

Counting roots of fully triangular polynomials over finite fields

José Gustavo Coelho, Fabio Enrique Brochero Martínez

September 2022

Abstract

Let \mathbb{F}_q be a finite field with q elements, $f \in \mathbb{F}_q[x_1, \dots, x_n]$ a polynomial in n variables and let us denote by $N(f)$ the number of roots of f in \mathbb{F}_q^n . In this paper we consider the family of fully triangular polynomials, i.e., polynomials of the form

$$f(x_1, \dots, x_n) = a_1 x_1^{d_{1,1}} + a_2 x_1^{d_{1,2}} x_2^{d_{2,2}} + \dots + a_n x_1^{d_{1,n}} \dots x_n^{d_{n,n}} - b,$$

where $d_{i,j} > 0$ for all $1 \leq i \leq j \leq n$. For these polynomials, we obtain explicit formulas for $N(f)$ when the augmented degree matrix of f is row-equivalent to the augmented degree matrix of a linear polynomial or a quadratic diagonal polynomial.

Keywords— triangular polynomials, degree matrix, augmented degree matrix, generalized Markoff-Hurwitz equation

1 Introduction

The classical Markov equation is of the form $x^2 + y^2 + z^2 = 3xyz$ and it was studied by Markov in the integer ring. In particular, he showed that the solutions of this equation satisfy a recursive relation, such that the solutions can be ordered forming a binary tree. Hurwitz considered a generalization of the form

$$x_1^2 + \dots + x_n^2 = ax_1 x_2 \dots x_n,$$

and he showed that this equation does not have non-trivial integer solutions when $a > n \geq 3$.

This equation can be further generalized in many ways such as changing the number of variables and the exponents, considering the equation in other rings or fields, etc. Many authors have considered generalizations where the equation is over finite fields.

One possible generalization is to consider equations of the form

$$a_1 x_1^{m_1} + a_2 x_2^{m_2} + \dots + a_n x_n^{m_n} = bx_1 \dots x_n, \quad (1)$$

where $m_j > 0$, $a_j \in \mathbb{F}_q^*$ for all $j = 1, \dots, n$ and $b \in \mathbb{F}_q^*$, where \mathbb{F}_q is the finite field with q elements. These equations were studied by Carlitz and Baoulina [4, 5], which determined the number of solutions in \mathbb{F}_q^n under certain restrictions of the exponents.

The generalized Markoff-Hurwitz equation is an equation of the form

$$x_1^{m_1} + x_2^{m_2} + \dots + x_n^{m_n} = bx_1^{t_1}x_2^{t_2} \dots x_n^{t_n}. \quad (2)$$

where $m_j, t_j > 0$ for all $j = 1, \dots, n$ and $b \in \mathbb{F}_q^*$. The equation in the case when $m_1 = m_2 = \dots = m_n = n$ and $t_1 = \dots = t_n = 1$ defines a hypersurface known as Calabi-Yau's hypersurface and it has been intensively studied by some authors [6, 7]. Some results about the number of solutions for the general equation (2) can be found in the literature; for instance, the number of solutions over \mathbb{F}_q was calculated by Carlitz in the case when $\gcd(m \sum_{i=1}^n t_i/m_i - m, q-1) = 1$, where $m = m_1 m_2 \dots m_n$. The case when $\gcd(m \sum_{i=1}^n t_i/m_i - m, q-1) > 1$ was considered by Cao, Jiang and Gao [1, 2], assuming some arithmetic conditions.

Cao, Wen and Wang [3] have also determined the number of solutions in \mathbb{F}_q^n for equations of the form

$$a_1 x_1^{d_{1,1}} \dots x_n^{d_{1,n}} + \dots + a_n x_1^{d_{n,1}} \dots x_n^{d_{n,n}} = 0,$$

where $d_{i,j} > 0$, i.e., all exponents are positive, assuming that the matrix $(d_{i,j})_{i,j}$ is row equivalent to a diagonal matrix D , when the elements in the diagonal of D are only 1's and 2's.

In this paper we will determine the number of solutions of equations

$$a_1 x_1^{d_{1,1}} + a_2 x_1^{d_{1,2}} x_2^{d_{2,2}} + \dots + a_n x_1^{d_{1,n}} \dots x_n^{d_{n,n}} = b,$$

where $d_{i,j} > 0$ for all $1 \leq i \leq j \leq n$ and the exponents $d_{i,j}$ satisfy some arithmetical conditions. In fact, we show sufficient conditions in order to the equation to have, in $(\mathbb{F}_q^*)^n$, the same number of solutions of a more simple equation. In this case we say that the equations are $*$ -equivalent. Next, we use this equivalence in order to calculate the total number of solutions.

The remainder of the paper will be organized as follows. In Section 2, we will introduce some preliminary results. In Section 3, we will describe triangular polynomials and relations among them. The main results will be given in Section 4.

2 Preliminaries

Let p be a prime number, q a power of p and $\mathbb{F}_q[x_1, \dots, x_n]$ the polynomial ring over \mathbb{F}_q with n variables. For each $D = (d_1, \dots, d_n) \in \mathbb{Z}_{\geq 0}^n$ let us define the monomial $X^D = x_1^{d_1} \dots x_n^{d_n}$. Given a polynomial $f \in \mathbb{F}_q[x_1, \dots, x_n]$ of the form

$$f(x_1, \dots, x_n) = \sum_{j=1}^m a_j X^{D_j}, \quad (3)$$

where $D_j = (d_{1j}, \dots, d_{nj}) \in \mathbb{Z}_{\geq 0}^n$ and $a_j \neq 0$ for all $j = 1, \dots, m$, we define $N(f)$ as the number of roots of $f(x_1, \dots, x_n)$ over \mathbb{F}_q^n and $N^*(f)$ as the number of roots over $(\mathbb{F}_q^*)^n$. Let us define

the degree matrix of f as $D_f = (D_1^T, \dots, D_m^T)$ and the augmented degree matrix of f as $\tilde{D}_f = ((\tilde{D}_1)^T, \dots, (\tilde{D}_m)^T)$, where $(\tilde{D}_j)^T = (1, D_j)$.

It is well known that the group of multiplicative characters of a finite field is cyclic. Let ω be a multiplicative character over \mathbb{F}_q with order $q-1$, and therefore ω is a generator of the multiplicative characters group, i.e., $\widehat{\mathbb{F}_q^*} = \{\omega^k : k = 0, 1, \dots, q-2\}$. Let us define Tr as the trace function from \mathbb{F}_q to \mathbb{F}_p and δ_p be a primitive p -th complex root of unity. For each integer $0 \leq k \leq q-2$, we define the Gauss sum of ω^{-k} over \mathbb{F}_q as follows:

$$G(k) = \sum_{a \in \mathbb{F}_q^*} \omega(a)^{-k} \delta_p^{Tr(a)}.$$

The following result allows us to express $N^*(f)$ in terms of ω and the Gauss sums.

Lemma 1. *Let f be a polynomial of the form (3), then*

$$N^*(f) = \frac{(q-1)^n}{q} + \frac{(q-1)^{n+1-m}}{q} \sum \prod_{j=1}^m \omega(a_j)^{v_j} G(v_j),$$

where the sum is taken over all vectors $v = (v_1, \dots, v_m)$ with $0 \leq v_i \leq q-2$ for $i = 1, \dots, m$ such that $\tilde{D}_f v^T \equiv 0 \pmod{q-1}$.

Proof. See Lemma 2.4 in [1]. □

Definition 2. *Two polynomials $f = \sum_j a_j X_j^D$ and $g = \sum_j a_j X_j^{D'}$ are said to be $*$ -equivalent if they have the same coefficient vector (a_1, \dots, a_m) and the congruences $\tilde{D}_f v^T \equiv 0 \pmod{q-1}$ and $\tilde{D}_g v^T \equiv 0 \pmod{q-1}$ have the same set of solutions.*

It follows from Lemma 1 that if f and g are $*$ -equivalent polynomials, then $N^*(f) = N^*(g)$, i.e., they have the same number of roots over $(\mathbb{F}_q^*)^n$.

It is easy to check that the coefficient vectors of two polynomials are equal, but we'd like to know when the linear systems $\tilde{D}_f v^T = 0$ and $\tilde{D}_g v^T = 0$ have the same set of solutions. It can be verified that two matrices D and E with coefficients in \mathbb{Z}_{q-1}^m such that $Dv^T \equiv 0 \pmod{q-1}$ and $Ev^T \equiv 0 \pmod{q-1}$ have the same set of solutions if there is an invertible matrix M over \mathbb{Z}_{q-1} such that $MD = E$, and in this case, we say that D and E are row-equivalent. Hence, if two polynomials f and g have the same coefficient vector and there is an invertible matrix M over \mathbb{Z}_{q-1} such that $M\tilde{D}_f = \tilde{D}_g$, then f and g are $*$ -equivalent.

In particular, the elementary row operations are

- (i) swapping two rows;
- (ii) adding a multiple of a row to another;
- (iii) multiplying a row by an element in \mathbb{Z}_{q-1}^* ;

which can be represented by multiplying invertible matrices, so if we can apply these operations in \tilde{D}_f to obtain \tilde{D}_g , the congruence systems have the same solutions. We will use this sufficient criterion to prove $*$ -equivalency when needed.

It is worth noting that even though $N^*(f) = N^*(g)$ for two $*$ -equivalent polynomials f and g , that doesn't mean they have the same set of roots. For instance, the polynomials $f(x, y) = x^2y^3 + xy^2$ and $g(x, y) = xy + x^3y^2$ in $\mathbb{F}_5[x, y]$ are $*$ -equivalent, but it can be verified that they have distinct sets of roots over $(\mathbb{F}_5^*)^2$.

3 Triangular polynomials

Let f be a polynomial in $\mathbb{F}_q[x_1, \dots, x_k]$, and let us define $f_k \in \mathbb{F}_q[x_1, \dots, x_k]$ as

$$f_k(x_1, \dots, x_k) = f(x_1, \dots, x_k, 0, \dots, 0).$$

We say that f and g are totally $*$ -equivalent if f_k is $*$ -equivalent to g_k for all $1 \leq k \leq n$. In general, it is not true that f being $*$ -equivalent to g implies that f_k is $*$ -equivalent to g_k for all k .

Let us introduce a class of polynomials for which a sufficient criterion for total $*$ -equivalence can be determined. We say that $f \in \mathbb{F}_q[x_1, \dots, x_n]$ is a triangular polynomial if it is of the form

$$f(x_1, \dots, x_n) = \sum_{i=1}^n a_i X^{D_i} - b; \quad a_1, \dots, a_n \in \mathbb{F}_q^*, b \in \mathbb{F}_q, \quad (4)$$

where $D_j = (d_{1,j}, \dots, d_{j,j}, 0, \dots, 0)$, $d_{j,j} > 0$ for all $1 \leq j \leq n$ and $d_{i,j} \geq 0$ for all $1 \leq i < j$. If we additionally have that $d_{i,j} > 0$ for all $1 \leq i \leq j \leq n$, we refer to this polynomial as a *fully* triangular polynomial.

Lemma 3. *Let $f, g \in \mathbb{F}_q[x_1, \dots, x_n]$ be two $*$ -equivalent triangular polynomials, M the invertible $(n+1) \times (n+1)$ matrix over \mathbb{Z}_{q-1} such that $M\tilde{D}_f = \tilde{D}_g$ and M_k the submatrix obtained from M by picking the first $k+1$ rows and columns. If M_k is invertible, then f_k and g_k are also $*$ -equivalent.*

Proof. Since f and g are triangular matrices, we can partition their degree matrices and the matrix M into blocks

$$\tilde{D}_f = \begin{bmatrix} \tilde{D}_{f_k} & D_1 \\ 0 & D_2 \end{bmatrix}, \quad \tilde{D}_g = \begin{bmatrix} \tilde{D}_{g_k} & E_1 \\ 0 & E_2 \end{bmatrix}, \quad M = \begin{bmatrix} M_k & N_1 \\ N_2 & N_3 \end{bmatrix},$$

such that \tilde{D}_{g_k} and \tilde{D}_{f_k} are $(k+1) \times k$ blocks, M_k is a $(k+1) \times (k+1)$ block and the blocks $D_1, D_2, E_1, E_2, N_1, N_2, N_3$ have appropriate dimensions. From the $*$ -equivalency between f and g we know that

$$\begin{aligned} \begin{bmatrix} \tilde{D}_{g_k} & E_1 \\ 0 & E_2 \end{bmatrix} &= \tilde{D}_g = M\tilde{D}_f \\ &= \begin{bmatrix} M_k & N_1 \\ N_2 & N_3 \end{bmatrix} \begin{bmatrix} \tilde{D}_{f_k} & D_1 \\ 0 & D_2 \end{bmatrix} \\ &= \begin{bmatrix} M_k \tilde{D}_{f_k} & M_k D_1 + N_1 D_2 \\ N_2 \tilde{D}_{f_k} & N_2 D_1 + N_3 D_2 \end{bmatrix}, \end{aligned}$$

where considering the equality of the upper left block gives us $M_k \tilde{D}_{f_k} = \tilde{D}_{g_k}$, implying that f_k and g_k are $*$ -equivalent because M_k is invertible. \square

Hence, if f, g are two $*$ -equivalent triangular polynomials, with $M \tilde{D}_f = \tilde{D}_g$ and the submatrices M_k are invertible for every $1 \leq k \leq n-1$, then f and g are totally $*$ -equivalent. We now present a specific set of operations which always results in transformation matrices that satisfy these conditions.

Lemma 4. *Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ be a triangular polynomial. Let us denote by r_1, \dots, r_{n+1} the rows in \tilde{D}_f and consider the following invertible row operations:*

$$(i) \ r_i \leftarrow c \cdot r_i, \ 2 \leq i \leq n+1, \ c \in \mathbb{Z}_{q-1}^*.$$

$$(ii) \ r_j \leftarrow r_j + c \cdot r_i, \ 2 \leq j < i, \ c \in \mathbb{Z}_{q-1}.$$

Any $$ -equivalency obtained using only these row operations is totally $*$ -equivalent.*

Proof. Any matrix M obtained from those operations is of the form

$$M = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & m_{1,1} & m_{1,2} & \cdots & m_{1,n-1} & m_{1,n} \\ 0 & 0 & m_{2,2} & \cdots & m_{2,n-1} & m_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & m_{n-1,n-1} & m_{n-1,n} \\ 0 & 0 & 0 & \cdots & 0 & m_{n,n} \end{bmatrix}, \quad (5)$$

where $m_{i,j} \in \mathbb{Z}_{q-1}$ and the elements in the diagonal are invertible. For every $1 \leq k < n-1$ the determinant of M_k is $\prod_{i=1}^k m_{i,i}$, which is invertible over \mathbb{Z}_{q-1} and thus every M_k is invertible, making the $*$ -equivalency total. \square

Although one could believe that all complete equivalences between triangular matrices can be attained using those two operations, this assumption is not correct. For instance, $f = x_1 + x_1^3 x_2^5$, $g = x_1^2 + x_1^4 x_2 \in \mathbb{F}_7[x_1, x_2]$ are totally $*$ -equivalent polynomials, i.e., $M \tilde{D}_f = \tilde{D}_g$ where M is the invertible matrix

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 5 \end{bmatrix},$$

but from a straightforward calculation it can be proved that there is no invertible upper triangular matrix N that satisfies $N \tilde{D}_f = \tilde{D}_g$. The following result tells us when a triangular polynomial is totally $*$ -equivalent to a diagonal polynomial through the two operations given in Lemma 4.

Theorem 5. *Let f be a triangular polynomial of the form (4) and*

$$g(x_1, \dots, x_n) = a_1 x_1^{e_1} + \cdots + a_n x_n^{e_n} - b,$$

be a diagonal polynomial where $e_1, \dots, e_n \in \mathbb{Z}_{>0}$. Then f is totally $$ -equivalent to g if the following two conditions are true:*

(i) for all $1 \leq j \leq n$ there is a $m_{j,j} \in \mathbb{Z}_{q-1}^*$ such that $d_{j,j} = m_{j,j}e_j$,

(ii) for all $1 \leq i < j \leq n$ we have $\gcd(d_{j,j}, q-1) \mid d_{i,j}$.

Proof. The augmented degree matrices of f and g are

$$\tilde{D}_f = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & | & 1 \\ d_{1,1} & d_{1,2} & d_{1,3} & \cdots & d_{1,n-1} & d_{1,n} & | & 0 \\ 0 & d_{2,2} & d_{2,3} & \cdots & d_{2,n-1} & d_{2,n} & | & 0 \\ 0 & 0 & d_{3,3} & \cdots & d_{3,n-1} & d_{3,n} & | & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & | & \vdots \\ 0 & 0 & 0 & \cdots & d_{n-1,n-1} & d_{n-1,n} & | & 0 \\ 0 & 0 & 0 & \cdots & 0 & d_{n,n} & | & 0 \end{bmatrix}, \quad \tilde{D}_g = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & | & 1 \\ e_1 & 0 & 0 & \cdots & 0 & 0 & | & 0 \\ 0 & e_2 & 0 & \cdots & 0 & 0 & | & 0 \\ 0 & 0 & e_3 & \cdots & 0 & 0 & | & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & | & \vdots \\ 0 & 0 & 0 & \cdots & e_{n-1} & 0 & | & 0 \\ 0 & 0 & 0 & \cdots & 0 & e_n & | & 0 \end{bmatrix},$$

where the last columns are present only if $b \neq 0$.

Let us suppose that conditions (i) and (ii) are true. Since (i) implies that there is an element $m_{j,j} \in \mathbb{Z}_{q-1}^*$ such that $d_{j,j} = m_{j,j}e_j$, condition (ii) becomes $\gcd(e_j m_{j,j}, q-1) \mid d_{i,j}$. As $\gcd(m_{j,j}, q-1) = 1$, that implies condition (ii) is equivalent to $(e_j, q-1) \mid d_{i,j}$, which is in turn equivalent to the existence of $m_{i,j} \in \mathbb{Z}_{q-1}$ such that $d_{i,j} = m_{i,j}e_j$ over \mathbb{Z}_{q-1} . We can then use these values of $m_{i,j}$ to construct an invertible matrix M of the form (5), such that when we multiply M by \tilde{D}_g gives us

$$M\tilde{D}_g = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & | & 1 \\ m_{1,1}e_1 & m_{1,2}e_2 & m_{1,3}e_3 & \cdots & m_{1,n-1}e_{n-1} & m_{1,n}e_n & | & 0 \\ 0 & m_{2,2}e_2 & m_{2,3}e_3 & \cdots & m_{2,n-1}e_{n-1} & m_{2,n}e_n & | & 0 \\ 0 & 0 & m_{3,3}e_3 & \cdots & m_{3,n-1}e_{n-1} & m_{3,n}e_n & | & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & | & \vdots \\ 0 & 0 & 0 & \cdots & m_{n-1,n-1}e_{n-1} & m_{n-1,n}e_n & | & 0 \\ 0 & 0 & 0 & \cdots & 0 & m_{n,n}e_n & | & 0 \end{bmatrix},$$

that is equal to \tilde{D}_f . □

For the specific cases where the diagonal polynomials are linear or quadratic this criterion is simpler.

Corollary 6. *Let f be a triangular polynomial of the form (4) and*

$$g(x_1, \dots, x_n) = a_1 x_1^e + \cdots + a_n x_n^e - b,$$

be a diagonal polynomial, where $e \in \mathbb{Z}_{>0}$.

- a) *If $e = 1$ and $\gcd(d_{j,j}, q-1) = 1$ for all $1 \leq j \leq n$, then f is totally $*$ -equivalent to g .*
- b) *If $e = 2$, q is odd, that there exists a $m_{j,j} \in \mathbb{Z}_{q-1}^*$ such that $d_{j,j} = 2m_{j,j}$ for all $1 \leq j \leq n$ and that $2 \mid d_{i,j}$ for all $1 \leq i < j \leq n$, then f is $*$ -equivalent to g .*

Proof. The statements in each item imply the conditions given in Theorem 5. In fact,

-
- a) If $\gcd(d_{j,j}, q-1) = 1$, then condition (ii) is always verified and $d_{j,j}$ is invertible, verifying condition (i).
 - b) The statement that there is an invertible $m_{j,j}$ in \mathbb{Z}_{q-1} such that $d_{j,j} = 2m_{j,j}$ for all $1 \leq j \leq n$ is, in this case, equivalent to condition (i). Since $m_{j,j}$ is invertible, we have $\gcd(m_{j,j}, q-1) = 1$, which implies that $\gcd(2, q-1) = \gcd(2m_{j,j}, q-1) = \gcd(d_{j,j}, q-1)$. Considering q odd, we have $\gcd(2, q-1) = 2$, and the statement $2 \mid d_{i,j}$ for all $1 \leq i < j \leq n$ is equivalent to condition (ii).

□

We remark that two polynomials being *-equivalent does not mean that they have the same number of roots in \mathbb{F}_q^n . For instance, the polynomials $f(x, y, z) = 11x^{13} + 5x^{21}y^{19} + 12x^2y^3z^{17}$ and $g(x, y, z) = 11x + 5y + 12z$ are *-equivalent in $\mathbb{F}_{31}[x, y, z]$, thus $N^*(f) = 870 = N^*(g)$. However, it can be verified that $N(f) = 1861 \neq 961 = N(g)$.

Let f be a fully triangular polynomial. For any root (c_1, c_2, \dots, c_n) of f , if $c_j = 0$ and j is the smallest index that satisfies this condition, then $f(c_1, \dots, c_{j-1}, 0, c'_{j+1}, \dots, c'_n) = 0$ for any $c'_{j+1}, \dots, c'_n \in \mathbb{F}_q$. This is due to the fact that the terms involving the variables x_{j+1}, \dots, x_n vanish, thereby not impacting the value of the polynomial. Thus, by adding over the indices of the first coordinates that are equal to 0 among the roots, we derive the following identity:

$$N(f) = \begin{cases} N^*(f) + \sum_{k=1}^{n-1} N^*(f_k)q^{n-k-1}, & \text{if } b \neq 0, \\ q^{n-1} + N^*(f) + \sum_{k=1}^{n-1} N^*(f_k)q^{n-k-1}, & \text{if } b = 0. \end{cases} \quad (6)$$

Now, let f be totally *-equivalent to a polynomial g . From Lemma 1 we have that $N^*(f_k) = N^*(g_k)$ for all $1 \leq k \leq n$. Thus,

$$N(f) = \begin{cases} N^*(g) + \sum_{k=1}^{n-1} N^*(g_k)q^{n-k-1}, & \text{if } b \neq 0, \\ q^{n-1} + N^*(g) + \sum_{k=1}^{n-1} N^*(g_k)q^{n-k-1}, & \text{if } b = 0. \end{cases} \quad (7)$$

Therefore, if we know that f is totally *-equivalent to a polynomial g , and $N^*(g_k)$ is known for any k , we can substitute these values into (7) to compute $N(f)$.

For instance, let us consider the polynomials $f, g \in \mathbb{F}_{10007}[x, y]$ given by $f(x, y, z) = x^{1001} + x^{2001}y^{3001} + x^{4001}y^{5001}z^{6001} + 7001$ and $g(x, y, z) = x + y + z + 7001$. By straightforward calculation, we can verify that f is totally *-equivalent to g , so

$$\begin{aligned} N(f) &= N^*(x + y + z + 7001) + N^*(x + y + 7001) + qN^*(x + 7001) \\ &= 100110031 + 10005 + 10007 \cdot 1 \\ &= 100130043. \end{aligned}$$

3.1 Roots with non-zero coordinates for diagonal polynomials

Let g be the linear polynomial given by

$$g(x_1, \dots, x_n) = a_1x_1 + \dots + a_nx_n - b, \quad (8)$$

where $a_1, \dots, a_n \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. In this case the exact value of $N^*(g_k)$ is known, which can be substituted in (7) to compute $N(f)$ for any f polynomial $*$ -equivalent to g .

Lemma 7. *For a linear polynomial g of the form (8), the number of roots in $(\mathbb{F}_q^*)^k$ of g_k is*

$$N^*(g_k) = \begin{cases} \frac{(q-1)^k}{q} - \frac{(-1)^k}{q}, & \text{if } b \neq 0, \\ \frac{(q-1)^k}{q} - \frac{(-1)^k}{q} + (-1)^k, & \text{if } b = 0. \end{cases} \quad (9)$$

Proof. See Lemma 2 in [2]. □

In the case when f is totally $*$ -equivalent to a quadratic diagonal polynomial

$$g(x_1, \dots, x_n) = a_1 x_1^2 + \dots + a_n x_n^2 - b, \quad (10)$$

where $a_1, \dots, a_n \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, we will need a way to compute the number of roots of g_k , $1 \leq k \leq n$ in \mathbb{F}_q^* . The following result about quadratic forms is classic.

Theorem 8. *Let \mathbb{F}_q be a finite field, where q is odd, and g a polynomial as in (10). The number of roots of $g(x_1, \dots, x_n)$ in \mathbb{F}_q^n is*

$$N(g) = \begin{cases} q^{n-1} - \eta((-1)^{n/2} a_1 \dots a_n) q^{(n-2)/2}, & \text{if } n \text{ even and } b \neq 0, \\ q^{n-1} + \eta((-1)^{(n-1)/2} b a_1 \dots a_n) q^{(n-1)/2}, & \text{if } n \text{ odd and } b \neq 0, \\ q^{n-1} + \eta((-1)^{n/2} a_1 \dots a_n) (q^{n/2} - q^{(n-2)/2}), & \text{if } n \text{ even and } b = 0, \\ q^{n-1}, & \text{if } n \text{ odd and } b = 0, \end{cases} \quad (11)$$

where η is the quadratic multiplicative character in \mathbb{F}_q .

Proof. See Theorem 10.5.1 in [8]. □

We notice from this result that the number of roots only depends on the values of $\eta(a_j)$ for $1 \leq j \leq n$ and $\eta(b)$.

We also remark that Theorem 11 let us calculate $N(g_k)$ for any k . We will need the following definitions and results in order to calculate $N^*(g_k)$ for any k .

Definition 9. *Let η be the quadratic character in \mathbb{F}_q . For a coefficient vector $(a_1, a_2, \dots, a_n) \in (\mathbb{F}_q^*)^n$ let us define the following functions:*

$$r(k) = \#\{1 \leq j \leq k : \eta(a_j) = 1\}, \quad s(k) = \#\{1 \leq j \leq k : \eta(a_j) = -1\}, \quad 1 \leq k \leq n.$$

For simplicity, let us denote $r = r(n)$, $s = s(n)$.

Let us partition the set of roots of g_k in classes $A_{i,j}$ fixing the number i (respectively j) of non-zero coordinates of the roots whose corresponding coefficients are squares (respectively non-squares). For any root in $A_{i,j}$, let $\{u_1, \dots, u_{i+j}\}$ be the indices of the $i+j$ non-zero coordinates. Then the non-zero coordinates, arranged in the same order, form a root in $(\mathbb{F}_q^*)^{i+j}$ of the polynomial

$$g_{u_1, \dots, u_{i+j}} = a_{u_1} x_{u_1}^2 + \dots + a_{u_{i+j}} x_{u_{i+j}}^2 - b.$$

Let $g_{u'_1, \dots, u'_{i+j}}$ be any other polynomial of the same form with the same numbers i and j of square and non-square coefficients. It is easy to construct a bijection between the roots of $g_{u_1, \dots, u_{i+j}}$ and $g_{u'_1, \dots, u'_{i+j}}$ in \mathbb{F}_q^{i+j} , and also in $(\mathbb{F}_q^*)^{i+j}$. Thus, $N(g_{u_1, \dots, u_{i+j}})$ and $N^*(g_{u_1, \dots, u_{i+j}})$ depend only on i and j . Since the number of roots is the only information that matters to us, we will denote any such polynomial simply by $g_{i,j}$ and the quantities as $N(g_{i,j})$ and $N^*(g_{i,j})$. Thus, the number of roots in each class $A_{i,j}$ is $\binom{r(k)}{i} \binom{s(k)}{j} N^*(g_{i,j})$, and the total number of roots of g_k is

$$N(g_{r(k), s(k)}) = N(g_k) = \sum_{\substack{0 \leq i \leq r(k) \\ 0 \leq j \leq s(k)}} \binom{r(k)}{i} \binom{s(k)}{j} N^*(g_{i,j}). \quad (12)$$

The following Binomial Inversion Lemma will allow us to obtain an expression of $N^*(g_k)$ in terms of $N(g_{i,j})$.

Lemma 10. *Let G be an abelian group and $f : \mathbb{Z}_{\geq 0} \rightarrow G$ a function. Let F be the function defined by $F(r) = \sum_{i=0}^r \binom{r}{i} f(i)$, then f can be written in terms of F as*

$$f(r) = \sum_{i=0}^r (-1)^{r+i} \binom{r}{i} F(i).$$

Proof. See Section 5.3 in [11]. □

Using Lemma 10 twice in (12), it follows that

$$N^*(g_{r(k), s(k)}) = N^*(g_k) = \sum_{i=0}^{r(k)} \sum_{j=0}^{s(k)} (-1)^{r(k)+s(k)+i+j} \binom{r(k)}{i} \binom{s(k)}{j} N(g_{i,j}). \quad (13)$$

From Theorem 8, and the fact that $\eta(-1) = (-1)^{(q-1)/2}$, we obtain that

$$N(g_{i,j}) = \begin{cases} q^{i+j-1} - (-1)^j (-1)^{(q-1)(i+j)/4} q^{(i+j-2)/2}, & \text{if } i+j \text{ even and } b \neq 0, \\ q^{i+j-1} + (-1)^j (-1)^{(q-1)(i+j-1)/4} \eta(b) q^{(i+j-1)/2}, & \text{if } i+j \text{ odd and } b \neq 0, \\ q^{i+j-1} + (-1)^j (-1)^{(q-1)(i+j)/4} (q^{(i+j)/2} - q^{(i+j-2)/2}), & \text{if } i+j \text{ even and } b = 0, \\ q^{i+j-1}, & \text{if } i+j \text{ odd and } b = 0. \end{cases} \quad (14)$$

By expressing $N^*(g_k)$ in terms of $N(g_{i,j})$, we can use (14) to get an explicit value for $N^*(g_k)$, which can be used in (7) to determine $N(f)$.

Theorem 11. *Let \mathbb{F}_q be a finite field with q an odd number, g a quadratic diagonal polynomial as in (10), and $r(k)$, $s(k)$ be as in Definition 9. Let us define the complex constants*

$$\zeta_1 = (q(-1)^{(q-1)/2})^{1/2} - 1, \quad \zeta_2 = -(q(-1)^{(q-1)/2})^{1/2} - 1.$$

We have that

a) if $b \neq 0$, then

$$\begin{aligned} N^*(g_k) &= \frac{(q-1)^k}{q} - \frac{1}{2q}(\zeta_1^{r(k)}\zeta_2^{s(k)} + \zeta_2^{r(k)}\zeta_1^{s(k)}) \\ &\quad + \frac{\eta(b)}{2(q(-1)^{(q-1)/2})^{1/2}}(\zeta_1^{r(k)}\zeta_2^{s(k)} - \zeta_2^{r(k)}\zeta_1^{s(k)}). \end{aligned} \quad (15)$$

b) if $b = 0$, then

$$N^*(g_k) = \frac{(q-1)^k}{q} - \frac{q-1}{2q}(\zeta_1^{r(k)}\zeta_2^{s(k)} + \zeta_2^{r(k)}\zeta_1^{s(k)}). \quad (16)$$

Proof. Firstly, we remark that both constants ζ_1 and ζ_2 are related to the values of geometric sums. For any positive integer u , we have

$$\zeta_1^u = (-1)^u \sum_{i=0}^u \binom{u}{i} (-1)^i (q(-1)^{(q-1)/2})^{i/2}, \quad \zeta_2^u = (-1)^u \sum_{i=0}^u \binom{u}{i} (q(-1)^{(q-1)/2})^{i/2}.$$

We will now establish the proof for the scenario when $b \neq 0$ and the analogous case can be reasoned in a similar fashion. Since $b \neq 0$, (14) reduces to

$$N(g_{i,j}) = \begin{cases} q^{i+j-1} - (-1)^j (-1)^{(q-1)(i+j)/4} q^{(i+j-2)/2}, & \text{if } i+j \text{ even,} \\ q^{i+j-1} + (-1)^j (-1)^{(q-1)(i+j-1)/4} \eta(b) q^{(i+j-1)/2}, & \text{if } i+j \text{ odd,} \end{cases}$$

which can be rewritten as

$$\begin{aligned} N(g_{i,j}) &= q^{i+j-1} + \frac{(1 + (-1)^{i+j})}{2} \left(-(-1)^j (-1)^{(q-1)(i+j)/4} q^{(i+j-2)/2} \right) \\ &\quad + \frac{(1 - (-1)^{i+j})}{2} \left((-1)^j (-1)^{(q-1)(i+j-1)/4} \eta(b) q^{(i+j-1)/2} \right). \end{aligned}$$

This can be used in (13) to obtain an equation with a right-hand side that can be partitioned into geometric sums, through a straightforward computation, yields our result. \square

4 Main results

We are going to determine the number of roots of fully triangular polynomials in some cases, starting by the simplest case, when it is totally $*$ -equivalent to a linear polynomial.

Theorem 12. *Let f be a fully triangular polynomial as in (4) that is totally $*$ -equivalent to a linear polynomial g of form (8). Then,*

$$N(f) = \begin{cases} \frac{q^n - (-1)^n}{q+1}, & \text{if } b \neq 0, \\ \frac{2q^n + (-1)^n(q-1)}{q+1}, & \text{if } b = 0. \end{cases}$$

Proof. Let us consider the case where $b \neq 0$, because the other is analogous. In this case, (9) from Lemma 7 tells us $N^*(g_k) = \frac{(q-1)^k}{q} - \frac{(-1)^k}{q}$, and (7) implies $N(f) = N^*(g) + \sum_{k=1}^{n-1} N^*(g_k)q^{n-k-1}$. Therefore,

$$\begin{aligned} N(f) &= \frac{(q-1)^n}{q} - \frac{(-1)^n}{q} + \sum_{k=1}^n q^{n-k-1} \left[\frac{(q-1)^k}{q} - \frac{(-1)^k}{q} \right] \\ &= \frac{(q-1)^n}{q} - \frac{(-1)^n}{q} + q^{n-2} \left[\sum_{k=1}^n \left(\frac{q-1}{q} \right)^k + \left(\frac{-1}{q} \right)^k \right] \\ &= \frac{q^n - (-1)^n}{q+1}. \end{aligned}$$

□

We remark that notably, the number of roots in \mathbb{F}_q^n of the fully triangular polynomial f is *not* equal to the number of roots of the linear polynomial g , which is equal to q^{n-1} . We also remark that diagonal polynomials are triangular but not fully triangular, thus any result that requires f to be fully triangular cannot be used on diagonal polynomials.

Notice that the coefficient vector of the fully triangular polynomial does not affect the number of roots of fully triangular polynomials $*$ -equivalent to linear polynomials, yielding the following result:

Corollary 13. *Let f and h be two fully triangular polynomial with n variables of the form (4), such that the constant terms are zero in both of them or non-zero in both of them. If f and h are totally $*$ -equivalent to linear polynomials they have the same number of roots.*

Proof. Even when f and h have different coefficients, Theorem 12 implies that the number of roots depends only on the number of variables and also if the constant term is zero or not. □

In the following result we consider the cases when the fully triangular polynomial is totally $*$ -equivalent to a quadratic diagonal polynomial.

Theorem 14. *Let \mathbb{F}_q be a finite field with q an odd number and f be a fully triangular polynomial of the form (4). Let us suppose that f is totally $*$ -equivalent to a quadratic diagonal polynomial g of the form (10). Let ζ_1, ζ_2 be the constants as in Theorem 11. We have that*

a) *if $b \neq 0$, then*

$$\begin{aligned} N(f) &= q^{n-2}(q-1) - \frac{1}{2q} \cdot (\zeta_1^r \zeta_2^s + \zeta_2^r \zeta_1^s) + \frac{\eta(b)}{2(q(-1)^{(q-1)/2})^{1/2}} \cdot (\zeta_1^r \zeta_2^s - \zeta_2^r \zeta_1^s) \\ &\quad + \sum_{k=1}^{n-1} q^{n-k-1} \left(-\frac{1}{2q} \cdot (\zeta_1^{r(k)} \zeta_2^{s(k)} + \zeta_2^{r(k)} \zeta_1^{s(k)}) + \frac{\eta(b)}{2(q(-1)^{(q-1)/2})^{1/2}} \cdot (\zeta_1^{r(k)} \zeta_2^{s(k)} - \zeta_2^{r(k)} \zeta_1^{s(k)}) \right); \end{aligned}$$

b) if $b = 0$, then

$$\begin{aligned} N(f) &= q^{n-1} + q^{n-2}(q-1) + \left(\frac{q-1}{2q}\right)(\zeta_1^r \zeta_2^s + \zeta_2^r \zeta_1^s) \\ &\quad + \left(\frac{q-1}{2}\right) \sum_{k=1}^{n-1} q^{n-k-2} (\zeta_1^{r(k)} \zeta_2^{s(k)} + \zeta_2^{r(k)} \zeta_1^{s(k)}). \end{aligned}$$

Proof. Let us prove the result in the case when $b \neq 0$, because the other case is analogous. In this case, (15) in Theorem 14 implies

$$\begin{aligned} N^*(g_k) &= \frac{(q-1)^k}{q} - \frac{1}{2q} (\zeta_1^{r(k)} \zeta_2^{s(k)} + \zeta_2^{r(k)} \zeta_1^{s(k)}) \\ &\quad + \frac{\eta(b)}{2(q(-1)^{(q-1)/2})^{1/2}} (\zeta_1^{r(k)} \zeta_2^{s(k)} - \zeta_2^{r(k)} \zeta_1^{s(k)}), \end{aligned}$$

and from (7) we have $N(f) = N^*(g) + \sum_{k=1}^{n-1} N^*(g_k) q^{n-k-1}$. Therefore,

$$\begin{aligned} N(f) &= \frac{(q-1)^n}{q} - \frac{1}{2q} \cdot (\zeta_1^r \zeta_2^s + \zeta_2^r \zeta_1^s) + \frac{\eta(b)}{2(q(-1)^{(q-1)/2})^{1/2}} \cdot (\zeta_1^r \zeta_2^s - \zeta_2^r \zeta_1^s) \\ &\quad + \sum_{k=1}^{n-1} q^{n-k-1} \left(\frac{(q-1)^k}{q} - \frac{1}{2q} \cdot (\zeta_1^{r(k)} \zeta_2^{s(k)} + \zeta_2^{r(k)} \zeta_1^{s(k)}) + \frac{\eta(b)}{2(q(-1)^{(q-1)/2})^{1/2}} \cdot (\zeta_1^{r(k)} \zeta_2^{s(k)} - \zeta_2^{r(k)} \zeta_1^{s(k)}) \right), \end{aligned}$$

which simplifies to obtain the desired result. \square

Notice that the specific values in the vector coefficient $(a_1, a_2, \dots, a_n, -b)$ do not matter. In fact, to determine the number of roots is which of the coefficients a_j 's and b are squares or not. Thus we have the following result:

Corollary 15. *Let \mathbb{F}_q be a finite field with q an odd number. Let f and h be two fully triangular polynomial with n variables of the form (4) with coefficient vectors $(a_1, a_2, \dots, a_n, -b)$ and $(c_1, c_2, \dots, c_n, -d)$ respectively. Let us suppose that $\eta(a_1) = \eta(c_1), \dots, \eta(a_n) = \eta(c_n), \eta(b) = \eta(d)$. If f and h are totally $*$ -equivalent to quadratic diagonal polynomials, they have the same number of roots.*

Proof. The values of $r(k)$ and $s(k)$ for $1 \leq k \leq n$ will be the same for both polynomials. Hence from Theorem 15 they both have the same number of roots in \mathbb{F}_q^n . \square

Then for every choice of which coefficients in the coefficient vector we have fixed values for $r(k), s(k)$ for $1 \leq k \leq n$. We can substitute these values in Theorem 8 to find a closed expression for the number of roots. We will do this for two specific cases.

Corollary 16. *Let \mathbb{F}_q be a finite field with q an odd number and f be a fully triangular polynomial of the form (4) such that the coefficients a_1, \dots, a_n are either all squares, or are all non squares in \mathbb{F}_q . Let us suppose that f is totally $*$ -equivalent to a quadratic diagonal polynomial g of the form (10). We have that*

a) if $b \neq 0$, then

$$N(f) = q^{n-2}(q-1) - \frac{1}{2q} \cdot \left(\frac{\zeta_1^{n+1} - (q-1)\zeta_1^n - \zeta_1 q^{n-1}}{\zeta_1 - q} + \frac{\zeta_2^{n+1} - (q-1)\zeta_2^n - \zeta_2 q^{n-1}}{\zeta_2 - q} \right) \\ + \frac{\varepsilon \eta(b)}{2(q(-1)^{(q-1)/2})^{1/2}} \cdot \left(\frac{\zeta_1^{n+1} - (q-1)\zeta_1^n - \zeta_1 q^{n-1}}{\zeta_1 - q} - \frac{\zeta_2^{n+1} - (q-1)\zeta_2^n - \zeta_2 q^{n-1}}{\zeta_2 - q} \right);$$

where

$$\varepsilon = \begin{cases} 1, & \text{if } a_1, \dots, a_n \text{ are squares,} \\ -1, & \text{if } a_1, \dots, a_n \text{ are non squares.} \end{cases}$$

b) if $b = 0$, then

$$N(f) = 2q^{n-1} - q^{n-2} \\ + \frac{q-1}{2q} \left(\frac{\zeta_1^{n+1} - (q-1)\zeta_1^n - \zeta_1 q^{n-1}}{\zeta_1 - q} + \frac{\zeta_2^{n+1} - (q-1)\zeta_2^n - \zeta_2 q^{n-1}}{\zeta_2 - q} \right),$$

in both cases.

Proof. In the case when a_1, \dots, a_n are squares we have $r(k) = k$, $s(k) = 0$ for $1 \leq k \leq n$. Substituting into the expressions in Theorem 14 and computing the geometric sums yields the result.

For the case when none of the coefficients a_1, \dots, a_n is a square, we can multiply f by a non square coefficient a to obtain a polynomial with exactly the same roots, but whose coefficients aa_1, \dots, aa_n are squares, and the constant term ab is such that $\eta(ab) = -\eta(b)$. Thus in the case when $b = 0$ the number of roots is exactly the same as the all squares case, and in the case $b \neq 0$ the expression is essentially the same with a couple signs changed. \square

References

- [1] Kun Jiang, Wei Gao, Wei Cao. *Counting solutions to generalized Markoff-Hurwitz-type equations in finite fields*. Finite Fields and Their Applications, vol. 62, February 2020.
- [2] Wei Cao. *On generalized Markoff-Hurwitz-type Equations over finite fields*. Acta Applicandae Mathematicae, vol. 112, pgs. 275–281, 2010.
- [3] Ruyun Wang, Binbin Wen, Wei Cao. *Degree matrices and enumeration of rational points of some hypersurfaces over finite fields*. Journal of Number Theory, vol. 177, pgs. 91-99, 2017.
- [4] Leonard Carlitz. *Certain special equations in a finite field*. Monatshefte für Mathematik, vol. 58, pgs. 5-12, 1954.
- [5] Ioulia Baoulina. *On the number of solutions of the equation $a_1 x_1^{m_1} + \dots + a_n x_n^{m_n} = b x_1 \dots x_n$ in a finite field*. Acta Applicandae Mathematicae, vol. 85, pgs. 35-39, 2005.

-
- [6] Lei Fu, Danqing Wan. *Mirror congruence for rational points on Calabi-Yau varieties*. Asian Journal of Mathematics, vol. 10, pgs. 1-10, 2006.
 - [7] Antonio Rojas-Leon, Daqing Wan. *Moment zeta functions for toric Calabi-Yau hypersurfaces*. Communications in Number Theory and Physics, vol. 1, pgs. 539–578, 2007.
 - [8] Bruce C. Berndt, Ronald J. Evans, Kenneth S. Williams. *Gauss and Jacobi Sums*. Monographies et Études de la Société Mathématique du Canada, 1998.
 - [9] Henri Cohen. *Number Theory Volume I: Tools and Diophantine Equations*. Graduate Texts in Mathematics, Springer, 2007.
 - [10] Steven Roman. *Advanced Linear Algebra*. Graduate Texts in Mathematics, Springer, 2008.
 - [11] Ronald Graham, Donald Knuth, Oren Patashnik. *Concrete Mathematics*. 2nd ed., Addison-Wesley, 1994.
 - [12] Rudolf Lidl, Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2nd ed., 1997.