International Journal of Pure and Applied Mathematics

Volume 50 No. 4 2009, 569-576

ON THE NUMBER OF SOLUTIONS OF THE EQUATION $a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_s$ IN FINITE FIELDS

Luo Yanmei[1], Zhao Zhengjun[2], Cao Xiwang[3] §

[1,2,3]Department of Mathematics
Nanjing University of Aeronautics and Astronautics
Nanjing, 210016, P.R. CHINA
[1]e-mail: ymluo@nuaa.edu.cn
[2]e-mail: zzj0608115@126.com
[3]e-mail: xwcao@nuaa.edu.cn

Abstract: Let $\mathbb{F}_q$ be a finite field with $q = p^f$ elements, where p is an odd prime. Let $N(a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_s)$ denote the number of solutions of the equation

$$a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_s$$

in the finite field $\mathbb{F}_q$. We obtain the explicit formula for $N(a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_s)$, where $n \geq 3$, $s > n$, $a_i \in {\mathbb{F}_q}^*$, $b \in {\mathbb{F}_q}^*$. We also find explicit formulas for the number of solutions of $a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_s$, where $s < 3$ or $n \leq 5$ and $s \leq 4$.

AMS Subject Classification: 11T06, 11T23
Key Words: finite fields, solutions of equation, quadratic character

1. Introduction

Let p be an odd prime, $q = p^f$, $f \geq 1$, and let $\mathbb{F}_q$ be a finite field of q elements, ${\mathbb{F}_q}^* = \mathbb{F}_q \setminus \{0\}$. In 1954, L. Carlitz [6] proposed the problem of finding the explicit formula for the number of solutions in ${\mathbb{F}_q}^n$ of the equation

$$a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_n, \tag{1}$$

where $a_1, \cdots, a_n, b \in {\mathbb{F}_q}^*$, $n \geq 3$, and ${\mathbb{F}_q}^n = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$. He obtained formulas

Received: November 11, 2008

§Correspondence author

for $n = 3$ and also for $n = 4$ and claimed that it is a difficult problem to find the number of solutions for $n \geq 5$. Recently, I. Baoulina [1] obtained an explicit formula for the number of solutions of equation (1) with some restrictions on n and q. In other words, I. Baoulina partially solved the problem which L. Carlitz proposed as mentioned above. In 2005, I. Baoulina [2] generalized his results in [1]. Based on the results of Sun and Wan [10] and Sun and Yuan [11], he obtained an explicit formula for the number of solutions of equation $a_1x_1^{m_1} + \cdots + a_nx_n^{m_1} = bx_1 \cdots x_n$ in the finite field $\mathbb{F}_q$.

We denote by $N(f(x_1, \cdots, x_n) = b)$ the number of solutions of equation $f(x_1, \cdots, x_n) = b$ in ${\mathbb{F}_q}^n$, where $f(x_1, \cdots, x_n)$ is a polynomial in $\mathbb{F}_q[x_1, \cdots, x_n]$ and $b \in \mathbb{F}_q$. Let g be a fixed primitive element of $\mathbb{F}_q$. Note that by multiplying (1) by a properly chosen element of ${\mathbb{F}_q}^*$ and also by replacing x_i by $\alpha_i x_i$ for a suitable $\alpha_i \in {\mathbb{F}_q}^*$, and permuting the variables, (1) can be reduced to the form

$$x_1^2 + \cdots + x_m^2 + gx_{m+1}^2 + \cdots + gx_n^2 = cx_1 \cdots x_n, \tag{2}$$

where $c \in {\mathbb{F}_q}^*$ and $\frac{n}{2} \leq m \leq n$. Thus, it is sufficient to evaluate the number of solutions of equation (2).

The aim of this paper is to find explicit formulas for $N(a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_s)$ with $n \geq 3$, $s > n$, and $n \geq 3$, $s \leq 2$. We generalize the results of L. Carlitz [6] and give explicit formulas for $N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = bx_1x_2x_3)$, $N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = bx_1x_2x_3)$, and $N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = bx_1x_2x_3x_4)$, where $a_i, b \in {\mathbb{F}_q}^*$.

2. Some Preliminary Lemmas and Known Results

Let η denote the quadratic character on $\mathbb{F}_q$, i.e.,

$$\eta(x) = \begin{cases} 1, & x \text{ is a square,} \\ 0, & x = 0, \\ -1, & \text{non-square.} \end{cases}$$

Let ψ be a nontrivial multiplicative character, ε be the trivial multiplicative character on $\mathbb{F}_q$, and extend ψ to $\mathbb{F}_q$ by setting $\psi(0) = 0$. We define an exponential sum $T(\psi)$ corresponding to character ψ as

$$T(\psi) = \frac{1}{q-1} \sum_{x_1, \cdots, x_n \in \mathbb{F}_q} \psi(x_1^2 + \cdots + x_m^2 + gx_{m+1}^2 + \cdots + gx_n^2)\bar{\psi}(x_1 \cdots x_n).$$

The following lemma is the main result of [1], and fundamental for our question.

Lemma 2.1. *Let* $\gcd(n-2, \frac{q-1}{2}) = d$. *Then*

$$\begin{aligned} & N(x_1^2+\cdots+x_m^2+gx_{m+1}^2+\cdots+gx_n^2=cx_1\cdots x_n) \\ = \; & q^{n-1}+\frac{1}{2}(1+(-1)^n)(-1)^{m+\lfloor\frac{n(q-1)}{4}\rfloor}q^{\frac{n-2}{2}}(q-1) \\ & +(-1)^{m+1}((-1)^{\frac{q-1}{2}}q-1)^{n-m}\sum_{k=0,2|k}^{2m-n}(-1)^{\frac{k(q-1)}{4}}\left(\begin{array}{c}2m-n\\k\end{array}\right)q^{\frac{k}{2}} \\ & +\sum_{\psi^d=\varepsilon,\psi\neq\varepsilon}\bar{\psi}(c)T(\psi), \end{aligned}$$

where $\lfloor\frac{n(q-1)}{4}\rfloor$ *is the greatest integer less or equal to* $\frac{n(q-1)}{4}$, $\left(\begin{array}{c}2m-n\\k\end{array}\right)$ *is the binomial coefficient, and* $\sum_{\psi^d=\varepsilon,\psi\neq\varepsilon}$ *means that the summation is taken over all nontrivial character* ψ *on* $\mathbb{F}_q$ *of order dividing* d.

Proof. See [1, Lemma 1]. □

The following lemma is well known.

Lemma 2.2. *Let* $a_1,\cdots,a_n \in {\mathbb{F}_q}^*$, $b \in \mathbb{F}_q$, *and* $v(b) = -1$ *if* $b \in {\mathbb{F}_q}^*$, *and* $v(0) = q-1$. *Then*

$$N(a_1x_1^2+\cdots+a_nx_n^2=b) \;=\; \begin{cases} q^{n-1}+v(b)\eta((-1)^{\frac{n}{2}}a_1\cdots a_n)q^{\frac{n-2}{2}}, \\ \text{if } n\equiv 0(\text{mod } 2), \\ q^{n-1}+\eta((-1)^{\frac{n-1}{2}}a_1\cdots a_nb)q^{\frac{n-1}{2}}, \\ \text{if } n\equiv 1(\text{mod } 2). \end{cases}$$

Proof. See [5, Theorem 10.5.2]. □

By these lemmas, we have the following simple observations.

Lemma 2.3. *With notations defined as above, we have*

$$\begin{aligned} & N(x_1^2+\cdots+x_m^2+gx_{m+1}^2+\cdots+gx_n^2=0) \\ = \; & q^{n-1}+\frac{1}{2}(1+(-1)^n)(-1)^{m+\lfloor\frac{n(q-1)}{4}\rfloor}q^{\frac{n-2}{2}}(q-1). \end{aligned}$$

Proof. By Lemma 2.2, we know that, if $n \equiv 0(\text{mod } 2)$, then

$$\begin{aligned} & N(x_1^2+\cdots+x_m^2+gx_{m+1}^2+\cdots+gx_n^2=0) \\ = \; & q^{n-1}+\eta((-1)^{\frac{n}{2}}g^{n-m})q^{\frac{n-2}{2}}(q-1) \\ = \; & q^{n-1}+(-1)^{m+\frac{n(q-1)}{4}}q^{\frac{n-2}{2}}(q-1). \end{aligned} \tag{3}$$

If $n \equiv 1(\text{mod } 2)$, then

$$N(x_1^2+\cdots+x_m^2+gx_{m+1}^2+\cdots+gx_n^2=0) = q^{n-1}. \tag{4}$$

Combining (3) with (4) gives the result. □

Lemma 2.4. *If $d = a_1^2 - 4a_0a_2 \neq 0$, then*

$$\sum_{x\in\mathbb{F}_q} \eta(a_2x^2 + a_1x + a_0) = -\eta(a_2).$$

If $d = a_1^2 - 4a_0a_2 = 0$, then

$$\sum_{x\in\mathbb{F}_q} \eta(a_2x^2 + a_1x + a_0) = \eta(a_2)(q-1),$$

where $a_2 \in \mathbb{F}_q{}^*$, $a_1, a_0 \in \mathbb{F}_q$.

Proof. See [9, Theorem 5.48]. □

Remark. By this lemma, we have

$$\sum_{x\in\mathbb{F}_q} \eta(x^2 + a) = -1, \tag{5}$$

for any $a \in \mathbb{F}_q{}^*$.

3. Main Results

With the lemmas in Section 2, we obtain our main results as follows.

Theorem 3.1. *Let $\mathbb{F}_q$ be a finite field of q elements, where $q = p^f$, $f \geq 1$, and p is an odd prime. Then*

$$\begin{aligned}
& N(a_1x_1^2 + \cdots + a_nx_n^2 = cx_1\cdots x_s) \\
= \;& N(x_1^2 + \cdots + x_m^2 + gx_{m+1}^2 + \cdots + gx_n^2 = bx_1\cdots x_s) \\
= \;& q^{s-1} + \frac{1}{2}(1 + (-1)^n)(-1)^{m+\lfloor\frac{n(q-1)}{4}\rfloor}q^{\frac{2s-n-2}{2}}(q-1) \\
& +(-1)^{m+1}(q-1)^{s-n}((-1)^{\frac{q-1}{2}}q-1)^{n-m} \\
& \sum_{k=0,2|k}^{2m-n}(-1)^{\frac{k(q-1)}{4}}\begin{pmatrix} 2m-n \\ k \end{pmatrix}q^{\frac{k}{2}},
\end{aligned}$$

where g is a fixed primitive element of $\mathbb{F}_q$, $\begin{pmatrix} 2m-n \\ k \end{pmatrix}$ is the binomial coefficient, and $\lfloor\frac{n(q-1)}{4}\rfloor$ is the greatest integer less or equal to $\frac{n(q-1)}{4}$, a_i, b, $c \in \mathbb{F}_q{}^*$, $n \geq 3$, $\frac{n}{2} \leq m \leq n$, $s > n$.

Proof. By introduction, we know that the number of solutions of equation

$$a_1x_1^2 + \cdots + a_nx_n^2 = cx_1\cdots x_s, \tag{6}$$

where $a_1, \cdots, a_n, c \in {\mathbb{F}_q}^*$ and $n \geq 3$, $s > n$, is equal to the number of solutions of equation

$$x_1^2 + \cdots + x_m^2 + g x_{m+1}^2 + \cdots + g x_n^2 = b x_1 \cdots x_s, \tag{7}$$

where g is a fixed primitive element of $\mathbb{F}_q$, and $b \in {\mathbb{F}_q}^*$, $\frac{n}{2} \leq m \leq n$. We denote by $N(g, b; n, s)$ the number of solutions of equation (7). If $b = 0$, we denote $N(g, b; n, s)$ simply by $N(g, 0; n)$. As for (7), by Lemma 2.1 we have

$$\begin{aligned} & N(x_1^2 + \cdots + x_m^2 + g x_{m+1}^2 + \cdots + g x_n^2 = b x_1 \cdots x_s) \\ = \;& (q-1)^{s-n-1} \sum_{a \in {\mathbb{F}_q}^*} N(g, a; n, n) + N(x_{n+1} \cdots x_s = 0) N(g, 0; n). \end{aligned}$$

It is obvious that

$$N(x_{n+1} \cdots x_s = 0) = q^{s-n} - (q-1)^{s-n}. \tag{8}$$

Thus, by Lemma 2.1 and Lemma 2.3, we obtain that

$$\begin{aligned} & N(g, b; n, s) \\ = \;& (q-1)^{s-n-1} \sum_{a \in {\mathbb{F}_q}^*} [q^{n-1} + \frac{1}{2}(1 + (-1)^n)(-1)^{m + \lfloor \frac{n(q-1)}{4} \rfloor} q^{\frac{n-2}{2}} (q-1)] \\ & + (q-1)^{s-n-1} \sum_{a \in {\mathbb{F}_q}^*} \left[(-1)^{m+1} ((-1)^{\frac{q-1}{2}} q - 1)^{n-m} \Theta \right] \\ & + (q-1)^{s-n-1} \sum_{a \in {\mathbb{F}_q}^*} \sum_{\psi^d = \varepsilon, \psi \neq \varepsilon} \bar{\psi}(a) T(\psi) \\ & + [q^{s-n} - (q-1)^{s-n}][q^{n-1} + \frac{1}{2}(1 + (-1)^n)(-1)^{m + \lfloor \frac{n(q-1)}{4} \rfloor} q^{\frac{n-2}{2}} (q-1)] \\ = \;& (q-1)^{s-n} [q^{n-1} + \frac{1}{2}(1 + (-1)^n)(-1)^{m + \lfloor \frac{n(q-1)}{4} \rfloor} q^{\frac{n-2}{2}} (q-1)] \\ & + (-1)^{m+1} (q-1)^{s-n} ((-1)^{\frac{q-1}{2}} q - 1)^{n-m} \Theta \\ & + q^{s-1} + \frac{1}{2}(1 + (-1)^n)(-1)^{m + \lfloor \frac{n(q-1)}{4} \rfloor} q^{\frac{2s-n-2}{2}} (q-1) \\ & - (q-1)^{s-n} [q^{n-1} + \frac{1}{2}(1 + (-1)^n)(-1)^{m + \lfloor \frac{n(q-1)}{4} \rfloor} q^{\frac{n-2}{2}} (q-1)] \\ = \;& q^{s-1} + \frac{1}{2}(1 + (-1)^n)(-1)^{m + \lfloor \frac{n(q-1)}{4} \rfloor} q^{\frac{2s-n-2}{2}} (q-1) \\ & + (-1)^{m+1} (q-1)^{s-n} ((-1)^{\frac{q-1}{2}} q - 1)^{n-m} \Theta. \end{aligned}$$

Where $\Theta = \sum_{k=0,2|k}^{2m-n} (-1)^{\frac{k(q-1)}{4}} \begin{pmatrix} 2m-n \\ k \end{pmatrix} q^{\frac{k}{2}}$.

This completes the proof of Theorem 3.1. □

By this theorem, we know that, when $s > n$, $N(a_1x_1^2 + \cdots + a_nx_n^2 = cx_1 \cdots x_s)$ dose not depend on the coefficient c.

We intended to investigate explicit formulas for the number of solutions of equation $a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_s$ initially. For $n = 4$ or $n = 5$, $s = 3$ and $n = 5$, $s = 4$, we can use the method of L. Carlitz [6] and obtain explicit formulas. When $n > 5$, $3 \leq s < n$, it is difficult to give the explicit formula. In what follows, we discuss some special cases.

By permuting the variables, we can obtain that:

Proposition 3.2. *Let $a_1, \cdots, a_n, a \in {\mathbb{F}_q}^*$, and $b = \frac{a}{2}$. Then*

$$\begin{aligned} & N(a_1x_1^2 + \cdots + a_nx_n^2 = ax_1) = N(a_1x_1^2 + \cdots + a_nx_n^2 = 2bx_1) \\ = & \begin{cases} q^{n-1} - \eta((-1)^{\frac{n}{2}}a_1 \cdots a_n)q^{\frac{n-2}{2}}, & \text{if } n \equiv 0 (\text{mod } 2), \\ q^{n-1} + \eta((-1)^{\frac{n-1}{2}}a_2 \cdots a_n)q^{\frac{n-1}{2}}, & \text{if } n \equiv 1 (\text{mod } 2), \end{cases} \end{aligned}$$

and

$$\begin{aligned} & N(a_1x_1^2 + \cdots + a_nx_n^2 = ax_1x_2) = N(a_1x_1^2 + \cdots + a_nx_n^2 = 2bx_1x_2) \\ = & \begin{cases} q^{n-2}, \\ \text{if } a_1a_2 = b^2 \text{ and } n \equiv 0 (\text{mod } 2); \\ q^{n-2} + \eta((-1)^{\frac{n-1}{2}}a_1a_3 \cdots a_n)q^{\frac{n-3}{2}}(q-1), \\ \text{if } a_1a_2 = b^2 \text{ and } n \equiv 1 (\text{mod } 2); \\ q^{n-1} + \eta((-1)^{\frac{n}{2}}(a_1a_2 - b^2)a_3 \cdots a_n)q^{\frac{n-2}{2}}(q-1), \\ \text{if } a_1a_2 \neq b^2 \text{ and } n \equiv 0 (\text{mod } 2); \\ q^{n-1}, \\ \text{if } a_1a_2 \neq b^2 \text{ and } n \equiv 1 (\text{mod } 2). \end{cases} \end{aligned}$$

Using the methods of L. Carlitz [6] and Remark above repeatedly, we can get following propositions. Though the results below are elementary, we have not seen them in literature.

Proposition 3.3.

$$\begin{aligned} & N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = ax_1x_2x_3) \\ = & N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 2bx_1x_2x_3) \\ = & q^3 - q[\eta(-a_1a_4) + \eta(-a_2a_4) + \eta(-a_3a_4) + \eta(a_1a_2a_3a_4)], \end{aligned}$$

where $a_1, a_2, a_3, a_4, a \in {\mathbb{F}_q}^*$ and $b = \frac{a}{2}$.

Proposition 3.4.

$$\begin{aligned} & N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = ax_1x_2x_3) \\ = & N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = 2bx_1x_2x_3) \end{aligned}$$

$$= q^4 + q^2[\eta(a_2a_3a_4a_5) + \eta(a_1a_3a_4a_5) + \eta(a_1a_2a_4a_5)] + q\eta(-a_4a_5),$$

where $a_1, a_2, a_3, a_4, a_5, a \in \mathbb{F}_q{}^*$ *and* $b = \frac{a}{2}$.

Using the similar method, we get the following proposition.

Proposition 3.5. *With notations defined as above, we have*

$$\begin{aligned} & N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = ax_1x_2x_3x_4) \\ = \; & N(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = 2bx_1x_2x_3x_4) \\ = \; & q^4 - q^3 + 2q^2 - q - q(q-1)A_0 + q^2(q-1)\eta(-a_1a_5)A_1, \end{aligned}$$

where

$$A_0 = \eta(-a_1a_5) + \eta(-a_2a_5) - \eta(-a_4a_5) - \eta(a_1a_2a_4a_5)$$
$$A_1 = 1 + \eta(-a_1a_2a_3a_4)$$

if $q \equiv 3 (\mathrm{mod}\ 4)$, *and if* $q \equiv 1 (\mathrm{mod}\ 4)$, *then*

$$A = \sum_{j=0}^{3} \lambda^j(-\frac{a_1a_2a_4}{b^2a_3}),$$

where λ *is the multiplicative character on* $\mathbb{F}_q$ *of order* 4.

4. Concluding Remarks

Generally speaking, it is difficult to find explicit formulas for the number of solutions of some equations over finite fields. In the present paper, the result of Theorem 3.1 is the generalization of I. Baoulina [1]. Using the method of this paper, we can also generalize the result of I. Baoulina [2]. We intended to investigate explicit formulas for the number of solutions of equation $a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_s$ initially. For $n = 4$ or $n = 5$, $s = 3$ and $n = 5$, $s = 4$, we can use the method of L. Carlitz [6] and obtain explicit formulas. When $n > 5$, $3 \leq s < n$, it is difficult to give the explicit formula. However, we can use the results of I. Baoulina [1] to solve the problem partially, we will report the details in another paper.

References

[1] I. Baoulina, On the problem of explicit evaluation of the number of solutions of equation $a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_n$ in a finite field, In: *Current Trends in Number Theory* (Ed-s: S.D. Adhikari, S.A. Katre, B. Ramakrishnan), Hindustan Book Agency, New Delhi (2002), 27-37.

[2] I. Baoulina, On the number of solutions of equation $a_1x_1^{m_1}+\cdots+a_nx_n^{m_n}=bx_1\cdots x_n$ in a finite field, *Acta Appl. Math.*, **89** (2005), 35-39.

[3] I. Baoulina, On some equations over finite fields, *J. Theor. Nombres Bordeaux*, **17** (2005), 45-50.

[4] I. Baoulina, Generalizations of the Markoff-Hurwitz equations over finite fields, *J. Number Theory*, **118** (2006), 31-52.

[5] B.C. Berndt, R.J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, Wiley-Interscience, New York (1998).

[6] L. Carlitz, Certain special equations in a finite field, *Monatsh. Math.*, **58** (1954), 5-12.

[7] L.K. Hua, H.S. Vandiver, Characters over certain types of rings with applications to the theory of equations in a finite field, *Proc. Natl. Acad. Sci.*, **35** (1949), 94-99.

[8] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, GTM84, Springer-Verlag, New York (1990).

[9] R. Lidl, H. Niederreiter, Finite fields, *Encyclopedia of Mathematics and Its Applications*, **20**, Addison-Wesley, Reading, MA (1983).

[10] Sun Qi, Wan Daqing, On the sovability of the equation $\sum_{i=1}^{n}\frac{x_i}{d_i}\equiv 0(\mathrm{mod}\ 1)$ and its application, *Proc. Amer. Math. Soc.*, **100**, No. 2 (1987), 220-224.

[11] Sun Qi, Yuan Pinzhi, On the number of solutions of diagonal equations over a finite field, *Finite Fields and Their Applications*, **2** (1996), 35-41.