The Number of Solutions of Certain Equations over Finite Fields

HU Shuangnian¹, LIU Jianghan², QIN Zhentao³

¹. School of Mathematics and Statistics, Nanyang Institute of Technology, Nanyang 473004, Henan, China;
². College of Computer and Information Science, Southwest University, Chongqing 400715, China;
³. School of Mathematics and Computer, Panzhihua University, Panzhihua 617000, Sichuan, China

© Wuhan University 2022

Abstract: Let $s$ be a positive integer, $p$ be an odd prime, $q^s = p^t$, and let $F_q$ be a finite field of $q$ elements. Let $N_q(f)$ be the number of solutions of the following equations: $12(\ldots) = 0$ over the finite field $F_q$, with $2, n \geq t$, $k, j \geq 1$, $m_i(1 \leq i \leq n)$ are positive integers. In this paper, we find formulas for $N_q(f)$ when there is a positive integer $l$ such that $dD(\ldots)$, where $D = \text{lcm} \quad [d, \ldots, d]$, $d = \text{gcd}(\sum M, m, kM, (q-1)/D), M = \text{lcm} \quad [m, \ldots, m], d_i = \text{gcd}(m_i, q-1), 1 \leq i \leq n$. And we determine $N_q(f)$ explicitly under certain cases. This extends Markoff-Hurwitz-type equations over finite field.

Key words: finite field; rational point; diagonal equation; Markoff-Hurwitz-type equations

0 Introduction

Let $p$ be an odd prime. Let $F_q$ be a finite field of $q$ elements with $q = p^s$, $s \geq 1$ and $F_q^*$ denote the set of all the nonzero elements of $F_q$. Let $N(f = b)$ denote the number of solutions of the equation $f(x_1, x_2, \ldots, x_n) = b$ in $F_q^* = F_q \times \cdots \times F_q^*$, where $f(x_1, x_2, \ldots, x_n)$ is a polynomial in $F_q[x_1, \ldots, x_n]$ and $b \in F_q$. That is,

$N(f = b) = \# \{(x_1, x_2, \ldots, x_n) \in F_q^* \mid f(x_1, x_2, \ldots, x_n) = 0\}$

Studying the value of $N(f = b)$ is one of the main topics in finite fields. Generally speaking, it is nontrivial to give the formula for $N(f = b)$. Finding the explicit formula for $N(f = b)$ under certain condition has attracted lots of authors for many years.

Markoff-Hurwitz-type equations belong to the following type of the Diophantine equations

$x_1^2 + x_2^2 + \cdots + x_n^2 = ax_1x_2 \cdots x_n$

where $n$, $a$ are positive integers and $n \geq 3$. This type of equations was first studied by Markoff for the case $n = 3, a = 3$. More generally, these equations were studied by Hurwitz.

Recently, Baoulina [3-5] studied the generalized Markoff-Hurwitz-type equations

$a_1x_1^m + a_2x_2^m + \cdots + a_nx_n^m = ax_1x_2 \cdots x_n$

where $a_i, a \in F_q^*$ and $m_i$ are positive integers satisfying $m_i|(q-1)$ for $i = 1, \ldots, n$ and $n \geq 2$. Baoulina [4-6] and Pan et al [7] considered the further generalized Markoff-Hurwitz-type equations of the form:
where  \( n \geq 2 \),  \( m, k, l \) are positive integers. In what follows, we always let  \( d \in F_q^* \) for the number of solutions of the following equations

\[x_1^n + x_2^n + \cdots + x_n^n = ax_1^b x_2^b \cdots x_l^b
\]

over the finite field  \( F_q \) under some certain restrictions, where  \( n \geq 2 \),  \( t > n, m, |(q - 1)| \) for  \( i = 1, \ldots, n \) and  \( a \in F_q^* \).

Hu and Li\(^\dagger\) consider the rational points of the further generalized Markhoff-Hurwitz-type equations of the form

\[(a_1^n + a_2^n + \cdots + a_n^n)^t = ax_1^b x_2^b \cdots x_l^b
\]

over the finite field  \( F_q \) under some other restrictions, where  \( n \geq 2, t > n, k, k_j (n + 1 \leq j \leq t), m_i (1 \leq i \leq n) \) are positive integers. In what follows, we always let  \( d_j = \gcd(m_j, q - 1), 1 \leq j \leq n, M = \text{lcm}[m_1, \ldots, m_n]\),  \( D = \text{lcm}[d_1, \ldots, d_n] \),  \( d_0 = \gcd(d, k) \),  \( d = \gcd(\sum_{i=1}^{n} M / m_i - kM, (q - 1) / D) \).

For any positive integers  \( v_1, v_2, \ldots, v_r \), we let  \( I(v_1, v_2, \ldots, v_r) \) denote the number of  \( r \)-tuples  \( (j_1, j_2, \ldots, j_r) \) of integers with  \( 1 \leq j_1, \ldots, j_r \leq n - 1(1 \leq j \leq r) \), such that  \( j_1/v_1 + j_2/v_2 + \cdots + j_r/v_r \) is an integer. Denote by  \( N_q \) the number of solutions of (2) in  \( F_q^* \). Our main result is the following theorem.

**Theorem 1** Suppose that  \( \gcd(k_1, \ldots, k_r) = d \),  \( dD > 2 \) and there is a positive integer  \( l \) such that  \( dD | (p^l + 1) \), with  \( l \) chosen minimal. Then  \( 2 | l \) and

\[N_q = q^{l-1} + (-1)^{\nu_1} q^{l-2} (q - 1) I(d_1, \ldots, d_n) + (-1)^{\nu_2} q^{l-2} \sum_{r=2}^{n} I(d_r, \ldots, d_n) \]

\[+ (-1)^{\nu_3} q^{l-2} \sum_{r=2}^{n} I(d_1, d_r, \ldots, d_n) \]

\[+ (-1)^{\nu_4} q^{l-2} \sum_{r=2}^{n} I(d_1, d_2, \ldots, d_r) \]

\[= q^{l-1} + (-1)^{\nu_1} q^{l-2} (q - 1) I(d_1, \ldots, d_n) + \cdots + (-1)^{\nu_4} q^{l-2} \sum_{r=2}^{n} I(d_1, d_2, \ldots, d_r)\]

\[+ \sum_{j_1, \ldots, j_n} I(d_{j_1, \ldots, j_n}) + \sum_{d_1, \ldots, d_n} T_1(q^{l-2}/2) \frac{d_1 \cdots d_n}{D} q^{l-2} q^{(l-2)/2} \]

\[T_1 = \begin{cases} d - d_0, & \text{if } a \text{ is a } d \text{-th power in } F_q \\ -d_0, & \text{if } a \text{ is a } d_0 \text{-th power but not a } d \text{-th power in } F_q \\ 0, & \text{if } a \text{ is not a } d_0 \text{-th power in } F_q \end{cases}\]

This paper is organized as follows. In Section 1, we review some useful known lemmas which will be needed later. Subsequently, in Section 2, we prove Theorem 1. Some interesting applications of Theorem 1 will be provided as corollaries at the end of this paper.

### 1 Preliminary Lemmas

In this section, we present some useful lemmas that are needed in the proof of Theorem 1 as follows.

**Lemma 1**\(^\dagger\) For any positive integer  \( m \), the number of elements of  \( m \)-th power in  \( F_q^* \) is  \( q^{1/m} - 1 \).

**Lemma 2**\(^\dagger\) Let  \( t_1, t_2, \ldots, t_r \) be positive integers and  \( t' = \gcd(t_1, t_2, \ldots, t_r, q - 1) \). Then for any elements  \( a, \alpha \in F_q^* \), we have

\[N(ax_1^t \cdots x_r^t) = \alpha \]

\[= N(a(x_1^t \cdots x_r^t)^{t'}) = \alpha \]

\[= |(t(q - 1))^{-1} a^{-t'} \alpha | \text{, if } a^{-t'} \alpha \text{ is a } t'-\text{th power in } F_q^* \]

\[= 0, \text{ otherwise} \]

The following two lemmas are the main results in Ref.[6] and fundamental for our results.

**Lemma 3**\(^\dagger\) Let  \( n > 2 \). Suppose that there is a positive integer  \( l \) such that  \( 2l | s \) and  \( D | (p^l + 1) \). Then

\[N(x_1^n + \cdots + x_n^n) = 0\]

\[= q^{n-1} + (-1)^{\nu_1} q^{n-2} (q - 1) I(d_1, \ldots, d_n) \]

**Lemma 4**\(^\dagger\) Suppose that  \( dD > 2 \) and there is a positive integer  \( l \) such that  \( D | (p^l + 1) \), with  \( l \) chosen minimal. Then  \( 2 | l \) and

\[N((x_1^n + \cdots + x_n^n)^l) = ax_1^t \cdots x_n^t \]

\[= q^{l-1} + (-1)^{\nu_1} q^{l-2} (q - 1) I(d_1, \ldots, d_n) + \cdots + (-1)^{\nu_4} q^{l-2} \sum_{r=2}^{n} I(d_1, d_2, \ldots, d_r)\]

\[+ \sum_{d_1, \ldots, d_n} T_1(q^{l-2}/2) \frac{d_1 \cdots d_n}{D} q^{l-2} q^{(l-2)/2} T_1(q^{l-2}/2) \]

\[T_1 = \begin{cases} d - d_0, & \text{if } a \text{ is a } d \text{-th power in } F_q \\ -d_0, & \text{if } a \text{ is a } d_0 \text{-th power but not a } d \text{-th power in } F_q \\ 0, & \text{if } a \text{ is not a } d_0 \text{-th power in } F_q \end{cases}\]
and 
\[ T_2 = \begin{cases} d_a - 1, & \text{if } a \text{ is a } d_a\text{-th power in } F_q \\ -1, & \text{if } a \text{ is not a } d_a\text{-th power in } F_q \end{cases} \]

## 2 Proof of Theorem 1

In this section, we give the proof of Theorem 1.

**Proof of Theorem 1** Let \( \bar{N}_q \) (resp. \( \tilde{N}_q \)) denote the number of the solutions of the equations 
\[
(x_1^m + x_2^m + \cdots + x_n^m) = x_1 x_2 \cdots x_n x_{a+1}^{k+1} \cdots x_{b+1}^h \quad \text{with} \quad x_{a+1}^{k+1} \cdots x_{b+1}^h = 0 \quad \text{(resp.} \quad x_{a+1}^{k+1} \cdots x_{b+1}^h \neq 0 \text{). Clearly, one has}
\]
\[
N_q = \bar{N}_q + \tilde{N}_q
\]

Then we can solve the problem in two cases. One is \( x_{a+1}^{k+1} \cdots x_{b+1}^h = 0 \) and the other one is \( x_{a+1}^{k+1} \cdots x_{b+1}^h \neq 0 \).

**Case (i)** \( x_{a+1}^{k+1} \cdots x_{b+1}^h = 0 \). Then one has 
\[
N(x_{a+1}^{k+1} \cdots x_{b+1}^h) = N(x_{a+1} \cdots x_{b+1} = 0)
\]
\[
= \sum_{t=1}^{t=n} (t_n - t_{n-j})(q-1)^{t_{n-j}} = q^{r_n} - (q-1)^{r_n}
\]

Using the assumption there is a positive integer \( l \) such that \( 2|s \text{ and } dD/((p+l)+1) \). Thus, by (4) and Lemma 3, 
\[
\bar{N}_q = (q^{r_n} - (q-1)^{r_n}) N((x_1^m + \cdots + x_n^m)^) = 0
\]
\[
= (q^{r_n} - (q-1)^{r_n}) N(x_1^m + \cdots + x_n^m = 0)
\]
\[
= (q^{r_n} - (q-1)^{r_n}) q^{r_n} ((-1)^{(q/2)-1} q^{(q-2)/2})
\]
\[
\times (q-1)^{l} (d_1, \cdots, d_n)
\]

**Case (ii)** If \( x_{a+1}^{k+1} \cdots x_{b+1}^h \neq 0 \), we let \( \delta = x_{a+1}^{k+1} \cdots x_{b+1}^h \).

**Define** 
\[
U := \{ \beta \in F_q : \beta \text{ be a } d\text{-th power in } F_q \}
\]

Note that \( \gcd(k_1, \cdots, k_r, q-1) = d \). Then from Lemma 2, we can deduce that 
\[
\tilde{N}_q = N((x_1^m + x_2^m + \cdots + x_n^m)^) = \delta x_1 x_2 \cdots x_n
\]
\[
= d(q-1)^{r_n-1}
\]
\[
\times \sum_{U} N((x_1^m + x_2^m + \cdots + x_n^m)^) = \delta x_1 x_2 \cdots x_n
\]

Noting that integer \( l \) such that \( dD/\left((p+l)+1\right) \), with \( l \) chosen minimal. Thus for any given \( \delta \in U \), from

**Lemma 1** and Lemma 3, one has 
\[
\sum_{\delta \in U} N((x_1^m + \cdots + x_n^m)^) = \delta x_1 \cdots x_n
\]
\[
= \frac{q-1}{d} (q^{r_n} + (-1)^{r_n} + (-1)^{(q/2)-1} q^{(q-2)/2})
\]
\[
\times (q-1)^{l} I(d_1, \cdots, d_n)
\]

\[
+(-1)^{r_n} \sum_{j \in U} (q^{r_n+2}/q)^{r_n} \sum_{\delta \in U} I(d_1, \cdots, d_n)
\]
\[
+(-1)^{(q/2) - 1} \frac{d \cdots d_{n}}{D} q^{(q-2)/2} \left( d - d_0 \right)
\]
\[
-(-1)^{(q/2) - 1} \frac{d \cdots d_{n}}{D} q^{(q-2)/2} (d - d_0)
\]

Then by (6) together with (7), we have 
\[
\tilde{N}_q = (q-1)^{(q-1)} q^{n-1} + (-1)^{r_n} + (-1)^{(q/2)-1} q^{(q-2)/2}
\]
\[
\times (q-1)^{l} I(d_1, \cdots, d_n)
\]
\[
+(-1)^{r_n} \sum_{j \in U} (q^{r_n+2}/q)^{r_n} \sum_{\delta \in U} I(d_1, \cdots, d_n)
\]
\[
+(-1)^{(q/2) - 1} \frac{d \cdots d_{n}}{D} q^{(q-2)/2} \left( d - d_0 \right)
\]
\[
-(-1)^{(q/2) - 1} \frac{d \cdots d_{n}}{D} q^{(q-2)/2} (d - d_0)
\]

The desired result can follow immediately from (3), (5) and (8). This ends the proof of Theorem 1.

To conclude this section, we present some corollaries. It is clear that \( I(d_1, \cdots, d_n) \) plays a central role in Theorem 1. For any positive integers \( v_1, v_2, \cdots, v_r \), Sun and Wan [12] showed that \( I(v_1, v_2, \cdots, v_r) = 0 \) if and only if either \( \gcd(v_1, v_2, \cdots, v_r) = 1 \) for some \( j \) or \( t \) is odd, \( a_1/2, \cdots, a_t/2 \) are pairwise coprime, and each \( a_i \) is coprime with any odd number in \( \{v_1, v_2, \cdots, v_r\} \), where \( \{a_1, \cdots, a_t\} \) is the set of even integers among \( v_1, v_2, \cdots, v_r \). In Ref. [13], they also showed that \( I(v_1, v_2, \cdots, v_r) = 1 \) if and only if \( 2 \mid v_1, v_2, \cdots, v_r \) are pairwise coprime, and at least \( r-1 \) of the \( v_r/2 \) are odd.

Therefore we can easily deduce the following corollary.

**Corollary 1** Suppose that \( d_1, \cdots, d_m \) are odd, \( d_1, \cdots, d_s \) are even, \( d_1, \cdots, d_m, d_1/2, \cdots, d_s/2 \) are pairwise coprime, \( 0 \leq m \leq n \). Under the conditions of Theorem 1, we have 
\[
N_q = q^{r_n} + T_3 + (q-1)^{(q-1)} ((-1)^{r_n} + (-1)^{(q/2) - 1} q^{(q-2)/2} \left( d - d_0 \right)
\]
\[
+(-1)^{r_n} \sum_{j \in U} (q^{r_n+2}/q)^{r_n} \sum_{\delta \in U} I(d_1, \cdots, d_n)
\]
\[
+(-1)^{(q/2) - 1} \frac{d \cdots d_{n}}{D} q^{(q-2)/2} \left( d - d_0 \right)
\]
\[
-(-1)^{(q/2) - 1} \frac{d \cdots d_{n}}{D} q^{(q-2)/2} (d - d_0)
\]

where 
\[
T_3 = \begin{cases} q^{(q/2) - 1} (q-1), & \text{if } m = 0 \text{ and } n \text{ is even} \\ 0, & \text{otherwise} \end{cases}
\]

and
Let $v$ be a positive integer. It is also known (Ref. [14], Proposition 6.17) that

$$T_a = \begin{cases} 1, & \text{if } m = n \\ 2^{n-m-1}, & \text{if } m < n \end{cases}$$

Then we have the second corollary.

**Corollary 2** Suppose that \( d_1 = \cdots = d_s = D \). Under the conditions of Theorem 1, we have

$$N_q = q^{s-1} + (-1)^{(t/2-1)n} q^{-n/2-1} (q-1)^{s-1}$$

$$D = \sum_{n=0}^{s-1} (-1)^{n/2} q^{n/2} (D-1)^n + (q-1)^{s-n}$$

$$= \sum_{n=0}^{s-1} (-1)^{n/2} q^{n/2} (D-1)^n + (q-1)^{s-n}$$

Clearly, Corollaries 1-2 are some special cases of Theorem 1. For example, consider the further generalized Markoff-Hurwitz-type equation over \( F_q \),

$$x^5 + x^3 + x^2 = x_1 x_2 x_3 x_4 x_5$$

(9)

Clearly \( m_1 = 5, m_2 = 2, m_3 = 6, k = 2, k_4 = 2, k_5 = 4 \). Then we get \( d_1 = \gcd(5, 8) = 1 \), \( d_2 = \gcd(2, 8) = 2 \), \( d_3 = \gcd(6, 8) = 2 \), \( D = \text{lcm}(d_1, d_2, d_3) = 2 \), \( M = \text{lcm}(5, 2, 6) = 30 \), \( d_6 = \gcd(d, d_6) = 2 \) and \( d = \gcd(3 M / m_i - \cdots - \text{lcm}(q-1) / D) = 2 \). One can immediately conclude that (9) has 6817 solutions in \( F_q \) by Corollary 1.

**References**


[3] Baoulina I. On the number of solutions of the equation \( a_1 x_1^n + a_2 x_2^n + \cdots + a_n x_n^n = bx_1 \cdots x_n \) in a finite field [J]. Acta Appl Math, 2005, 89: 35-39.


[5] Baoulina I. On the equation \( x_1^n + x_2^n + \cdots + x_n^n = ax_1 \cdots x_n \) over a finite field [J]. Finite Fields Appl, 2007, 13: 887-895.

[6] Baoulina I. On the equation \( x_1^n + \cdots + x_n^n = ax_1 \cdots x_n \) over a finite field [J]. International Journal of Number Theory, 2006, 3: 351-363.


[12] Sun Q, Wan D Q. On the solvability of the equation \( \sum_{i=1}^{n} x_i \equiv 0 \pmod{1} \) and its applications [J]. Proc Am Math Soc, 1987, 100: 220-224.

[13] Sun Q, Wan D Q. On the Diophantine equation \( \sum_{i=1}^{n} x_i \equiv 0 \pmod{1} \) [J]. Proc Am Math Soc, 1991, 112: 25-29.