Wuhan University Journal of Natural Sciences

2022, Vol.27 No.1, 049-052

Article ID 1007-1202(2022)01-0049-04

DOI https://doi.org/10.1051/wujns/2022271049

The Number of Solutions of Certain Equations over Finite Fields

□ **HU Shuangnian[1], LIU Jianghan[2], QIN Zhentao[3]**

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 Mathmatics and Computer, Panzhihua University, Panzhihua 617000, Sichuan, China

Abstract: Let s be a positive integer, p be an odd prime, $q=p^s$, and let F_q be a finite field of q elements. Let N_q be the number of solutions of the following equations: $(x_1^{m_1}+x_2^{m_2}+\cdots+x_n^{m_n})^k = x_1x_2\cdots x_n x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}$ over the finite field F_q, with $n\geqslant 2$, $t>n,k$, and $k_j(n+1\leqslant j\leqslant t), m_i(1\leqslant i\leqslant n)$ are positive integers. In this paper, we find formulas for N_q when there is a positive integer l such that $dD|(p^l+1)$, where $D=\mathrm{lcm}\ [d_1,\cdots,d_n]$, $d=\gcd(\sum_{i=1}^{n}M/m_i-kM,(q-1)/D)$, $M=\mathrm{lcm}\ [m_1,\cdots,m_n]$, $d_j=\gcd\ (m_j,q-1)$, $1\leqslant j\leqslant n$. And we determine N_q 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

CLC number: O 156

Received date: 2021-11-02

Foundation item: Supported by the National Natural Science Foundation of China (12026224)

Biography: HU Shuangnian, male, Ph. D., Associate professor, research direction: number theory . E-mail: hushuagnian@163.com

0 Introduction

Let p be an odd prime. Let F_q be a finite field of q elements with $q=p^s$, $s\geqslant 1$ 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 $f(x_1,x_2,\cdots,x_n)=b$ in $F_q^n=F_q\times\cdots\times F_q$, where $f(x_1,x_2,\cdots,x_n)$ is a polynomial in $F_q[x_1,\cdots,x_n]$ and $b\in F_q$. That is,

$$N(f=b)=\#\{(x_1,x_2,\cdots,x_n)\in F_q^n\}|\,f(x_1,x_2,\cdots,x_n)=0\}$$

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 $n\geqslant 3$. This type of equations was first studied by Markoff[1] for the case $n=3, a=3$. More generally, these equations were studied by Hurwitz[2].

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

$$a_1x_1^{m_1}+a_2x_2^{m_2}+\cdots+a_nx_n^{m_n}=ax_1x_2\cdots x_n$$

where $a_i,a\in F_q^*$ and m_i are positive integers satisfying $m_i\,|(q-1)$ for $i=1,\cdots,n$ and $n\geqslant 2$. Baoulina[4-6] and Pan *et al*[7] considered the further generalized Markoff- Hurwitz-type equations of the form:

$$(a_1x_1^{m_1}+a_2x_2^{m_2}+\cdots+a_nx_n^{m_n})^k=ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} \qquad (1)$$

where $n\geqslant 2$, m_i,k_i,k are positive integers, $a,a_i\in F_q^*$, for $i=1,\cdots,n$. The special case (1) of $k=1$ is investigated by Cao[8]. Song and Chen[9] presented the formulas for the number of solutions of the following equations

$$x_1^{m_1}+x_2^{m_2}+\cdots+x_n^{m_n}=ax_1x_2\cdots x_t$$

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

Hu and Li[10] consider the rational points of the further generalized Markoff-Hurwitz-type equations of the form

$$(a_1x_1^{m_1}+a_2x_2^{m_2}+\cdots+a_nx_n^{m_n})^k=ax_1^{k_1}x_2^{k_2}\cdots x_t^{k_t}$$

over the finite field F_q under some certain cases, where $n\geqslant 2$, m_i, k_j, k and $t>n$ are positive integers, a_i, $a\in F_q^*$, for $1\leqslant i\leqslant n$, $1\leqslant j\leqslant t$.

In this paper, we consider the number of solutions of the following equations

$$(x_1^{m_1}+x_2^{m_2}+\cdots+x_n^{m_n})^k=x_1x_2\cdots x_nx_{n+1}^{k_{n+1}}\cdots x_t^{k_t} \qquad (2)$$

over the finite field F_q under some other restrictions, where $n\geqslant 2$, $t>n$, k, $k_j\,(n+1\leqslant j\leqslant t)$, $m_i\,(1\leqslant i\leqslant n)$ are positive integers. In what follows, we always let

$$d_j=\gcd(m_j,q-1),\ 1\leqslant j\leqslant n,\ M=\mathrm{lcm}[m_1,\cdots,m_n],$$
$$D=\mathrm{lcm}[d_1,\cdots,d_n],\ d_0=\gcd(d,k),$$
$$d=\gcd\Big(\sum_{i=1}^{n}M/m_i-kM,(q-1)/D\Big).$$

For any positive integers $\nu_1,\nu_2,\cdots,\nu_r$, we let $I(\nu_1,\nu_2,\cdots,\nu_r)$ denote the number of r-tuples $(j_1,j_2,\cdots,j_r)$ of integers with $1\leqslant j_i\leqslant \nu_i-1$ $(1\leqslant i\leqslant r)$, such that $j_1/\nu_1+j_2/\nu_2+\cdots+j_r/\nu_r$ is an integer. Denote by N_q the number of solutions of (2) in F_q^n. Our main result is the following theorem.

Theorem 1 Suppose that $\gcd(k_{n+1},\cdots,k_t)=d$, $\mathrm{d}D>2$ and there is a positive integer l such that $dD\,|\,(p^l+1)$, with l as chosen minimal. Then $2l\,|\,s$ and

$$N_q=q^{t-1}+(-1)^{((s/2l)-1)n}q^{t-n/2-1}(q-1)I(d_1,\cdots,d_n)$$
$$+q^{t-n}\Big((-1)^{n-1}+(-1)^{n-1}\sum_{r=2}^{n}((-1)^{rs/2l}q^{r/2})$$
$$\cdot\sum_{1\ \ j_1\ \cdots\ j_r\ \ n}I(d_{j_1},\cdots,d_{j_r})+(-1)^{((s/2l)-1)(n-1)}$$
$$\cdot\frac{d_1\cdots d_n}{D}q^{(n-1)/2}(d-d_0)-(-1)^{((s/2l)-1)n}\frac{d_1\cdots d_n}{D}q^{(n-2)/2}$$
$$\cdot(d_0-1)\Big)$$

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[9,11] For any positive integer m, the number of elements of m-th power in F_q^* is $\dfrac{q-1}{m}$.

Lemma 2[10] Let $t_1,t_2,\cdots,t_r$ be positive integers and $t'=\gcd(t_1,t_2,\cdots,t_r,q-1)$. Then for any elements $a,\alpha\in F_q^*$, we have

$$N(ax_1^{t_1}\cdots x_r^{t_r}=\alpha)$$
$$=N(a(x_1\cdots x_r)^{t'}=\alpha)$$
$$=\begin{cases} t'(q-1)^{r-1}, & \text{if } a^{-1}\alpha \text{ is a } t'\text{-th power in } F_q^* \\ 0, & \text{otherwise}\end{cases}$$

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

Lemma 3[6] Let $n>2$. Suppose that there is a positive integer l such that $2l\,|\,s$ and $dD\,|\,(p^l+1)$. Then

$$N(x_1^{m_1}+\cdots+x_n^{m_n}=0)$$
$$=q^{n-1}+(-1)^{((s/2l)-1)n}q^{(n-2)/2}(q-1)I(d_1,\cdots,d_n)$$

Lemma 4[6] Suppose that $\mathrm{d}D>2$ and there is a positive integer l such that $dD\,|\,(p^l+1)$, with l chosen minimal. Then $2l\,|\,s$ and

$$N((x_1^{m_1}+\cdots+x_n^{m_n})^k=ax_1\cdots x_n)$$
$$=q^{n-1}+(-1)^{n-1}+(-1)^{((s/2l)-1)n}q^{(n-2)/2}(q-1)I(d_1,\cdots,d_n)$$
$$+(-1)^{n-1}\sum_{r=2}^{n}(-1)^{rs/2l}q^{r/2}\sum_{1\leqslant j_1\leqslant\cdots\leqslant j_r\leqslant n}I(d_{j_1},\cdots,d_{j_r})$$
$$+(-1)^{((s/2l)-1)(n-1)}\frac{d_1\cdots d_n}{D}q^{(n-1)/2}T_1$$
$$-(-1)^{((s/2l)-1)n}\frac{d_1\cdots d_n}{D}q^{(n-2)/2}T_2$$

where

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

and

$$T_2=\begin{cases} d_0-1, \text{ if } a \text{ is a } d_0\text{-th power in } F_q \\ -1, \quad \text{if } a \text{ is not a } d_0\text{-th power in } F_q \end{cases}$$

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 $(x_1^{m_1}+x_2^{m_2}+\cdots+x_n^{m_n})^k=x_1x_2\cdots x_nx_{n+1}^{k_{n+1}}\cdots x_t^{k_t}$ with $x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}=0$ (resp. $x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}\neq 0$). Clearly, one has

$$N_q=\bar{N}_q+\tilde{N}_q \tag{3}$$

Then we can solve the problem in two cases. One is $x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}=0$ and the other one is $x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}\neq 0$.

Case (i) $x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}=0$. Then one has

$$\begin{aligned} N(x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}=0)&=N(x_{n+1}\cdots x_t=0)\\ &=\sum_{j=1}^{t-n}\binom{t-n}{j}(q-1)^{t-n-j}\\ &=q^{t-n}-(q-1)^{t-n} \end{aligned} \tag{4}$$

Using the assumption there is a positive integer l such that $2l\,|\,s$ and $dD\,|\,(p^l+1)$. Thus, by (4) and Lemma 3 ,

$$\begin{aligned} \bar{N}_q&=(q^{t-n}-(q-1)^{t-n})N((x_1^{m_1}+\cdots+x_n^{m_n})^k=0)\\ &=(q^{t-n}-(q-1)^{t-n})N(x_1^{m_1}+\cdots+x_n^{m_n}=0)\\ &=(q^{t-n}-(q-1)^{t-n})(q^{n-1}+(-1)^{((s/2l)-1)n}q^{(n-2)/2}\\ &\quad\times(q-1)I(d_1,\cdots,d_n)) \end{aligned} \tag{5}$$

Case (ii) If $x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}\neq 0$, we let $\delta=x_{n+1}^{k_{n+1}}\cdots x_t^{k_t}$. Define

$$U:=\{\beta\in F_q^*:\beta \text{ be a } d\text{-th power in } F_q^*\}$$

Note that $\gcd(k_{n+1},\cdots,k_t,q-1)=d$. Then from Lemma 2, we can deduce that

$$\begin{aligned} \tilde{N}_q&=N((x_1^{m_1}+x_2^{m_2}+\cdots+x_n^{m_n})^k=\delta x_1x_2\cdots x_n)\\ &=d(q-1)^{t-n-1}\\ &\quad\cdot\sum_{\delta\in U}N((x_1^{m_1}+x_2^{m_2}+\cdots+x_n^{m_n})^k=\delta x_1x_2\cdots x_n) \end{aligned} \tag{6}$$

Noting that integer l such that $dD\,|\,(p^l+1)$, with l chosen minimal. Thus for any given $\delta\in U$, from Lemma 1 and Lemma 3, one has

$$\begin{aligned} &\sum_{\delta\in U}N((x_1^{m_1}+\cdots+x_n^{m_n})^k=\delta x_1\cdots x_n)\\ &=\frac{q-1}{d}(q^{n-1}+(-1)^{n-1}+(-1)^{((s/2l)-1)n}q^{(n-2)/2}\\ &\quad\cdot(q-1)I(d_1,\cdots,d_n)\\ &\quad+(-1)^{n-1}\sum_{r=2}^{n}(-1)^{rs/2l}q^{r/2}\sum_{1\leqslant j_1\leqslant\cdots\leqslant j_r\leqslant n}I(d_{j_1},\cdots,d_{j_r})\\ &\quad+(-1)^{((s/2l)-1)(n-1)}\frac{d_1\cdots d_n}{D}q^{(n-1)/2}(d-d_0)\\ &\quad-(-1)^{((s/2l)-1)n}\frac{d_1\cdots d_n}{D}q^{(n-2)/2}(d_0-1)) \end{aligned} \tag{7}$$

Then by (6) together with (7), we have

$$\begin{aligned} \tilde{N}_q&=(q-1)^{t-n}(q^{n-1}+(-1)^{n-1}+(-1)^{((s/2l)-1)n}\\ &\quad\cdot q^{(n-2)/2}(q-1)I(d_1,\cdots,d_n)+(-1)^{n-1}\\ &\quad\cdot\sum_{r=2}^{n}(-1)^{rs/2l}q^{r/2}\sum_{1\leqslant j_1\leqslant\cdots\leqslant j_r\leqslant n}I(d_{j_1},\cdots,d_{j_r})\\ &\quad+(-1)^{((s/2l)-1)(n-1)}\frac{d_1\cdots d_n}{D}q^{(n-1)/2}(d-d_0)\\ &\quad-(-1)^{((s/2l)-1)n}\frac{d_1\cdots d_n}{D}q^{(n-2)/2}(d_0-1)) \end{aligned} \tag{8}$$

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 $\gcd(v_j,v_2,\cdots,v_r/v_j)=1$ for some j or t is odd, $\omega_1/2,\cdots,\omega_t/2$ are pairwise coprime, and each ω_j is coprime with any odd number in $\{v_1,v_2,\cdots,v_r\}$, where $\{\omega_1,\cdots,\omega_t\}$ 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 $2\,|\,r,v_1/2,\cdots,v_r/2$ are pairwise coprime, and at least $(r-1)$ of the $v_j/2$ are odd.

Therefore we can easily deduce the following corollary.

Corollary 1 Suppose that $d_1,\cdots,d_m$ are odd, $d_{m+1},\cdots,d_n$ are even, $d_1,\cdots,d_m,d_{m+1}/2,\cdots,d_n/2$ are pairwise coprime, $0\leqslant m\leqslant n$. Under the conditions of Theorem 1, we have

$$\begin{aligned} N_q&=q^{t-1}+T_3+(q-1)^{t-n}((-1)^{n-1}\\ &\quad+(-1)^{n-1}\sum_{r=2,2|r}^{n-m}\binom{n-m}{r}q^{r/2}+(-1)^{((s/2l)-1)(n-1)}q^{(n-1)/2}(d-d_0)\\ &\quad-(-1)^{((s/2l)-1)n}q^{(n-2)/2}(d_0-1))T_4 \end{aligned}$$

where

$$T_3=\begin{cases} q^{t-n/2-1}(q-1), \text{ if } m=0 \text{ and } n \text{ is even}\\ \qquad 0, \quad \text{otherwise} \end{cases}$$

and

$$T_4=\begin{cases}1, & \text{if } m=n\\ 2^{n-m-1}, & \text{if } m<n\end{cases}$$

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

$$I(\underbrace{v,\cdots,v}_{r})=\frac{(v-1)^r+(-1)^r(v-1)}{v}$$

Then we have the second corollary.

Corollary 2 Suppose that $d_1=\cdots=d_n=D$. Under the conditions of Theorem 1, we have

$$\begin{aligned}N_q&=q^{t-1}+(-1)^{((s/2l)-1)n}q^{t-n/2-1}(q-1)\\&\cdot\frac{(D-1)^n+(-1)^n(D-1)}{D}+(q-1)^{t-n}\\&\cdot((-1)^{n-1}\sum_{m=0}^{n}(-1)^{ms/2l}q^{m/2}\frac{(D-1)^m+(-1)^m(D-1)}{D}\\&+(-1)^{((s/2l)-1)(n-1)}D^{n-1}q^{(n-1)/2}(d-d_0)\\&-(-1)^{((s/2l)-1)n}D^{n-1}q^{(n-2)/2}(d_0-1))\end{aligned}$$

Clearly, Corollaries 1-2 are some special cases of Theorem 1. For example, consider the further generalized Markoff-Hurwitz-type equation over F_{3^2}

$$(x_1^5+x_2^2+x_3^6)^2=x_1x_2x_3x_4^2x_5^4 \tag{9}$$

Clearly $m_1=5, m_2=2, m_3=6$, $k=2, k_4=2, k_5=4$. Then we get $d_1=\gcd(5,8)=1$, $d_2=\gcd(2,8)=2$, $d_3=\gcd(6,8)=2$, $D=\operatorname{lcm}(d_1,d_2,d_3)=2$, $M=\operatorname{lcm}$ (5, 2, 6)=30, $d_0=\gcd(d,k)=2$ and $d=\gcd(\sum_{i=1}^{3}M/m_i-kM,(q-1)/D)=2$. One can immediately conclude that (9) has 6 817 solutions in F_{3^2} by Corollary 1.

References

[1] Markoff A. Sur les formes binaires indéfinies [J]. *Math Ann*, 1880, **17**:379-399.

[2] Hurwitz A. Ubereine Aufgabe der unbestimmten analysis [J]. *Arch Math Phys*, 1907, **3**: 185-196.

[3] Baoulina I. On the number of solutions of the equation $a_1x_1^{m_1}+a_2x_2^{m_2}+\cdots+a_nx_n^{m_n}=bx_1x_2\cdots x_n$ in a finite field[J]. *Acta Appl Math*, 2005, **89**: 35-39.

[4] Baoulina I. Generalizations of the Markoff-Hurwitz equations over finite fields [J]. *Journal of Number Theory*, 2006, **118**(1): 31-52.

[5] Baoulina I. On the equation $x_1^{m_1}+x_2^{m_2}+\cdots+x_n^{m_n}=ax_1x_2\cdots x_n$ over a finite field [J]. *Finite Fields Appl*, 2007, **13**: 887-895.

[6] Baoulina I. On the equation $(x_1^{m_1}+\cdots+x_n^{m_n})^k=ax_1\cdots x_n$ over a finite field [J]. *International Journal of Number Theory*, 2006, **3**: 351-363.

[7] Pan X, Zhao X, Cao W. A problem of Carlitz and its generalizations [J]. *Archiv der Mathematik*, 2014, **102**(4): 337-343.

[8] Cao W. On gengeralized Markoff-Hurwitz-type equations over finite fields [J]. *Acta Appl Math*, 2010, **112**:275-281.

[9] Song J, Chen Y. The number of some equations over finite fields [J]. *Journal of University of Chinese Academy of Sciences*, 2015, **32**:582-587.

[10] Hu S N, Li Y Y. The number of solutions of generalized Markoff-Hurwitz-type equations over finite fields [J]. *Journal of Zhejiang University* (*Science Edition*), 2017, **44**(5): 516-519(Ch).

[11] Lidl R, Niederreiter H, Cohn F M. *Finite Fields* [M]. Cambridge: Cambridge University Press, 1997.

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

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

[14] Small C. *Arithmetic of Finite Fields* [M]. New York: Marcel Dekker, 1991.

□