = 1 - \frac{2}{\zeta^b+\zeta^{-b}}$. Hence, for determining such bent functions, it is important to study the value $1 - \frac{2}{\zeta^b+\zeta^{-b}}$ of Kloosterman sums. Kononen [15] presented a solution for $b = 0$.

Divisibility results for Kloosterman sums are vital and have many applications. On divisibility results of Kloosterman sums, many works can be found in [19,3–6,14]. Moloney [16] analyzed divisibility results for $K_q(a)$ by p-adic methods.

This paper will study the special value $1 - \frac{2}{\zeta^b+\zeta^{-b}}$ of Kloosterman sums. By the π-adic expansions of $K_q(a)$ and $1 - \frac{2}{\zeta^b+\zeta^{-b}}$, we obtain some necessary conditions for $K_q(a) = 1 - \frac{2}{\zeta^b+\zeta^{-b}}$, where π is a prime of local field $\mathbb{Q}_p(\zeta)$ satisfying $\pi^{p-1} + p = 0$ and $\zeta \equiv 1 + \pi \mod \pi^2$. Further, we prove that if $p = 11$, for any $a \in \mathbb{F}_q$, $K_q(a) \neq 1 - \frac{2}{\zeta^b+\zeta^{-b}}$, and if $p \geq 13$, $a \in \mathbb{F}_{p^s}$ and $s = \gcd(2, m)$, $K_q(a) \neq 1 - \frac{2}{\zeta^b+\zeta^{-b}}$. Hence, these results explain that some class of binomial regular bent functions does not exist.

The rest of the paper is organized as follows. Section 2 introduces some background knowledge. Section 3 gives the π-adic expansion of Kloosterman sums and elements in $\mathbb{Q}_p(\zeta)$. Section 4 presents results on special values of Kloosterman sums. Section 5 proves some results on bent functions for application. Section 6 makes a conclusion.

2. Preliminaries

2.1. Local fields and Gauss sums

Throughout this paper, let $q = p^m$, $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$, where p is a prime and m is a positive inte-