Finite Fields and Their Applications 40 (2016) 201–223

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On a class of diagonal equations over finite fields

Ioulia N. Baoulina

Department of Mathematics, Moscow State Pedagogical University, Krasnoprudnaya str. 14, Moscow 107140, Russia

ARTICLE INFO

Article history:
Received 12 February 2016
Received in revised form 10 April 2016
Accepted 26 April 2016
Available online 4 May 2016
Communicated by Daqing Wan

To the memory of my first teacher in number theory, Elena B. Gladkova (1953–2015)

MSC:
11G25
11T24

Keywords:
Equation over a finite field
Diagonal equation
Gauss sum
Jacobi sum

ABSTRACT

Using properties of Gauss and Jacobi sums, we derive explicit formulas for the number of solutions to a diagonal equation of the form $x_1^{2^m}+\cdots+x_n^{2^m}=0$ over a finite field of characteristic $p\equiv\pm 3 \pmod 8$. All of the evaluations are effected in terms of parameters occurring in quadratic partitions of some powers of p.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic $p>2$ with $q=p^s$ elements, η be the quadratic character on $\mathbb{F}_q$ ($\eta(x)=+1,-1,0$ according as x is a square, a non-square or zero in $\mathbb{F}_q$), and $\mathbb{F}_q^*=\mathbb{F}_q\setminus\{0\}$. A diagonal equation over $\mathbb{F}_q$ is an equation of the type

E-mail address: jbaulina@mail.ru.

http://dx.doi.org/10.1016/j.ffa.2016.04.005

$$a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}=b, \tag{1}$$

where $a_1,\ldots,a_n\in\mathbb{F}_q^*$, $b\in\mathbb{F}_q$ and $d_1,\ldots,d_n$ are positive integers. As x_j runs through all elements of $\mathbb{F}_q$, $x_j^{d_j}$ runs through the same elements as $x_j^{\gcd(d_j,q-1)}$ does with the same multiplicity. Therefore, without loss of generality, we may assume that d_j divides $q-1$ for all j. Denote by $N[a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}=b]$ the number of solutions to (1) in $\mathbb{F}_q^n$.

The pioneering work on diagonal equations has been done by Weil [14], who expressed the number of solutions in terms of Gauss sums. For certain choices of coefficients $a_1,\ldots,a_n,b$, exponents $d_1,\ldots,d_n$ and finite fields $\mathbb{F}_q$, the explicit formulas for the number of solutions can be deduced from Weil's expression, see [3,4,6,8,10–13,15,16] for some results in this direction. However, in general, it is a difficult task to determine $N[a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}=b]$.

In this paper, we consider a diagonal equation of the form

$$x_1^{2^m}+\cdots+x_n^{2^m}=0, \tag{2}$$

where m is a positive integer with $2^m\mid(q-1)$. It is well known (see [4, Theorem 10.5.1] or [10, Theorems 6.26 and 6.27]) that

$$N[x_1^2+\cdots+x_n^2=0]=\begin{cases} q^{n-1}+\eta((-1)^{n/2})q^{(n-2)/2}(q-1) & \text{if } n \text{ is even},\\ q^{n-1} & \text{if } n \text{ is odd}.\end{cases}$$

Moreover, if $p\equiv 3 \pmod 4$ and $2\mid s$, then it follows from the result of Wolfmann [15, Corollary 4] that

$$N[x_1^4+\cdots+x_n^4=0]=q^{n-1}+(-1)^{((s/2)-1)n}q^{(n-2)/2}(q-1)\cdot\frac{3^n+(-1)^n\cdot 3}{4}.$$

Further, for any m with $2^m\mid(q-1)$, it is not hard to show that

$$N[x_1^{2^m}+x_2^{2^m}=0]=\begin{cases} 2^m(q-1)+1 & \text{if } 2^{m+1}\mid(q-1),\\ 1 & \text{if } 2^m\parallel(q-1).\end{cases}$$

The goal of this paper is to determine explicitly $N[x_1^{2^m}+\cdots+x_n^{2^m}=0]$ for an arbitrary n in the case when $p\equiv\pm3 \pmod 8$ and

$$m\geq\begin{cases} 3 & \text{if } p\equiv 3 \pmod 8),\\ 2 & \text{if } p\equiv -3 \pmod 8).\end{cases}$$

In Section 3, we treat the case $p\equiv 3 \pmod 8$. The main results of this section are Theorems 18 and 19, in which we cover the cases $2^{m+1}\mid(q-1)$ and $2^m\parallel(q-1)$, respectively. Our main results in Section 4 are Theorems 22 and 23, in which we deal with the case $p\equiv -3 \pmod 8$. All of the evaluations in Sections 3 and 4 are effected in