JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Ioulia N. BAOULINA

On the Carlitz problem on the number of solutions to some special equations over finite fields

Tome 23, n[o] 1 (2011), p. 1-20.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_1_1_0>

Journal de Théorie des Nombres
de Bordeaux **23** (2011), 1-20

On the Carlitz problem on the number of solutions to some special equations over finite fields

par Ioulia N. BAOULINA

Résumé. On considère une équation de la forme suivante

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

sur le corps fini $\mathbb{F}_q = \mathbb{F}_{p^s}$. Carlitz a obtenu des formules pour le nombre de solutions de cette équation dans le cas $n = 3$ et le cas $n = 4$ avec $q \equiv 3 \pmod 4$. Dans des travaux anciens, on a démontré des formules pour le nombre de solutions lorsque $d = \gcd(n-2, (q-1)/2) = 1$ ou 2 ou 4, et aussi lorsque $d > 1$ et -1 est une puissance de p modulo $2d$. Dans ce papier, on démontre des formules pour le nombre de solutions lorsque $d = 2^t$, $t \geq 3$, $p \equiv 3$ ou $5 \pmod 8$ ou $p \equiv 9 \pmod{16}$. On obtient aussi une borne inférieure pour le nombre de solutions dans le cas général.

Abstract. We consider an equation of the type

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

over the finite field $\mathbb{F}_q = \mathbb{F}_{p^s}$. Carlitz obtained formulas for the number of solutions to this equation when $n = 3$ and when $n = 4$ and $q \equiv 3 \pmod 4$. In our earlier papers, we found formulas for the number of solutions when $d = \gcd(n-2, (q-1)/2) = 1$ or 2 or 4; and when $d > 1$ and -1 is a power of p modulo $2d$. In this paper, we obtain formulas for the number of solutions when $d = 2^t$, $t \geq 3$, $p \equiv 3$ or $5 \pmod 8$ or $p \equiv 9 \pmod{16}$. For general case, we derive lower bounds for the number of solutions.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 2$ with $q = p^s$ elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. By η denote the quadratic character on $\mathbb{F}_q$ ($\eta(x) = +1, -1, 0$ accordingly as x is a square, a nonsquare or zero in $\mathbb{F}_q$). L. Carlitz [7] proposed the problem of finding an explicit formula for the number of solutions in $\mathbb{F}_q^n$ to the equation

$$a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_n, \tag{1.1}$$

where $a_1, \dots, a_n, b \in \mathbb{F}_q^*$ and $n \geq 3$. He proved that (1.1) has

$$q^2 + 1 + [\eta(-a_1a_2) + \eta(-a_1a_3) + \eta(-a_2a_3)]\, q$$

solutions if $n = 3$. Moreover, Carlitz showed that, for $n = 4$, equation (1.1) has

$$q^3 - 1 - [\eta(-a_1a_2) + \eta(-a_1a_3) + \eta(-a_1a_4) + \eta(-a_2a_3) + \eta(-a_2a_4) + \eta(-a_3a_4)]q \\ - \eta(a_1a_2a_3a_4)q + Tq$$

solutions, where $T = 0$ if $q \equiv 3 \pmod 4$, and

$$T = [\eta(a_1) + \eta(a_2) + \eta(a_3) + \eta(a_4)] \sum_{x \in \mathbb{F}_q} \eta\left(x\left(x^2 + \frac{4a_1a_2a_3a_4}{b^2}\right)\right)$$

if $q \equiv 1 \pmod 4$. Combining Carlitz's expression for $n = 4$, $q \equiv 1 \pmod 4$ with the result of Katre and Rajwade [8, Theorem 2] gives the explicit formula for the number of solutions.

For $n = 3$, $a_1 = a_2 = a_3 = 1$, $b = 3$ (so-called Markoff equation) A. Baragar [5] studied a structure of the set of solutions and calculated the zeta-function.

Let g be a generator of the cyclic group $\mathbb{F}_q^*$. Notice that by multiplying (1.1) by properly chosen element of $\mathbb{F}_q^*$ and also by replacing x_i by h_ix_i for a suitable $h_i \in \mathbb{F}_q^*$ and permuting the variables, (1.1) can be reduced to the form

$$x_1^2 + \cdots + x_m^2 + gx_{m+1}^2 + \cdots + gx_n^2 = cx_1 \cdots x_n, \tag{1.2}$$

where $c \in \mathbb{F}_q^*$ and $n/2 \leq m \leq n$. It follows from this that it is sufficient to evaluate the number of solutions to (1.2).

Denote by N_q the number of solutions to (1.2) in $\mathbb{F}_q^n$. In [1], we found formulas for N_q when $\gcd(n-2, (q-1)/2) = 1$ or 2. In another paper [2], we determined N_q when $d = \gcd(n-2, (q-1)/2) > 1$ and -1 is a power of p modulo $2d$. Besides, we considered there the case when n is even, $m = n/2$, $2d \nmid (n-2)$, and -1 is a power of p modulo d. In [3], we obtained formulas for N_q when $\gcd(n-2, (q-1)/2) = 4$.

The aim of this paper is to find certain explicit formulas for N_q when $\gcd(n-2, (q-1)/2) = 2^t$ with $t \geq 3$. Our main results are Theorems 3.1, 3.2, 4.1, 4.2, 5.1 and 5.2, in which we cover the cases $p \equiv 3$ or $5 \pmod 8$ and $p \equiv 9 \pmod{16}$ (Theorems 4.1 and 4.2 include the case $t = 2$). All of the evaluations in Sections 3-5 are effected in terms of parameters occurring in quadratic partitions of some powers of q. Besides, in Section 6 we obtain explicit lower bounds for N_q and show that (1.2) has at least one nontrivial solution except in the case $m = n = q = 3$.

2. Preliminary Lemmas

Let g be a generator of the cyclic group $\mathbb{F}_q^*$. Let $n \geq 3$ and $n/2 \leq m \leq n$. Let ψ be a nontrivial character on $\mathbb{F}_q$. We extend ψ to all of $\mathbb{F}_q$ by setting $\psi(0) = 0$. The sum $T(\psi)$ over $\mathbb{F}_q$ is defined by

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

In the following lemma we express N_q in terms of $T(\psi)$ (for proof, see [1, Lemma 1]).

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

$$\begin{aligned} N_q = & q^{n-1} + \frac{1}{2}[1 + (-1)^n](-1)^{m+\lfloor \frac{n}{2} \rfloor \frac{q-1}{2}} q^{\frac{n-2}{2}}(q-1) \\ & + (-1)^{m+1}[(-1)^{\frac{q-1}{2}} q - 1]^{n-m} \sum_{\substack{k=0 \\ 2|k}}^{2m-n} (-1)^{\frac{k(q-1)}{4}} \binom{2m-n}{k} q^{\frac{k}{2}} \\ & + \sum_{\substack{\psi^d = \varepsilon \\ \psi \neq \varepsilon}} \bar{\psi}(c) T(\psi), \end{aligned}$$

where $\sum_{\psi^d=\varepsilon,\psi\neq\varepsilon}$ *means that the summation is taken over all nontrivial characters* ψ *on* $\mathbb{F}_q$ *of order dividing* d.

Let ψ be a nontrivial character on $\mathbb{F}_q$. The Gauss sum $G(\psi)$ over $\mathbb{F}_q$ is defined by

$$G(\psi) = \sum_{x \in \mathbb{F}_q} \psi(x) e^{2\pi i \frac{\mathrm{Tr}(x)}{p}},$$

where $\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{s-1}}$ is the trace of x from $\mathbb{F}_q$ to $\mathbb{F}_p$.

Lemma 2.2. *For any nontrivial character* ψ *on* $\mathbb{F}_q$,

$$|G(\psi)| = \sqrt{q}.$$

Proof. See [6, Theorem 1.1.4(c)] or [9, Theorem 5.11]. □

The next lemma, which is Lemma 2 of [1], gives a relationship between sum $T(\psi)$ and Gauss sums.

Lemma 2.3. *Let* $\gcd(n-2,(q-1)/2) = d$, $d > 1$. *Let* ψ *be a character of order* δ *on* $\mathbb{F}_q$, *where* $\delta > 1$ *and* $\delta \mid d$. *Let* λ *be a character on* $\mathbb{F}_q$ *chosen so that* $\lambda^2 = \psi$ *and*

$$\mathrm{ord}\lambda = \begin{cases} \delta & \text{if } \delta \text{ is odd,} \\ 2\delta & \text{if } \delta \text{ is even.} \end{cases}$$

Then

$$T(\psi)=\frac{1}{2q}\,\lambda(g^{n-m})G(\psi)\left[\,G(\bar\lambda)^2-G(\bar\lambda\eta)^2\right]^{n-m}$$
$$\times\left[\left[\,G(\bar\lambda)+G(\bar\lambda\eta)\right]^{2m-n}+(-1)^{n+\frac{n-2}{\delta}}\left[\,G(\bar\lambda)-G(\bar\lambda\eta)\right]^{2m-n}\right].$$

Corollary 2.1. *With the notation of Lemma* 2.3*,*

$$|T(\psi)|\le\begin{cases}2^{m-1}q^{\frac{n-1}{2}} & \text{if } 2m\neq n,\\ 2^{\frac{n}{2}}q^{\frac{n-1}{2}} & \text{if } 2m=n.\end{cases}$$

Proof. Appealing to Lemma 2.2, we deduce that

$$\begin{aligned}|T(\psi)|&\le\frac{1}{q}\,|G(\psi)|\cdot(|G(\bar\lambda)|^2+|G(\bar\lambda\eta)|^2)^{n-m}\\&\quad\times\sum_{\substack{k=0\\ k\equiv n+\frac{n-2}{\delta}\ (\mathrm{mod}\ 2)}}^{2m-n}\binom{2m-n}{k}|G(\bar\lambda)|^{2m-n-k}|G(\bar\lambda\eta)|^k\\&=\frac{1}{q}\cdot\sqrt{q}\cdot 2^{n-m}q^{n-m}\cdot q^{m-\frac{n}{2}}\sum_{\substack{k=0\\ k\equiv n+\frac{n-2}{\delta}\ (\mathrm{mod}\ 2)}}^{2m-n}\binom{2m-n}{k}\\&\le\begin{cases}2^{m-1}q^{\frac{n-1}{2}} & \text{if } 2m\neq n,\\ 2^{\frac{n}{2}}q^{\frac{n-1}{2}} & \text{if } 2m=n,\end{cases}\end{aligned}$$

as desired. □

The aim of the remainder of this section is to obtain a modification of the special case $\gcd(n-2,(q-1)/2)=2^t$ of Lemma 2.1, when $p\equiv 2^{h-1}\pm 1\pmod{2^h}$ with $h\ge 3$.

Lemma 2.4. *Let $\delta>1$ be an integer with $2\delta\mid(q-1)$. Then*

$$\sum_{\substack{\psi^\delta=\varepsilon\\ \psi\neq\varepsilon}}\bar\psi(c)T(\psi)=\frac{1}{2}\sum_{\substack{\lambda^{2\delta}=\varepsilon\\ \lambda^2\neq\varepsilon}}\bar\lambda(c^2)T(\lambda^2).$$

Proof. Let χ be a character of order 2δ on $\mathbb{F}_q$. Then χ^2 has order δ. We have

$$\begin{aligned}\sum_{\substack{\lambda^{2\delta}=\varepsilon\\ \lambda^2\neq\varepsilon}}\bar\lambda(c^2)T(\lambda^2)&=\sum_{\substack{j=1\\ j\neq\delta}}^{2\delta-1}\bar\chi^j(c^2)T(\chi^{2j})=\sum_{j=1}^{\delta-1}\left[\bar\chi^j(c^2)T(\chi^{2j})+\bar\chi^{j+\delta}(c^2)T(\chi^{2(j+\delta)})\right]\\&=2\sum_{j=1}^{\delta-1}(\bar\chi^2)^j(c)T((\chi^2)^j)=2\sum_{\substack{\psi^\delta=\varepsilon\\ \psi\neq\varepsilon}}\bar\psi(c)T(\psi),\end{aligned}$$

as desired. □

For $p\equiv 2^{h-1}\pm 1\,(\text{mod }2^h)$, it is convenient to set

$$w=\begin{cases} h+1 & \text{if } p\equiv 2^{h-1}-1 \pmod{2^h},\\ h & \text{if } p\equiv 2^{h-1}+1 \pmod{2^h}.\end{cases}$$

Lemma 2.5. *Let $p\equiv 2^{h-1}\pm 1 \pmod{2^h}$, $h\geq 3$, and λ be a character of order 2^r on $\mathbb{F}_q$, where $r\geq w$. Then $G(\bar\lambda)=G(\bar\lambda\eta)$.*

Proof. See [4, Lemma 2.13]. □

Comparing Lemmas 2.3 and 2.5, we obtain the next result.

Lemma 2.6. *Let $p\equiv 2^{h-1}\pm 1 \pmod{2^h}$, $h\geq 3$, $\gcd(n-2,(q-1)/2)=2^t$, and λ be a character of order 2^r on $\mathbb{F}_q$, where $w\leq r\leq t+1$. Then*

$$T(\lambda^2)=\begin{cases} 2^{n-1}G(\bar\lambda)^nG(\lambda^2)/q & \text{if } m=n,\\ 0 & \text{if } m<n.\end{cases}$$

Finally, Lemmas 2.1, 2.4 and 2.6 imply

Lemma 2.7. *Let $p\equiv 2^{h-1}\pm 1 \pmod{2^h}$, $h\geq 3$, $\gcd(n-2,(q-1)/2)=2^t$, $t\geq w-1$. If $m=n$ then*

$$N_q=q^{n-1}+q^{\frac{n-2}{2}}(q-1)-\sum_{\substack{k=0\\2|k}}^{n}\binom{n}{k}q^{\frac{k}{2}}$$
$$+\sum_{\substack{\psi^{2^{w-2}}=\varepsilon\\ \psi\neq\varepsilon}}\bar\psi(c)T(\psi)+\frac{2^{n-2}}{q}\sum_{r=w}^{t+1}\sum_{\substack{\lambda^{2^r}=\varepsilon\\ \lambda^{2^{r-1}}\neq\varepsilon}}\bar\lambda(c^2)G(\bar\lambda)^nG(\lambda^2).$$

If $m<n$ then

$$N_q=q^{n-1}+(-1)^mq^{\frac{n-2}{2}}(q-1)$$
$$+(-1)^{m+1}(q-1)^{n-m}\sum_{\substack{k=0\\2|k}}^{2m-n}\binom{2m-n}{k}q^{\frac{k}{2}}+\sum_{\substack{\psi^{2^{w-2}}=\varepsilon\\ \psi\neq\varepsilon}}\bar\psi(c)T(\psi).$$

Remark 1. Let a be a nonsquare in $\mathbb{F}_q$. Suppose that $p\equiv 1 \pmod 4$. Then $(a^{\frac{q-1}{4}})^2+1=0$ and the equation $x^2+1=0$ has exactly two roots in $\mathbb{F}_p$. Hence $a^{\frac{q-1}{4}}\in\mathbb{F}_p$. By abuse of notation, let $a^{\frac{q-1}{4}}$ also denote any integer $\equiv a^{\frac{q-1}{4}} \pmod p$. Similarly, if $p\equiv 1$ or $3 \pmod 8$ and s is even, we have $(a^{\frac{q-1}{8}}+a^{\frac{3(q-1)}{8}})^2+2=0$ and the equation $x^2+2=0$ has exactly two roots in $\mathbb{F}_p$. Therefore $a^{\frac{q-1}{8}}+a^{\frac{3(q-1)}{8}}\in\mathbb{F}_p$ and we identify $a^{\frac{q-1}{8}}+a^{\frac{3(q-1)}{8}}$ with any integer $\equiv a^{\frac{q-1}{8}} + a^{\frac{3(q-1)}{8}} \pmod{p}$. This abuse of notation will be kept in the sequel.

Remark 2. In Lemmas 3.3, 4.2 and 5.2 of [4], we evaluated certain sums of the form

$$\frac{1}{q}\sum_{\substack{j=1\\ 2\nmid j}}^{2^r} \psi^j(a)G(\psi^j)^n G(\bar{\psi}^{2j}),$$

where ψ is a character of order 2^r on $\mathbb{F}_q$ and $2^r \mid (n-2)$. It is easy to see that these lemmas and also Lemmas 2.14, 2.15, 2.17 and 2.18 of [4] remain valid with $2^r \mid (n-2)$ replaced by $2^{r-1} \mid (n-2)$ (in Lemma 2.15, the factor $(-1)^j$ will be replaced by $(-1)^{j+\frac{n-2}{2^{k+j}}}$). Furthermore, $2^r \mid (q-1)$ implies that -1 is a 2^{r-1}th power in $\mathbb{F}_q$. Hence, for any positive integer $u \le r$, c^2 is a 2^uth power in $\mathbb{F}_q$ if and only if c is a 2^{u-1}th power in $\mathbb{F}_q$. In view of these observations, in Sections 3-5 we employ the mentioned results for $2^{r-1} \mid (n-2)$ and $a = c^2$ without any additional comments.

3. The Case $p \equiv 3 \pmod 8$

The next lemma is a special case of [3, Lemma 12].

Lemma 3.1. *Let $p \equiv 3 \pmod 8$, $4 \mid s$, $2 \mid n$, and η denote the quadratic character on $\mathbb{F}_q$. Then*

$$T(\eta) = \begin{cases} -2^{n-1}q^{\frac{n-1}{2}} & \text{if } m = n,\\ 0 & \text{if } m < n. \end{cases}$$

Lemma 3.2. *Let $p \equiv 3 \pmod 8$, $8 \mid (n-2)$, and ψ be a character of order 4 on $\mathbb{F}_q$ such that $\psi(g) = i$. Then*

$$\bar{\psi}(c)T(\psi) + \psi(c)T(\bar{\psi}) = 2^{n-\frac{m}{2}+1}M^{n-m}q^{\frac{n-2}{4}}T\sum_{\substack{k=0\\ 2\mid k}}^{m-\frac{n}{2}} \binom{m-\frac{n}{2}}{k} L^{m-\frac{n}{2}-k}q^{\frac{k}{2}},$$

where

$$T = \begin{cases} \sin\frac{\pi m}{4} & \text{if } c \text{ is a 4th power in } \mathbb{F}_q,\\ -\sin\frac{\pi m}{4} & \text{if } c \text{ is a square but not a 4th power in } \mathbb{F}_q,\\ \cos\frac{\pi m}{4} & \text{if } cg \text{ is a 4th power in } \mathbb{F}_q,\\ -\cos\frac{\pi m}{4} & \text{if } cg \text{ is a square but not a 4th power in } \mathbb{F}_q. \end{cases} \tag{3.1}$$

The integers L and $|M|$ are uniquely determined by

$$q = L^2 + 2M^2, \qquad L \equiv -1 \pmod 4, \qquad p \nmid L. \tag{3.2}$$

If $m < n$ then the sign of M is determined by

$$2M \equiv L(g^{\frac{q-1}{8}} + g^{\frac{3(q-1)}{8}}) \pmod p. \tag{3.3}$$

Proof. Since $8 \mid (n-2)$, we have

$$\cos\frac{\pi(n-m)}{4} = \cos\frac{\pi(2-m)}{4} = \sin\frac{\pi m}{4},$$
$$\sin\frac{\pi(n-m)}{4} = \sin\frac{\pi(2-m)}{4} = \cos\frac{\pi m}{4},$$

and the result easily follows from [3, Lemma 18] (see the proof of [3, Theorem 19]). □

Lemmas 2.7, 3.1 and 3.2 enable us to determine N_q when $m < n$.

Theorem 3.1. *Let* $\gcd(n-2,(q-1)/2) = 2^t$, $t \geq 3$, $p \equiv 3 \pmod 8$, *and* $m < n$. *Then*

$$N_q = q^{n-1} + (-1)^m q^{\frac{n-2}{2}}(q-1) + (-1)^{m+1}(q-1)^{n-m} \sum_{\substack{k=0 \\ 2\mid k}}^{2m-n} \binom{2m-n}{k} q^{\frac{k}{2}}$$
$$+ 2^{n-\frac{m}{2}+1} M^{n-m} q^{\frac{n-2}{4}} T \sum_{\substack{k=0 \\ 2\mid k}}^{m-\frac{n}{2}} \binom{m-\frac{n}{2}}{k} L^{m-\frac{n}{2}-k} q^{\frac{k}{2}},$$

where T *is determined by* (3.1) *and the integers* L *and* M *are uniquely determined by* (3.2) *and* (3.3).

Next, we consider the case $m = n$.

Lemma 3.3. *Let* $p \equiv 3 \pmod 8$ *and* ψ *be a character of order* 2^r *on* $\mathbb{F}_q$, *where* $r \geq 4$ *and* $2^{r-1} \mid (n-2)$. *Then*

$$\frac{1}{q}\sum_{\substack{j=1 \\ 2\nmid j}}^{2^r} \psi^j(c^2) G(\psi^j)^n G(\bar{\psi}^{2j}) = 2^{r-1} q^{\frac{(2^{r-2}-1)n-2^{r-2}+2}{2^{r-1}}}$$
$$\times \begin{cases} L_r & \text{if } c \text{ is a } 2^{r-1}\text{th power in } \mathbb{F}_q, \\ -L_r & \text{if } c \text{ is a } 2^{r-2}\text{th power but not a } 2^{r-1}\text{th power in } \mathbb{F}_q, \\ -M_r & \text{if } c \text{ is a } 2^{r-4}\text{th power but not a } 2^{r-3}\text{th power in } \mathbb{F}_q, \\ 0 & \text{otherwise.} \end{cases}$$

The integers L_r *and* $|M_r|$ *are uniquely determined by*

$$q^{\frac{n-2}{2^{r-2}}} = L_r^2 + 2M_r^2, \qquad L_r \equiv -1 \pmod 4, \qquad p \nmid L_r. \tag{3.4}$$

If c *is a* 2^{r-4}*th power but not a* 2^{r-3}*th power in* $\mathbb{F}_q$ *then the sign of* M_r *is determined by*

$$2M_r \equiv L_r\bigl(c^{\frac{q-1}{2^{r-1}}} + c^{\frac{3(q-1)}{2^{r-1}}}\bigr) \pmod p. \tag{3.5}$$

Proof. See [4, Lemma 3.3]. □

Lemmas 2.7, 3.1, 3.2 and 3.3 imply

Theorem 3.2. *Let* $\gcd(n-2,(q-1)/2)=2^t$, $t\ge 3$, $p\equiv 3 \pmod 8$, *and* $m=n$. *If* c *is a* 2^t*th power in* $\mathbb{F}_q$ *then*

$$N_q = q^{n-1}+q^{\frac{n-2}{2}}(q-1)-\sum_{\substack{k=0\\2|k}}^{n}\binom{n}{k}q^{\frac{k}{2}}-2^{n-1}q^{\frac{n-1}{2}}+2^{\frac{n}{2}+1}q^{\frac{n-2}{4}}\sum_{\substack{k=0\\2|k}}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}L^{\frac{n}{2}-k}q^{\frac{k}{2}}$$
$$+\,2^{n-2}\sum_{r=4}^{t+1}2^{r-1}q^{\frac{(2^{r-2}-1)n-2^{r-2}+2}{2^{r-1}}}L_r.$$

If c *is a* 2^{t-1}*th power but not a* 2^t*th power in* $\mathbb{F}_q$ *then*

$$N_q = q^{n-1}+q^{\frac{n-2}{2}}(q-1)-\sum_{\substack{k=0\\2|k}}^{n}\binom{n}{k}q^{\frac{k}{2}}-2^{n-1}q^{\frac{n-1}{2}}+2^{\frac{n}{2}+1}q^{\frac{n-2}{4}}\sum_{\substack{k=0\\2|k}}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}L^{\frac{n}{2}-k}q^{\frac{k}{2}}$$
$$+\,2^{n-2}\sum_{r=4}^{t}2^{r-1}q^{\frac{(2^{r-2}-1)n-2^{r-2}+2}{2^{r-1}}}L_r-2^{n+t-2}q^{\frac{(2^{t-1}-1)n-2^{t-1}+2}{2^t}}L_{t+1}.$$

If $t\ge 4$ *and* c *is a* 2^{t-2}*th power but not a* 2^{t-1}*th power in* $\mathbb{F}_q$ *then*

$$N_q = q^{n-1}+q^{\frac{n-2}{2}}(q-1)-\sum_{\substack{k=0\\2|k}}^{n}\binom{n}{k}q^{\frac{k}{2}}-2^{n-1}q^{\frac{n-1}{2}}+2^{\frac{n}{2}+1}q^{\frac{n-2}{4}}\sum_{\substack{k=0\\2|k}}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}L^{\frac{n}{2}-k}q^{\frac{k}{2}}$$
$$+\,2^{n-2}\sum_{r=4}^{t-1}2^{r-1}q^{\frac{(2^{r-2}-1)n-2^{r-2}+2}{2^{r-1}}}L_r-2^{n+t-3}q^{\frac{(2^{t-2}-1)n-2^{t-2}+2}{2^{t-1}}}L_{t}.$$

If $t\ge 5$ *and* c *is a* 2^v*th power but not a* 2^{v+1}*th power in* $\mathbb{F}_q$, $2\le v\le t-3$, *then*

$$N_q = q^{n-1}+q^{\frac{n-2}{2}}(q-1)-\sum_{\substack{k=0\\2|k}}^{n}\binom{n}{k}q^{\frac{k}{2}}-2^{n-1}q^{\frac{n-1}{2}}+2^{\frac{n}{2}+1}q^{\frac{n-2}{4}}\sum_{\substack{k=0\\2|k}}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}L^{\frac{n}{2}-k}q^{\frac{k}{2}}$$
$$+\,2^{n-2}\sum_{r=4}^{v+1}2^{r-1}q^{\frac{(2^{r-2}-1)n-2^{r-2}+2}{2^{r-1}}}L_r-2^{n+v-1}q^{\frac{(2^{v}-1)n-2^{v}+2}{2^{v+1}}}L_{v+2}$$
$$-\,2^{n+v+1}q^{\frac{(2^{v+2}-1)n-2^{v+2}+2}{2^{v+3}}}M_{v+4}.$$

If c is a square but not a 4th power in $\mathbb{F}_q$ then

$$N_q = q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0\\ 2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} - 2^{n-1}q^{\frac{n-1}{2}} - 2^{\frac{n}{2}+1}q^{\frac{n-2}{4}} \sum_{\substack{k=0\\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} L^{\frac{n}{2}-k} q^{\frac{k}{2}}$$
$$- \begin{cases} 0 & \text{if } t = 3, \\ 2^{n+2} q^{\frac{7n-6}{16}} M_5 & \text{if } t \geq 4. \end{cases}$$

If c is not a square in $\mathbb{F}_q$ then

$$N_q = q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0\\ 2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} + 2^{n-1}q^{\frac{n-1}{2}} - 2^{n+1}q^{\frac{3n-2}{8}} M_4.$$

The integers L, L_r and $|M_r|$ are uniquely determined by (3.2) *and* (3.4), $4 \leq r \leq t+1$. *If c is a 2^{r-4}th power but not a 2^{r-3}th power in $\mathbb{F}_q$, $4 \leq r \leq t+1$, then the sign of M_r is determined by* (3.5).

4. The Case $p \equiv 5 \pmod 8$

The next lemma is the special case $4 \mid (n-2)$ of [3, Lemma 11].

Lemma 4.1. *Let $p \equiv 1 \pmod 4$, $4 \mid (n-2)$, and η denote the quadratic character on $\mathbb{F}_q$. Then*

$$T(\eta) = (-1)^{m+1} 2^{\frac{n}{2}} B^{n-m} q^{\frac{n-2}{4}} \sum_{\substack{k=0\\ 2|k}}^{m-\frac{n}{2}} \binom{m-\frac{n}{2}}{k} A^{m-\frac{n}{2}-k} q^{\frac{k}{2}},$$

where the integers A and B are uniquely determined by

$$q = A^2 + B^2, \qquad A \equiv 1 \pmod 4, \qquad p \nmid A, \tag{4.1}$$

$$B g^{\frac{q-1}{4}} \equiv A \pmod p. \tag{4.2}$$

First, we consider the case $m < n$. Lemmas 2.7 and 4.1 imply

Theorem 4.1. *Let $\gcd(n-2, (q-1)/2) = 2^t$, $t \geq 2$, $p \equiv 5 \pmod 8$, and $m < n$. Then*

$$N_q = q^{n-1} + (-1)^m q^{\frac{n-2}{2}}(q-1) + (-1)^{m+1}(q-1)^{n-m} \sum_{\substack{k=0\\ 2|k}}^{2m-n} \binom{2m-n}{k} q^{\frac{k}{2}}$$
$$+ (-1)^{m+1} 2^{\frac{n}{2}} B^{n-m} q^{\frac{n-2}{4}} \eta(c) \sum_{\substack{k=0\\ 2|k}}^{m-\frac{n}{2}} \binom{m-\frac{n}{2}}{k} A^{m-\frac{n}{2}-k} q^{\frac{k}{2}},$$

where the integers A and B are uniquely determined by (4.1) *and* (4.2).

Next, we consider the case $m=n$.

Lemma 4.2. *Let $p\equiv 5 \pmod 8$ and ψ be a character of order 2^r on $\mathbb{F}_q$, where $r\ge 3$ and $2^{r-1}\mid (n-2)$. Then*

$$\frac{1}{q}\sum_{\substack{j=1\\ 2\nmid j}}^{2^r}\psi^j(c^2)G(\psi^j)^nG(\bar{\psi}^{2j})=(-1)^{\frac{s}{2^{r-2}}}\cdot 2^{r-1}q^{\frac{(2^{r-1}-1)n-2^{r-1}+2}{2^r}}$$
$$\times\begin{cases}-E_r & \text{if } c \text{ is a } 2^{r-1}\text{th power in } \mathbb{F}_q,\\ E_r & \text{if } c \text{ is a } 2^{r-2}\text{th power but not a } 2^{r-1}\text{th power in } \mathbb{F}_q,\\ -F_r & \text{if } c \text{ is a } 2^{r-3}\text{th power but not a } 2^{r-2}\text{th power in } \mathbb{F}_q,\\ 0 & \text{otherwise.}\end{cases}$$

The integers E_r and $|F_r|$ are uniquely determined by

$$q^{\frac{n-2}{2^{r-1}}}=E_r^2+F_r^2,\qquad E_r\equiv 1 \pmod 4,\qquad p\nmid E_r. \tag{4.3}$$

If c is a 2^{r-3}th power but not a 2^{r-2}th power in $\mathbb{F}_q$, then the sign of F_r is determined by

$$F_r c^{\frac{q-1}{2^{r-1}}}\equiv E_r \pmod p. \tag{4.4}$$

Proof. See [4, Lemma 4.2]. □

Lemmas 2.7, 4.1 and 4.2 imply

Theorem 4.2. *Let $\gcd(n-2,(q-1)/2)=2^t$, $t\ge 2$, $p\equiv 5 \pmod 8$, and $m=n$. If c is a 2^tth power in $\mathbb{F}_q$ then*

$$N_q=q^{n-1}+q^{\frac{n-2}{2}}(q-1)-\sum_{\substack{k=0\\ 2\mid k}}^{n}\binom{n}{k}q^{\frac{k}{2}}-2^{\frac{n}{2}}q^{\frac{n-2}{4}}\sum_{\substack{k=0\\ 2\mid k}}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}A^{\frac{n}{2}-k}q^{\frac{k}{2}}$$
$$-2^{n-2}\sum_{r=3}^{t}2^{r-1}q^{\frac{(2^{r-1}-1)n-2^{r-1}+2}{2^r}}E_r-(-1)^{\frac{s}{2^{t-1}}}\cdot 2^{n+t-2}q^{\frac{(2^t-1)n-2^t+2}{2^{t+1}}}E_{t+1}.$$

If c is a 2^{t-1}th power but not a 2^tth power in $\mathbb{F}_q$ then

$$N_q=q^{n-1}+q^{\frac{n-2}{2}}(q-1)-\sum_{\substack{k=0\\ 2\mid k}}^{n}\binom{n}{k}q^{\frac{k}{2}}-2^{\frac{n}{2}}q^{\frac{n-2}{4}}\sum_{\substack{k=0\\ 2\mid k}}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}A^{\frac{n}{2}-k}q^{\frac{k}{2}}$$
$$-2^{n-2}\sum_{r=3}^{t}2^{r-1}q^{\frac{(2^{r-1}-1)n-2^{r-1}+2}{2^r}}E_r+(-1)^{\frac{s}{2^{t-1}}}\cdot 2^{n+t-2}q^{\frac{(2^t-1)n-2^t+2}{2^{t+1}}}E_{t+1}.$$

If $t \geq 3$ and c is a 2^vth power but not a 2^{v+1}th power in $\mathbb{F}_q$, $1 \leq v \leq t-2$, then

$$N_q = q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0\\2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} - 2^{\frac{n}{2}} q^{\frac{n-2}{4}} \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} A^{\frac{n}{2}-k} q^{\frac{k}{2}}$$
$$- 2^{n-2} \sum_{r=3}^{v+1} 2^{r-1} q^{\frac{(2^{r-1}-1)n-2^{r-1}+2}{2^r}} E_r + 2^{n+v-1} q^{\frac{(2^{v+1}-1)n-2^{v+1}+2}{2^{v+2}}} E_{v+2}$$
$$- (-1)^{\frac{s}{2^{v+1}}} \cdot 2^{n+v} q^{\frac{(2^{v+2}-1)n-2^{v+2}+2}{2^{v+3}}} F_{v+3}.$$

If c is not a square in $\mathbb{F}_q$ then

$$N_q = q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0\\2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} + 2^{\frac{n}{2}} q^{\frac{n-2}{4}} \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} A^{\frac{n}{2}-k} q^{\frac{k}{2}}$$
$$- (-1)^{\frac{s}{2}} \cdot 2^n q^{\frac{3n-2}{8}} F_3.$$

The integers A, E_r and $|F_r|$ are uniquely determined by (4.1) and (4.3), $3 \leq r \leq t+1$. If c is a 2^{r-3}th power but not a 2^{r-2}th power in $\mathbb{F}_q$, $3 \leq r \leq t+1$, then the sign of F_r is determined by (4.4).

5. The Case $p \equiv 9 \pmod{16}$

Lemma 5.1. *Let $p \equiv 1 \pmod 8$. Suppose that $2^{r-3} \mid s$ for some positive integer $r \geq 4$. Let A and $|B|$ be uniquely determined by (4.1) and let $|A_0|$ and $|B_0|$ be uniquely determined by $p = A_0^2 + B_0^2$, $2 \mid B_0$. Then $2^{r-1} \mid B$ and*

$$\frac{B}{2^{r-1}} \equiv \frac{B_0 s}{2^{r-1}} \pmod 2.$$

Proof. Since $p \equiv 1 \pmod 8$, we have $4 \mid B_0$. By [8, Proposition 4],

$$B = \pm \sum_{\substack{k=0\\2\nmid k}}^{s} (-1)^{\frac{k-1}{2}} \binom{s}{k} A_0^{s-k} B_0^k.$$

Since $2^{r-3} \mid s$, it is not hard to see that $2^{r-3} \Big| \binom{s}{k}$ for each odd k. Thus,

$$B \equiv \pm A_0^{s-1} B_0 s \pmod{2^r},$$

so that $2^{r-1} \mid B$ and

$$\frac{B}{2^{r-1}} \equiv \pm \frac{A_0^{s-1} B_0 s}{2^{r-1}} \equiv \frac{B_0 s}{2^{r-1}} \pmod 2,$$

as desired. □

Lemma 5.2. *Let $p \equiv 1 \pmod 8$, $8 \mid (n-2)$, $2 \mid s$ and ψ be a character of order 4 on $\mathbb{F}_q$ such that $\psi(g) = i$. Then*

$$\bar{\psi}(c)T(\psi) + \psi(c)T(\bar{\psi}) = 2^{n-\frac{m}{2}+1} M^{n-m} q^{\frac{n-2}{8}} T \sum_{\substack{k=0 \\ 2|k}}^{m-\frac{n}{2}} \binom{m-\frac{n}{2}}{k} L^{m-\frac{n}{2}-k} q^{\frac{k}{2}},$$

where

$$T = \begin{cases} E\sin\frac{\pi m}{4} + F\cos\frac{\pi m}{4} & \text{if } c \text{ is a 4th power in } \mathbb{F}_q, \\ -E\sin\frac{\pi m}{4} - F\cos\frac{\pi m}{4} & \text{if } c \text{ is a square} \\ & \text{but not a 4th power in } \mathbb{F}_q, \\ -F\sin\frac{\pi m}{4} + E\cos\frac{\pi m}{4} & \text{if } cg \text{ is a 4th power in } \mathbb{F}_q, \\ F\sin\frac{\pi m}{4} - E\cos\frac{\pi m}{4} & \text{if } cg \text{ is a square} \\ & \text{but not a 4th power in } \mathbb{F}_q. \end{cases} \tag{5.1}$$

The integers L and $|M|$ are uniquely determined by (3.2). If $m < n$ then the sign of M is determined by (3.3). The integers E and F are uniquely determined by

$$q^{\frac{n-2}{4}} = E^2 + F^2, \quad E \equiv 1 \pmod 4, \quad p \nmid E, \tag{5.2}$$

$$Fg^{\frac{q-1}{4}} \equiv E \pmod p. \tag{5.3}$$

Proof. Let A and B be determined by (4.1) and (4.2). Lemma 5.1 implies that $8 \mid B$. In view of Lemma 21 of [3] and the remarks at the beginning of the proof of Lemma 3.2, we conclude that (see the proof of Theorem 22 of [3])

$$\bar{\psi}(c)T(\psi) + \psi(c)T(\bar{\psi}) = 2^{n-\frac{m}{2}+1} M^{n-m} q^{\frac{n-2}{8}} T \sum_{\substack{k=0 \\ 2|k}}^{m-\frac{n}{2}} \binom{m-\frac{n}{2}}{k} L^{m-\frac{n}{2}-k} q^{\frac{k}{2}},$$

where T is determined by (5.1),

$$E = \sum_{\substack{k=0 \\ 2|k}}^{\frac{n-2}{4}} (-1)^{\frac{k}{2}} \binom{\frac{n-2}{4}}{k} A^{\frac{n-2}{4}-k} B^k, \qquad F = \sum_{\substack{k=0 \\ 2\nmid k}}^{\frac{n-2}{4}} (-1)^{\frac{k-1}{2}} \binom{\frac{n-2}{4}}{k} A^{\frac{n-2}{4}-k} B^k.$$

Since $q = |A+Bi|^2$, we have $q^{\frac{n-2}{4}} = |E+Fi|^2 = E^2 + F^2$. Further, since $A \equiv 1 \pmod 4$ and $2 \mid B$, we deduce that $E \equiv A^{\frac{n-2}{4}} \equiv 1 \pmod 4$. Also, $B^2 \equiv -A^2 \pmod p$ implies $E \equiv 2^{\frac{n-2}{4}-1} A^{\frac{n-2}{4}} \pmod p$, and so $p \nmid E$. Finally,

$$
\begin{aligned}
Fg^{\frac{q-1}{4}} &\equiv Bg^{\frac{q-1}{4}} \sum_{\substack{k=0\\ 2\nmid k}}^{\frac{n-2}{4}} (-1)^{\frac{k-1}{2}} \binom{\frac{n-2}{4}}{k} A^{\frac{n-2}{4}-k} \cdot (-1)^{\frac{k-1}{2}} A^{k-1} \\
&\equiv 2^{\frac{n-2}{4}-1} A^{\frac{n-2}{4}} \equiv E \pmod{p}.
\end{aligned}
$$

This completes the proof. □

Lemmas 2.7, 4.1 and 5.2 allow us to give the explicit formula for N_q when $m < n$.

Theorem 5.1. *Let* $\gcd(n-2, (q-1)/2) = 2^t$, $t \geq 3$, $p \equiv 9 \pmod{16}$, *and* $m < n$. *Then*

$$
\begin{aligned}
N_q = {}& q^{n-1} + (-1)^m q^{\frac{n-2}{2}}(q-1) + (-1)^{m+1}(q-1)^{n-m} \sum_{\substack{k=0\\ 2\mid k}}^{2m-n} \binom{2m-n}{k} q^{\frac{k}{2}} \\
&+ (-1)^{m+1} 2^{\frac{n}{2}} B^{n-m} q^{\frac{n-2}{4}} \eta(c) \sum_{\substack{k=0\\ 2\mid k}}^{m-\frac{n}{2}} \binom{m-\frac{n}{2}}{k} A^{m-\frac{n}{2}-k} q^{\frac{k}{2}} \\
&+ 2^{n-\frac{m}{2}+1} M^{n-m} q^{\frac{n-2}{8}} T \sum_{\substack{k=0\\ 2\mid k}}^{m-\frac{n}{2}} \binom{m-\frac{n}{2}}{k} L^{m-\frac{n}{2}-k} q^{\frac{k}{2}},
\end{aligned}
$$

where T *is determined by* (5.1). *The integers* A, B, E, F, L *and* M *are uniquely determined by* (3.2), (3.3), (4.1), (4.2), (5.2) *and* (5.3).

Next, we consider the case $m = n$.

Lemma 5.3. *Let* $p \equiv 9 \pmod{16}$ *and* ψ *be a character of order* 2^r *on* $\mathbb{F}_q$, *where* $r \geq 4$ *and* $2^{r-1} \mid (n-2)$. *Then*

$$
\begin{aligned}
\frac{1}{q} \sum_{\substack{j=1\\ 2\nmid j}}^{2^r} \psi^j(c^2) G(\psi^j)^n G(\bar{\psi}^{2j}) &= (-1)^{\frac{B}{2^{r-1}}} \cdot 2^{r-1} q^{\frac{(2^{r-1}-3)n-2^{r-1}+6}{2^r}} \\
&\times \begin{cases} E_r L_r & \text{if } c \text{ is a } 2^{r-1}\text{th power in } \mathbb{F}_q, \\ -E_r L_r & \text{if } c \text{ is a } 2^{r-2}\text{th power but not a } 2^{r-1}\text{th power in } \mathbb{F}_q, \\ F_r L_r & \text{if } c \text{ is a } 2^{r-3}\text{th power but not a } 2^{r-2}\text{th power in } \mathbb{F}_q, \\ (F_r - E_r) M_r & \text{if } c \text{ is a } 2^{r-4}\text{th power but not a } 2^{r-3}\text{th power in } \mathbb{F}_q, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}
$$

The integer $|B|$ *is uniquely determined by* (4.1). *The integers* E_r *and* $|F_r|$ *are uniquely determined by* (4.3). *If* c *is a* 2^{r-4}*th power but not a* 2^{r-2}*th* *power in* $\mathbb{F}_q$ *then the sign of* F_r *is determined by*

$$E_r \equiv \begin{cases} F_r c^{\frac{q-1}{2^{r-1}}} \pmod{p} & \text{if } c \text{ is a } 2^{r-3}\text{th power} \\ & \text{but not a } 2^{r-2}\text{th power in } \mathbb{F}_q, \\ F_r c^{\frac{q-1}{2^{r-2}}} \pmod{p} & \text{if } c \text{ is a } 2^{r-4}\text{th power} \\ & \text{but not a } 2^{r-3}\text{th power in } \mathbb{F}_q. \end{cases} \tag{5.4}$$

The integers L_r *and* $|M_r|$ *are uniquely determined by* (3.4). *If* c *is a* 2^{r-4}*th power but not a* 2^{r-3}*th power in* $\mathbb{F}_q$ *then the sign of* M_r *is determined by* (3.5).

Proof. We define the integers $|A_0|$ and $|B_0|$ by the conditions $p = A_0^2 + B_0^2$, $2 \mid B_0$. By Lemma 5.1, $B/2^{r-1}$ and $B_0 s/2^{r-1}$ have the same parity. Hence $(-1)^{B/2^{r-1}} = (-1)^{B_0 s/2^{r-1}}$, and the result follows from [4, Lemma 5.2]. $\square$

Lemmas 2.7, 4.1, 5.2 and 5.3 imply

Theorem 5.2. *Let* $\gcd(n-2,(q-1)/2) = 2^t$, $t \geq 3$, $p \equiv 9 \pmod{16}$, *and* $m = n$. *If* c *is a* 2^t*th power in* $\mathbb{F}_q$ *then*

$$\begin{aligned} N_q = {} & q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0 \\ 2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} - 2^{\frac{n}{2}} q^{\frac{n-2}{4}} \sum_{\substack{k=0 \\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} A^{\frac{n}{2}-k} q^{\frac{k}{2}} \\ & + 2^{\frac{n}{2}+1} q^{\frac{n-2}{8}} E \sum_{\substack{k=0 \\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} L^{\frac{n}{2}-k} q^{\frac{k}{2}} + 2^{n-2} \sum_{r=4}^{t} 2^{r-1} q^{\frac{(2^{r-1}-3)n-2^{r-1}+6}{2^r}} E_r L_r \\ & + (-1)^{\frac{B}{2^t}} \cdot 2^{n+t-2} q^{\frac{(2^t-3)n-2^t+6}{2^{t+1}}} E_{t+1} L_{t+1}. \end{aligned}$$

If c *is a* 2^{t-1}*th power but not a* 2^t*th power in* $\mathbb{F}_q$ *then*

$$\begin{aligned} N_q = {} & q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0 \\ 2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} - 2^{\frac{n}{2}} q^{\frac{n-2}{4}} \sum_{\substack{k=0 \\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} A^{\frac{n}{2}-k} q^{\frac{k}{2}} \\ & + 2^{\frac{n}{2}+1} q^{\frac{n-2}{8}} E \sum_{\substack{k=0 \\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} L^{\frac{n}{2}-k} q^{\frac{k}{2}} + 2^{n-2} \sum_{r=4}^{t} 2^{r-1} q^{\frac{(2^{r-1}-3)n-2^{r-1}+6}{2^r}} E_r L_r \\ & - (-1)^{\frac{B}{2^t}} \cdot 2^{n+t-2} q^{\frac{(2^t-3)n-2^t+6}{2^{t+1}}} E_{t+1} L_{t+1}. \end{aligned}$$

If $t \geq 4$ and c is a 2^{t-2}th power but not a 2^{t-1}th power in $\mathbb{F}_q$ then

$$
\begin{aligned}
N_q = {} & q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0\\2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} - 2^{\frac{n}{2}} q^{\frac{n-2}{4}} \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} A^{\frac{n}{2}-k} q^{\frac{k}{2}} \\
& + 2^{\frac{n}{2}+1} q^{\frac{n-2}{8}} E \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} L^{\frac{n}{2}-k} q^{\frac{k}{2}} + 2^{n-2} \sum_{r=4}^{t-1} 2^{r-1} q^{\frac{(2^{r-1}-3)n-2^{r-1}+6}{2^r}} E_r L_r \\
& - 2^{n+t-3} q^{\frac{(2^{t-1}-3)n-2^{t-1}+6}{2^t}} E_t L_t + (-1)^{\frac{B}{2^t}} \cdot 2^{n+t-2} q^{\frac{(2^t-3)n-2^t+6}{2^{t+1}}} F_{t+1} L_{t+1}.
\end{aligned}
$$

If $t \geq 5$ and c is a 2^vth power but not a 2^{v+1}th power in $\mathbb{F}_q$, $2 \leq v \leq t-3$, then

$$
\begin{aligned}
N_q = {} & q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0\\2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} - 2^{\frac{n}{2}} q^{\frac{n-2}{4}} \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} A^{\frac{n}{2}-k} q^{\frac{k}{2}} \\
& + 2^{\frac{n}{2}+1} q^{\frac{n-2}{8}} E \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} L^{\frac{n}{2}-k} q^{\frac{k}{2}} + 2^{n-2} \sum_{r=4}^{v+1} 2^{r-1} q^{\frac{(2^{r-1}-3)n-2^{r-1}+6}{2^r}} E_r L_r \\
& - 2^{n+v-1} q^{\frac{(2^{v+1}-3)n-2^{v+1}+6}{2^{v+2}}} E_{v+2} L_{v+2} + 2^{n+v} q^{\frac{(2^{v+2}-3)n-2^{v+2}+6}{2^{v+3}}} F_{v+3} L_{v+3} \\
& + (-1)^{\frac{B}{2^{v+3}}} \cdot 2^{n+v+1} q^{\frac{(2^{v+3}-3)n-2^{v+3}+6}{2^{v+4}}} (F_{v+4} - E_{v+4}) M_{v+4}.
\end{aligned}
$$

If c is a square but not a 4th power in $\mathbb{F}_q$ then

$$
\begin{aligned}
N_q = {} & q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0\\2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} - 2^{\frac{n}{2}} q^{\frac{n-2}{4}} \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} A^{\frac{n}{2}-k} q^{\frac{k}{2}} \\
& - 2^{\frac{n}{2}+1} q^{\frac{n-2}{8}} E \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} L^{\frac{n}{2}-k} q^{\frac{k}{2}} + (-1)^{\frac{B}{8}} 2^{n+1} q^{\frac{5n-2}{16}} F_4 L_4 \\
& + \begin{cases} 0 & \text{if } t = 3, \\ (-1)^{\frac{B}{16}} \cdot 2^{n+2} q^{\frac{13n-10}{32}} (F_5 - E_5) M_5 & \text{if } t \geq 4. \end{cases}
\end{aligned}
$$

If c is not a square in $\mathbb{F}_q$ then

$$N_q = q^{n-1} + q^{\frac{n-2}{2}}(q-1) - \sum_{\substack{k=0\\2|k}}^{n} \binom{n}{k} q^{\frac{k}{2}} + 2^{\frac{n}{2}} q^{\frac{n-2}{4}} \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} A^{\frac{n}{2}-k} q^{\frac{k}{2}}$$
$$+ 2^{\frac{n}{2}+1} q^{\frac{n-2}{8}} F \sum_{\substack{k=0\\2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} L^{\frac{n}{2}-k} q^{\frac{k}{2}} + (-1)^{\frac{B}{8}} \cdot 2^{n+1} q^{\frac{5n-2}{16}} (F_4 - E_4) M_4.$$

The integers A, $|B|$, E, $|F|$, E_r, $|F_r|$, L, L_r and $|M_r|$ are uniquely determined by (3.2), (3.4), (4.1), (4.3) *and* (5.2), $4 \le r \le t+1$. *If c is a 2^{r-4}th power but not a 2^{r-2}th power in $\mathbb{F}_q$, $4 \le r \le t+1$, then the sign of F_r is determined by* (5.4). *If c is a 2^{r-4}th power but not a 2^{r-3}th power in $\mathbb{F}_q$, $4 \le r \le t+1$, then the sign of M_r is determined by* (3.5). *If c is not a square in $\mathbb{F}_q$ then the sign of F is determined by*

$$F c^{\frac{q-1}{4}} \equiv E \pmod{p}.$$

6. Lower bounds for the number of solutions

The following result is a straightforward consequence of Lemma 2.1 and Corollary 2.1.

Theorem 6.1. *Let* $\gcd(n-2, (q-1)/2) = d$. *Then*

$$N_q \ge q^{n-1} + \frac{1}{2}[1+(-1)^n](-1)^{m+\lfloor \frac{n}{2} \rfloor \frac{q-1}{2}} q^{\frac{n-2}{2}}(q-1)$$
$$+ (-1)^{m+1}[(-1)^{\frac{q-1}{2}} q - 1]^{n-m} \sum_{\substack{k=0\\2|k}}^{2m-n} (-1)^{\frac{k(q-1)}{4}} \binom{2m-n}{k} q^{\frac{k}{2}}$$
$$- \begin{cases} 2^{m-1}(d-1) q^{\frac{n-1}{2}} & \textit{if } 2m \ne n, \\ 2^{\frac{n}{2}}(d-1) q^{\frac{n-1}{2}} & \textit{if } 2m = n. \end{cases}$$

We can simplify this inequality and obtain a compact expression for lower bound.

Theorem 6.2. *Let* $\gcd(n-2, (q-1)/2) = d$. *Then*

$$N_q \ge \begin{cases} q^{n-1} - 2^{m-1} d q^{\frac{n-1}{2}} + q^{\lfloor \frac{n-1}{2} \rfloor} + (-1)^{n-1} & \textit{if } 2m \ne n, \\ q^{n-1} - 2^{\frac{n}{2}} d q^{\frac{n-1}{2}} + q^{\frac{n-2}{2}} - 1 & \textit{if } 2m = n. \end{cases}$$

Proof. We have

$$
\begin{aligned}
&(-1)^{m+1}[(-1)^{\frac{q-1}{2}}q-1]^{n-m}\sum_{\substack{k=0\\2|k}}^{2m-n}(-1)^{\frac{k(q-1)}{4}}\binom{2m-n}{k}q^{\frac{k}{2}}\\
&=\frac{1}{2}\,[\,1+(-1)^n](-1)^{m+1+\lfloor\frac{n}{2}\rfloor\frac{q-1}{2}}q^{\frac{n}{2}}+(-1)^{n-1}\\
&\quad+(-1)^{n-1}\sum_{\substack{0\le j\le n-m\\0\le k\le 2m-n\\2|k\\(j,k)\ne(0,0),(n-m,2m-n)}}(-1)^{j+\left(j+\frac{k}{2}\right)\frac{q-1}{2}}\binom{n-m}{j}\binom{2m-n}{k}q^{j+\frac{k}{2}}\\
&\ge\frac{1}{2}\,[\,1+(-1)^n](-1)^{m+1+\lfloor\frac{n}{2}\rfloor\frac{q-1}{2}}q^{\frac{n}{2}}+(-1)^{n-1}\\
&\quad-q^{\lfloor\frac{n-1}{2}\rfloor}\sum_{\substack{0\le j\le n-m\\0\le k\le 2m-n\\2|k\\(j,k)\ne(0,0),(n-m,2m-n)}}\binom{n-m}{j}\binom{2m-n}{k}\\
&\ge\frac{1}{2}\,[1+(-1)^n](-1)^{m+1+\lfloor\frac{n}{2}\rfloor\frac{q-1}{2}}q^{\frac{n}{2}}+(-1)^{n-1}+q^{\lfloor\frac{n-1}{2}\rfloor}+\frac{1}{2}\,[1+(-1)^n]q^{\frac{n-2}{2}}\\
&\quad-q^{\frac{n-1}{2}}\cdot\begin{cases}2^{m-1} & \text{if } 2m\ne n,\\ 2^{\frac{n}{2}} & \text{if } 2m=n,\end{cases}
\end{aligned}
$$

and the result follows from Theorem 6.1. □

Corollary 6.1. *Let* $\gcd(n-2,(q-1)/2)=d$. *Then*

$$N_q>\begin{cases}q^{n-1}-2^{n-2}dq^{\frac{n-1}{2}}+1 & \textit{if } m<n,\\ q^{n-1}-2^{n-1}dq^{\frac{n-1}{2}}+1 & \textit{if } m=n.\end{cases}$$

Remark 3. In the case $p\equiv 2^{h-1}\pm 1 \pmod{2^h}$, $h\ge 3$, $\gcd(n-2,(q-1)/2)=2^t$, $t\ge w-1$, $m<n$, if instead of Lemma 2.1 one uses Lemma 2.7, then one obtains lower bounds for N_q, given in Theorem 6.1, Theorem 6.2 and Corollary 6.1, with d replaced by 2^{w-2}.

Note that equation (1.2) always has the trivial solution $(0,\dots,0)$. The estimates in Corollary 6.1 can be employed to establish the existence of nontrivial solutions to (1.2).

Theorem 6.3. *Equation* (1.2) *always has a nontrivial solution unless* $m=n=q=3$.

Proof. First, suppose that $q=3$. Then $d=1$ and

$$\begin{aligned}\sum_{\substack{k=0\\2|k}}^{2m-n}(-1)^{\frac{k(q-1)}{4}}\binom{2m-n}{k}q^{\frac{k}{2}}&=\sum_{\substack{k=0\\2|k}}^{2m-n}\binom{2m-n}{k}(i\sqrt{q})^k\\&=(-1)^n\cdot 2^{2m-n-1}\left[\left(\frac{-1+i\sqrt{3}}{2}\right)^{2m-n}+\left(\frac{-1-i\sqrt{3}}{2}\right)^{2m-n}\right]\\&=\begin{cases}(-1)^n\cdot 2^{2m-n} & \text{if } 3\mid(2m-n),\\(-1)^{n-1}\cdot 2^{2m-n-1} & \text{if } 3\nmid(2m-n).\end{cases}\end{aligned}$$

Appealing to Lemma 2.1, we find that

$$N_q=\begin{cases}3^{n-1}-2^n+(-1)^{m+\frac{n}{2}}\cdot 2\cdot 3^{\frac{n-2}{2}} & \text{if } 2\mid n \text{ and } 3\mid(2m-n),\\3^{n-1}+2^{n-1}+(-1)^{m+\frac{n}{2}}\cdot 2\cdot 3^{\frac{n-2}{2}} & \text{if } 2\mid n \text{ and } 3\nmid(2m-n),\\3^{n-1}-2^n & \text{if } 2\nmid n \text{ and } 3\mid(2m-n),\\3^{n-1}+2^{n-1} & \text{if } 2\nmid n \text{ and } 3\nmid(2m-n).\end{cases}$$

Since $3^{n-1}-2^n>2^{n-1}+1$ for each $n\geq 4$, we see that $N_q=1$ if and only if $m=n=3$.

Next, suppose that $q\geq 5$. If $m<n$ then, by Corollary 6.1,

$$N_q>2^{n-1}q^{\frac{n-1}{2}}\left(\left(\frac{q}{4}\right)^{\frac{n-1}{2}}-\frac{d}{2}\right)+1>2^{n-1}q^{\frac{n-1}{2}}\left(\left(\frac{q}{4}\right)^{\frac{n-1}{2}}-\frac{q}{4}\right)+1\geq 1.$$

Now assume that $m=n$. Note that, by Corollary 6.1, the inequality $(q/4)^{\frac{n-1}{2}}\geq d$ implies $N_q>1$. Since

$$\begin{aligned}\left(\frac{q}{4}\right)^{\frac{n-1}{2}}&=\left(1+\frac{q-4}{4}\right)^{\frac{n-1}{2}}\geq 1+\frac{n-1}{2}\cdot\frac{q-4}{4}\\&\geq\begin{cases}n>d & \text{if } q\geq 13 \text{ and } n\geq 3,\\q-3\geq\dfrac{q-1}{2}\geq d & \text{if } q\geq 5 \text{ and } n\geq 9,\end{cases}\end{aligned}$$

it remains to examine the case when $q\in\{5,7,9,11\}$ and $n\in\{3,4,5,6,7,8\}$. Direct calculations show that the inequality $(q/4)^{\frac{n-1}{2}}\geq d$ holds except when $q=5$, $n=4$ or 6. Finally, we observe that for any $c\in\mathbb{F}_5^*$ the equation $x_1^2+x_2^2+x_3^2+x_4^2=cx_1x_2x_3x_4$ has the nontrivial solution (0,0,1,2) and the equation $x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2=cx_1x_2x_3x_4x_5x_6$ has the nontrivial solution (0,0,0,0,1,2). This completes the proof. $\square$

Remark 4. Theorem 6.3 can also be proved without using the low bounds for N_q. Indeed,

$$\begin{aligned} N_q &\geq \#\{(x_2,\ldots,x_n)\in\mathbb{F}_q^{n-1} \mid x_2^2+\cdots+x_m^2+gx_{m+1}^2+\cdots+gx_n^2=0\} \\ &= \begin{cases} q^{n-2} & \text{if } n \text{ is even,} \\ q^{n-2}+\eta((-1)^{\frac{n-1}{2}}g^{n-m})q^{\frac{n-3}{2}}(q-1) & \text{if } n \text{ is odd,} \end{cases} \\ &\geq q^{\frac{n-3}{2}}(q^{\frac{n-1}{2}}-q+1), \end{aligned}$$

where, in the penultimate step, we used the explicit formulas for the number of solutions to quadratic equations (see [6, Theorem 10.5.1] or [9, Theorems 6.26 and 6.27]). Hence $N_q > 1$ except possibly for $n=3$. From Lemma 2.1, we deduce for $n=3$ that

$$N_q = \begin{cases} q^2+1-(-1)^{\frac{q-1}{2}}q & \text{if } m=2, \\ q^2+1+(-1)^{\frac{q-1}{2}}3q & \text{if } m=3. \end{cases}$$

Thus $N_q=1$ if and only if $m=n=q=3$. Note that for $n>3$ we actually proved that (1.2) always has a nontrivial solution with $x_1\cdots x_n=0$.

In view of Remark 4, it is of interest to give conditions for the existence of a solution with $x_1\cdots x_n\neq 0$. Let N_q^* be the number of solutions to equation (1.2) in $(\mathbb{F}_q^*)^n$. From the proof of [1, Lemma 1],

$$\begin{aligned} N_q^* = {} & \frac{(q-1)^n}{q} + \frac{(-1)^{m+1}[(-1)^{\frac{q-1}{2}}q-1]^{n-m}}{q} \sum_{\substack{k=0 \\ 2|k}}^{2m-n} (-1)^{\frac{k(q-1)}{4}} \binom{2m-n}{k} q^{\frac{k}{2}} \\ & + \sum_{\substack{\psi^d=\varepsilon \\ \psi\neq\varepsilon}} \bar{\psi}(c)T(\psi). \end{aligned}$$

Proceeding then by the same arguments as in the proofs of Theorems 6.2 and 6.3, we find that

$$N_q^* = \begin{cases} 0 & \text{if } q=3 \text{ and } 3 \mid (2m-n), \\ 2^{n-1} & \text{if } q=3 \text{ and } 3 \nmid (2m-n), \end{cases}$$

and

$$N_q^* > \frac{(q-1)^n}{q} - \begin{cases} 2^{n-2}dq^{\frac{n-1}{2}} & \text{if } m<n, \\ 2^{n-1}dq^{\frac{n-1}{2}} & \text{if } m=n, \end{cases}$$

and obtain the next result.

Theorem 6.4. *Equation* (1.2) *is always solvable with* $x_1\cdots x_n\neq 0$ *except in the following cases:*
(a) $q=3$ *and* $3\mid(2m-n)$;
(b) $q=5$, $m=n=4$ *and* c *is a nonsquare in* $\mathbb{F}_q$.

7. Acknowledgments

It is my pleasure to thank Professor B. Sury for his kind invitation and hospitality at the Bangalore Centre of the Indian Statistical Institute during December 2009, when this paper was finalized. I would like to thank Professor R. Balasubramanian for his interest and very helpful discussions. I thank Yashonidhi Pandey for translating the abstract into French. I thank the referee for useful suggestions which improved the quality of this paper.

References

[1] I. Baoulina, *On the problem of explicit evaluation of the number of solutions of the 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, Edited by S. D. Adhikari, S. A. Katre and B. Ramakrishnan, Hindustan Book Agency, New Delhi, 2002, 27–37.

[2] I. Baoulina, *On some equations over finite fields.* J. Théor. Nombres Bordeaux **17** (2005), 45–50.

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

[4] I. Baoulina, *On the number of solutions to the equation* $(x_1+\cdots+x_n)^2=ax_1\cdots x_n$ *in a finite field.* Int. J. Number Theory **4** (2008), 797–817.

[5] A. Baragar, *The Markoff Equation and Equations of Hurwitz.* Ph. D. Thesis, Brown University, 1991.

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

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

[8] S. A. Katre and A. R. Rajwade, *Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order* 4 *and the corresponding Jacobsthal sum.* Math. Scand. **60** (1987), 52–62.

[9] R. Lidl and H. Niederreiter, *Finite Fields.* Cambridge Univ. Press, Cambridge, 1997.

Ioulia N. Baoulina
Statistics and Mathematics Unit
Indian Statistical Institute
8th Mile, Mysore Road
R. V. College Post
Bangalore 560059, India
E-mail: jbaulina@mail.ru