COUNTING SOLUTIONS OF SPECIAL LINEAR EQUATIONS
OVER FINITE FIELDS

LUCAS REIS

Abstract. Let $q$ be a prime power, $\mathbb{F}_q$ be the finite field with $q$ elements and $d_1, \ldots, d_k$ be positive integers. In this note we explore the number of solutions $(z_1, \ldots, z_k) \in \mathbb{F}_q^k$ of the equation

$$L_1(x_1) + \cdots + L_k(x_k) = b,$$

with the restrictions $z_i \in \mathbb{F}_{q^{d_i}}$, where each $L_i(x)$ is a non-zero polynomial of the form $\sum_{j=0}^{m_i} a_j x^{q^j} \in \mathbb{F}_q[x]$. We characterize the elements $b \in \mathbb{F}_q$ for which the equation above has a solution and, in affirmative case, we determine the exact number of solutions. As an application of our main result, we obtain the cardinality of the sumset

$$\sum_{i=1}^k \mathbb{F}_{q^{d_i}} := \{ \alpha_1 + \cdots + \alpha_k | \alpha_i \in \mathbb{F}_{q^{d_i}} \}.$$

We also discuss the existence and number of elements in $\mathbb{F}_{q^n}$ with several prescribed traces over intermediary $\mathbb{F}_q$-extensions of $\mathbb{F}_{q^n}$.

1. Introduction

Let $\mathbb{F}_q$ be the finite fields with $q$ elements, where $q$ is a prime power and let $\mathbb{F}$ be any finite extension of $\mathbb{F}_q$. Given a multivariate polynomial $f(x_1, \ldots, x_k)$ with coefficients in $\mathbb{F}_q$ and $b \in \mathbb{F}$, an interesting question is to determine the number of solutions $(z_1, \ldots, z_k) \in \mathbb{F}^k$ for the equation

$$f(x_1, \ldots, x_k) = b.$$

For generic $f$, this problem is quite challenging but some special cases have been extensively explored. For instance, $f(x_1, \ldots, x_n) = x_1^{d_1} + \cdots + x_k^{d_k}$ yield the so called diagonal equations; a major contribution for this kind of equation is given by Weil [4], who provides an implicit formula for the number of solutions in terms of Jacobi sums. Since then, many other authors studied diagonal equations; for more details, see Section 7.3 of [3] and the references therein. Another interesting example is $f(x, y) = y^n + g(x) \in \mathbb{F}_q[x, y]$ and $b = 0$ with direct connection with algebraic curves over finite fields. In fact, the later can be reduced to the case that $f(x, y)$ is irreducible in $\mathbb{F}_q[x, y]$. In this case, if the curve defined by the equation $f(x, y) = 0$ does not contain singular points, the number $N$ of solutions in $\mathbb{F}^2$ for the equation $f(x, y) = 0$ satisfies

$$|N - (Q + 1)| \leq 2g_f \sqrt{Q},$$

where $g_f$ is the genus of the curve.

Date: April 20, 2020.

2010 Mathematics Subject Classification. Primary 11D72, Secondary 12E20 and 15A03.

Key words and phrases. equations over finite fields, normal elements, linearized polynomials.
where \( g_f \) is the genus of the plane curve \( C : y^n + g(x) = 0 \) and \( Q \) is the cardinality of \( \mathbb{F} \). The latter is known as the Hasse-Weil bound (see Theorem 9.18 of [1]). For a more detailed information on counting solutions of multivariate equations over finite fields, we recommend Chapter 7 of [3].

In this paper we are interested in the case that \( f(x_1, \ldots, x_k) \) is written as \( L_1(x_1) + \cdots + L_k(x_k) \), where each \( L_i(x) \) is a non zero polynomial of the form \( \sum_{j=0}^{m_i} a_{i,j} x^j \in \mathbb{F}_q[x] \). In addition, we consider solutions \((z_1, \ldots, z_k)\) with each \( z_i \) in a specified extension \( \mathbb{F}_{q^d_i} \) of \( \mathbb{F}_q \), where \( d_1, \ldots, d_k \) are given positive integers. Of course, this is far more general than counting solutions in \( \mathbb{F}_k \) for a generic finite extension \( \mathbb{F} \) of \( \mathbb{F}_q \). In other words, for a fixed \( b \in \mathbb{F}_q \), we are interested in the number of solutions \((z_1, \ldots, z_k) \in \mathbb{F}_q^k \) for the system of equations

\[
L_1(x_1) + \cdots + L_k(x_k) = b \quad \text{and} \quad x_i^{q^{d_i}} - x_i = 0, \ 1 \leq i \leq k.
\]

The main result of this paper provides a criterion for when a generic \( b \in \mathbb{F}_q \) yield a solution for (1.1) and, in affirmative case, we determine the exact number of solutions. We observe that, if for a polynomial \( g \in \mathbb{F}_q[x] \) with \( g(x) = \sum_{i=0}^{m} a_i x^i \) we set \( L_g(x) = \sum_{i=0}^{m} a_i x^i \), then each \( L_i \) in (1.1) is written uniquely as \( L_{f_i} \) for some \( f_i \in \mathbb{F}_q[x] \). From this observation, our main result can be stated as follows.

**Theorem 1.1.** Fix \( f_1, \ldots, f_k \in \mathbb{F}_q[x] \) non zero polynomials, \( d_1, \ldots, d_k \) positive integers and \( b \in \mathbb{F}_q \). Let \( \ell \) be any positive integer that is divisible by the numbers \( d_1, \ldots, d_k \), set \( G_{\ell}(x) = \gcd \left( x^\ell - 1, \frac{f_1(x)(x^{\ell-1})}{x^{\ell-1}}, \ldots, \frac{f_k(x)(x^{\ell-1})}{x^{\ell-1}} \right) \) and \( H_{\ell}(x) = x^{\ell-\deg(G_{\ell}(x))} \). For a polynomial \( f \in \mathbb{F}_q[x] \) with \( f(x) = \sum_{i=0}^{m} a_i x^i \), write \( L_f(x) = \sum_{i=0}^{m} a_i x^i \). Then the equation

\[
L_{f_1}(x_1) + \cdots + L_{f_k}(x_k) = b,
\]

has a solution \((z_1, \ldots, z_k) \in \mathbb{F}_q^k \) with the restrictions \( z_i \in \mathbb{F}_{q^{d_i}} \) if and only if

\[
L_{H_{\ell}}(b) = 0.
\]

In this case, the number of such solutions equals \( q^{d_1 + \cdots + d_k - \deg(H_{\ell}(x))} \).

Theorem 1.1 entails the following result in sumsets over finite fields.

**Corollary 1.2.** Fix \( k > 1 \) and \( d_1, \ldots, d_k \) positive integers. The number of solutions of

\[
x_1 + \cdots + x_k = 0,
\]

with the restrictions \( x_i \in \mathbb{F}_{q^{d_i}} \), equals \( q^{d_1 + \cdots + d_k - \lambda(d_1, \ldots, d_k)} \), where

\[
\lambda(d_1, \ldots, d_k) := d_1 + d_2 + \cdots + d_k + \sum_{j=2}^{k} (-1)^{j+1} \sum_{1 \leq i_1 < \cdots < i_j \leq k} \gcd(d_{i_1}, \ldots, d_{i_j}).
\]

In particular, the sumset \( \sum_{i=1}^{k} \mathbb{F}_{q^{d_i}} := \{ \alpha_1 + \cdots + \alpha_k \mid \alpha_i \in \mathbb{F}_{q^{d_i}} \} \), has cardinality \( q^{\lambda(d_1, \ldots, d_k)} \).

**Remark 1.3.** In contrast to the character sum methods that are frequently used when studying equations \( f(x_1, \ldots, x_n) = 0 \) (that, in general, do not provide exact results), we use a very elementary approach. Our method relies on considering the generating property of normal elements over finite fields, the linear structure of linearized polynomials \( \sum_{j=0}^{m} a_j x^j \) and the arithmetic of the polynomial ring \( \mathbb{F}_q[x] \).
Definition 2.1. (1) For a polynomial \( f \in \mathbb{F}_q[x] \) with \( f(x) = \sum_{i=0}^{m} a_i x^i \), the polynomial \( L_f(x) := \sum_{i=0}^{m} a_i x^{q^i} \) is the \( q \)-associate of \( f(x) \).
(2) Fix a positive integer. An element \( \beta \in \mathbb{F}_{q^n} \) is normal over \( \mathbb{F}_q \) if the elements \( \beta, \beta^q, \ldots, \beta^{q^{n-1}} \) form a basis for \( \mathbb{F}_{q^n} \) as an \( \mathbb{F}_q \)-vector space.

The existence of normal elements is known for any extension \( \mathbb{F}_{q^n} \) of \( \mathbb{F}_q \). The following lemma provides some basic properties of the \( q \)-associate of polynomials over \( \mathbb{F}_q \). Its proof is straightforward so we omit details.

Lemma 2.2. For any \( f, g \in \mathbb{F}_q[x] \), we have that \( L_{f+g}(x) = L_f(x) + L_g(x) \) and \( L_f(L_g(x)) = L_{fL_g}(x) \). In particular, if \( f \) divides \( g \), then \( L_f \) divides \( L_g \).

We emphasize that Lemma 2.2 will be frequently used along the way. Let \( C(n) \) denote the set of polynomials over \( \mathbb{F}_q \) that are either constant or has degree at most \( n - 1 \). We observe that \( C(n) \) is an \( n \)-dimensional \( \mathbb{F}_q \)-vector space and can be seen as the simplest presentation of the quotient ring \( \mathbb{F}_q[x]/\langle x^n-1 \rangle \); this fact will be further used.

We see that normal elements can be used to generate finite fields using sets \( C(n) \), as follows.

Lemma 2.3. Fix a positive integer and \( \beta \in \mathbb{F}_{q^n} \) a normal element. Then any \( \alpha \in \mathbb{F}_{q^n} \) is written uniquely as \( L_f(\beta) \) for some \( f \in C(n) \).

Proof. This follows directly from the assumption that \( \{ \beta, \beta^q, \ldots, \beta^{q^{n-1}} \} \) is an \( \mathbb{F}_q \)-basis for \( \mathbb{F}_{q^n} \).

We observe that, for \( \alpha \in \mathbb{F}_q \), \( L_{x^n-1}(\alpha) = 0 \) if and only if \( \alpha^n - \alpha = 0 \), i.e., \( \alpha \in \mathbb{F}_{q^n} \). In particular, from Lemma 2.2 the set \( I_n := \{ h \in \mathbb{F}_q[x] \mid L_h(\alpha) = 0 \} \) is a non zero ideal of \( \mathbb{F}_q[x] \), hence is generated by a polynomial \( m_{\alpha,q}(x) \in \mathbb{F}_q[x] \), which we can suppose to be monic.

Definition 2.4. For \( \alpha \in \mathbb{F}_q \), \( m_{\alpha,q} \) is the \( \mathbb{F}_q \)-order of \( \alpha \).

In particular, from definition, \( \alpha \in \mathbb{F}_{q^n} \) if and only if \( m_{\alpha,q} \) divides \( x^n - 1 \). From this observation and Lemma 2.3 the following corollary is straightforward.

Corollary 2.5. An element \( \beta \in \mathbb{F}_{q^n} \) is normal over \( \mathbb{F}_q \) if and only if \( m_{\beta,q}(x) = x^n - 1 \).

The following lemma displays the \( \mathbb{F}_q \)-order of \( \alpha = L_h(\beta) \) from the \( \mathbb{F}_q \)-order of \( \beta \).
Lemma 2.6. Let \( \beta \in \mathbb{F}_q \) and fix \( g \in \mathbb{F}_q[x] \). If \( \alpha = L_q(\beta) \), then
\[
m_{\alpha,q}(x) = \frac{m_{\beta,q}(x)}{\gcd(m_{\beta,q}(x), g(x))}.
\]

Proof. Set \( h(x) = \frac{m_{\beta,q}(x)}{\gcd(m_{\beta,q}(x), g(x))} \). In particular, \( g \cdot h \) is divisible by \( m_{\beta,q} \), hence \( L_h(\alpha) = L_q(h(\beta)) = 0 \) and so \( m_{\alpha,q}(x) \) divides \( h(x) \). If it divides strictly, there exists a nontrivial divisor \( f \) of \( h(x) \) such that \( \frac{L_{h(x)}(\alpha)}{L_{h(x)}} = 0 \), hence \( L_H(\beta) = 0 \), where \( H(x) = g(x) \cdot \frac{h(x)}{f(x)} \). In particular, \( m_{\beta,q} \) divides \( H \) or, equivalently, \( f \) divides \( \frac{g(x)}{\gcd(m_{\beta,q}(x), g(x))} \). However, from construction, the polynomials \( g(x) \gcd(m_{\beta,q}(x), g(x)) \) and \( h(x) \) are relatively prime and so they cannot have \( f \) as a common divisor. \( \square \)

From Lemmas 2.6 and 2.7 we have the following corollary.

Corollary 2.7. Fix \( n \) a positive integer, \( m \) a divisor of \( n \) and \( \beta \in \mathbb{F}_q^n \) a normal element. Then the elements of \( \mathbb{F}_q^m \) are written uniquely as \( \frac{x}{\gcd(x,m)} \) with \( h \in \mathbb{C}(m) \).

Proof. Fix \( \alpha \in \mathbb{F}_q^m \). From Lemma 2.7, there exists a unique \( H \in \mathbb{C}(n) \) such that \( \alpha = L_H(\beta) \). Since \( \beta \) is normal, \( m_{\beta,q}(x) = x^n - 1 \). From Lemma 2.6, \( m_{\alpha,q}(x) = \frac{x^n - 1}{\gcd(x^n - 1, H(x))} \). But \( \alpha \in \mathbb{F}_q^m \), hence \( m_{\alpha,q}(x) \) divides \( x^m - 1 \), i.e., \( \gcd(x^n - 1, H(x)) \) is divisible by \( \frac{x^m - 1}{x^n - 1} \). The latter implies that \( H(x) = \frac{x^n - 1}{x^m - 1} \cdot h(x) \). Since \( H \) is unique and \( H \in \mathbb{C}(n) \), we have that \( h \) is unique and \( h \in \mathbb{C}(m) \). \( \square \)

The following theorem provides the main auxiliary result of this paper.

Theorem 2.8. Fix \( n \) a positive integer, \( f(x) \) a divisor of \( x^n - 1 \) and \( \alpha \in \mathbb{F}_q \). If \( \beta \in \mathbb{F}_q^n \) is a normal element, then there exists a polynomial \( g \in \mathbb{F}_q[x] \) such that \( L_{f,g}(\beta) = \alpha \) if and only if \( m_{\alpha,q}(x) \) divides \( \frac{x^n - 1}{f(x)} \) or, equivalently, \( L_{x^n - 1}(\alpha) = 0 \).

Proof. The “only if part” follows directly from Lemma 2.6. For the “if part,” suppose that \( m_{\alpha,q}(x) \) divides \( \ell(x) = \frac{x^n - 1}{f(x)} \). But, \( \alpha \in \mathbb{F}_q^m \) is a normal element. From Lemma 2.7, there exists \( F \in \mathbb{C}(n) \) such that \( \alpha = L_F(\beta) \). But, from Lemma 2.6, \( m_{\alpha,q}(x) = \frac{x^n - 1}{\gcd(x^n - 1, F(x))} \). Therefore, \( f(x) \) divides \( \gcd(x^n - 1, F(x)) \), i.e., \( F = fg \) for some \( g \in \mathbb{F}_q[x] \). In other words, \( \alpha = L_{f,g}(\beta) \). \( \square \)

3. PROOF OF THE MAIN RESULT

Fix \( b \in \mathbb{F}_q \), \( d_1, \ldots, d_k \) positive integers and \( f_1, \ldots, f_k \in \mathbb{F}_q[x] \) non zero polynomials. Let \( \ell \) be any integer divisible by \( d_1, \ldots, d_k \) and fix \( \beta \in \mathbb{F}_q^\ell \) a normal element (over \( \mathbb{F}_q \)). In particular, \( \mathbb{F}_q^{d_i} \subseteq \mathbb{F}_q^\ell \) for any \( 1 \leq i \leq k \). For any \( (z_1, \ldots, z_k) \in \prod_{i=1}^k \mathbb{F}_q^{d_i} \), Corollary 2.7 entails that there exist a unique \( k \)-tuple \( (h_1, \ldots, h_k) \in \prod_{i=1}^k \mathbb{C}(d_i) \) such that \( z_i = L_{h_i(z_i)^{x^i - 1}}(\beta) \). In particular, if we set \( \varphi : \prod_{i=1}^k \mathbb{F}_q^{d_i} \rightarrow \mathbb{F}_q^\ell \) with
\[
(z_1, \ldots, z_k) \mapsto L_{f_1}(z_1) + \cdots + L_{f_k}(z_k),
\]
\(\varphi_\beta\) is an \(F_q\)-linear map between \(F_q\)-vector spaces with image set \(S_\beta\) equals \(\{L_h(\beta) \mid h \in S\}\), where

\[
S = \left\{ \sum_{i=1}^{k} \frac{f_i(x)(x^\ell - 1)}{x^{d_i} - 1}, h_i(x) \mid h_i \in C(d_i) \right\}.
\]

We observe that, since \(L_{x^\ell - 1}(\beta) = \beta^{q^\ell} - \beta = 0\), we have that \(S_\beta = \{L_h(\beta) \mid h \in S'\}\), where

\[
S' = \left\{ h(x) \cdot (x^\ell - 1) + \sum_{i=1}^{k} \frac{f_i(x)(x^\ell - 1)}{x^{d_i} - 1}, h_i(x) \mid h, h_i \in \mathbb{F}_q[x] \right\},
\]

is the ideal of \(\mathbb{F}_q[x]\) generated by the polynomials \(\frac{f_i(x)(x^\ell - 1)}{x^{d_i} - 1}\) and the polynomial \(x^\ell - 1\). Since \(\mathbb{F}_q[x]\) is an Euclidean Domain, such ideal is generated by the polynomial

\[
G_\ell(x) = \gcd \left( x^\ell - 1, \frac{f_1(x)(x^\ell - 1)}{x^{d_1} - 1}, \ldots, \frac{f_k(x)(x^\ell - 1)}{x^{d_k} - 1} \right).
\]

In particular, \(S_\beta = \{L_h(\beta) \mid h \in S^*\}\), where

\[
S^* = \{g(x) \cdot G_\ell(x) \mid g \in C(\ell - \deg(G_\ell(x)))\}.
\]

Therefore, the equation

\[
L_{f_1}(x_1) + \cdots + L_{f_k}(x_k) = b,
\]

has a solution \((z_1, \ldots, z_k) \in \mathbb{F}_q^k\) with the restrictions \(z_i \in \mathbb{F}_{q^{d_i}}\) if and only if \(b\) is of the form \(L_g(x)G_\ell(x)(\beta)\) for some \(g(x) \in \mathbb{F}_q[x]\). From Theorem 2.8 the later holds if and only if \(L_{H_\ell}(b) = 0\), where \(H_\ell(x) = \frac{G_\ell(x)}{\gcd(G_\ell(x))}\). For the number of solutions, we observe that such number coincides with the number of solutions for \(b = 0\). In this case, we are just looking at the kernel of \(\varphi_\beta\), which is an \(\mathbb{F}_q\)-vector space so it suffices to compute its dimension. We have seen that the image set of \(\varphi_\beta\) comprises the roots of \(L_{H_\ell}(y) = 0\) that lie in \(\mathbb{F}_q\). Since \(H_\ell\) divides \(x^\ell - 1\), \(H_\ell(0) \neq 0\). By a direct computation we see that the formal derivative of \(L_{H_\ell}\) equals \(H_\ell(0)\), hence \(L_{H_\ell}\) is a separable polynomial. In addition, since \(H_\ell\) divides \(x^\ell - 1\), Lemma 2.2 entails that all the roots of \(L_{H_\ell}(y) = 0\) lie in \(\mathbb{F}_q\). Therefore, the image set of \(\varphi_\beta\) has exactly \(\deg(L_{H_\ell}(x)) = q^{\deg(H_\ell(x))}\) elements and so it comprises an \(\mathbb{F}_q\)-vector space of dimension \(\deg(H_\ell(x))\). The Rank-Nullity Theorem entails that the kernel of \(\varphi_\beta\) is an \(\mathbb{F}_q\)-vector space with dimension \(\sum_{i=1}^{k} d_i - \deg(H_\ell(x))\), hence it has cardinality \(q^{d_1 + \cdots + d_k - \deg(H_\ell(x))}\).

3.1. Proof of Corollary 1.2. Let \(\ell\) be the least common multiple of the numbers \(d_1, \ldots, d_k\). We observe that Theorem 1.1 applies to Corollary 1.2 by setting \(f_i(x) = 1 \in \mathbb{F}_q\). In particular, the number of solutions of

\[
(3.1) \quad x_1 + \cdots + x_k = 0,
\]

with the restrictions \(x_i \in \mathbb{F}_{q^{d_i}}\) equals \(q^{d_1 + \cdots + d_k - \deg(H_\ell(x))}\), where

\[
H_\ell(x) = (x^\ell - 1)\gcd \left( x^\ell - 1, \frac{(x^\ell - 1)}{x^{d_1} - 1}, \ldots, \frac{(x^\ell - 1)}{x^{d_k} - 1} \right) = \operatorname{lcm}(x^{d_1} - 1, \ldots, x^{d_k} - 1).\]
Since \( \gcd(x^a - 1, x^b - 1) = x^{\gcd(a,b)} - 1 \) and \( \text{lcm}(x^a - 1, x^b - 1) = \frac{(x^a-1)(x^b-1)}{\gcd(x^a-1,x^b-1)} \) for any positive integers \( a, b \), by a simple Inclusion-Exclusion argument, we see that
\[
\text{lcm}(x^{d_1-1}, \ldots, x^{d_k-1}) = \prod_{i=1}^{k} x^{d_i-1} \]
and so the number of solutions of Eq. (3.1) equals
\[
q^{d_1} + \cdots + d_k - \lambda(d_1, \ldots, d_k).
\]
We proceed to the formula regarding the cardinality of the sumset
\[
S = \sum_{i=1}^{k} F_{q^{d_i}} := \{ \alpha_1 + \cdots + \alpha_k \mid \alpha_i \in F_{q^{d_i}} \}.
\]
This follows easily from the previous enumeration formula and the Rank-Nullity Theorem for the \( F_q \)-linear map \( \varphi : \prod_{i=1}^{k} F_{q^{d_i}} \to S \) given by
\[
(\alpha_1, \ldots, \alpha_k) \mapsto \sum_{i=1}^{k} \alpha_i.
\]

4. On Elements with Several Prescribed Traces

In this section, we consider a special class of system of linear equations over finite fields involving trace functions. We recall that, for a positive integer \( n > 1 \) and a divisor \( m < n \) of \( n \), the trace mapping \( \text{Tr}_{n/m} : F_{q^n} \to F_{q^m} \) is given by
\[
\alpha \mapsto \sum_{j=0}^{n/m-1} \alpha^q^{mj} = L_{T_{n,m}}(\alpha),
\]
where \( T_{n,m}(x) := x^{\frac{n}{m}-1} \).

Given a \( k \)-tuple \( (d_1, \ldots, d_k) \) of distinct divisors of \( n \) and \( (\beta_1, \ldots, \beta_k) \in \prod_{i=1}^{k} F_{q^{d_i}} \), we may ask if there is any element \( \alpha \in F_{q^n} \) such that \( \text{Tr}_{n/d_i}(\alpha) = \beta_i \). In other words, we are looking at solutions to the following system of equations:
\[
L_{T_{n,d_i}}(x) = \beta_i, \quad 1 \leq i \leq k.
\]

It is direct to verify that the trace function is transitive, i.e., \( \text{Tr}_{n/m}(\text{Tr}_{m/l}(x)) = \text{Tr}_{n/l}(x) \) whenever \( m \) divides \( n \) and \( l \) divides \( m \). In particular, if the system of equations above has a solution \( z \in F_{q^n} \), then
\[
\text{Tr}_{d_i/gcd(d_i,d_j)}(\beta_i) = \text{Tr}_{d_j/gcd(d_i,d_j)}(\beta_j), \quad 1 \leq i, j \leq k.
\]
Therefore, a necessary condition for the system above to have a solution is that Eq. (4.1) holds. In the following theorem, we show that such condition is also sufficient and we obtain the exactly number of solutions.

**Theorem 4.1.** Let \( n > 1 \) be a positive integer and let \( d_1, \ldots, d_k \) be distinct divisors of \( n \). Fix \( (\beta_1, \ldots, \beta_k) \in \prod_{i=1}^{k} F_{q^{d_i}} \), and consider the following system of equations:
\[
\text{Tr}_{n/d_i}(x) = \beta_i, \quad 1 \leq i \leq k,
\]
where $\text{Tr}_{d_i/\gcd(d_i,d_j)}(\beta_i) = \text{Tr}_{d_i/\gcd(d_i,d_j)}(\beta_j)$ for any $1 \leq i < j \leq k$. Then Eq. (4.2) has exactly $q^{n-\lambda(d_1,\ldots,d_k)}$ solutions, where

$$
\lambda(d_1,\ldots,d_k) = \sum_{j=1}^{k} (-1)^{j+1} \sum_{1 \leq i_1 < \cdots < i_j \leq k} \gcd(d_{i_1},\ldots,d_{i_j}).
$$

Proof. Fix $\beta \in \mathbb{F}_{q^n}$ a normal element. Since $\beta_i \in \mathbb{F}_{q^{d_i}}$, Corollary 2.7 entails that there exist unique $h_i \in \mathcal{C}(d_i)$ such that $\beta_i = L_{x^{d_i}-1} h_i(x)$ (mod $F$). Moreover, an arbitrary element of $\mathbb{F}_{q^n}$ is of the form $L_F(\beta)$ with $F \in \mathcal{C}(n)$. In particular, since $L_F(\beta) = 0$ if and only if $T(x) \equiv 0$ (mod $x^n - 1$), Eq. (4.2) is equivalent to the following system of congruences in $\mathbb{F}_q[x]$

$$
F(x) \cdot \frac{x^n - 1}{x^{d_i} - 1} \equiv h_i(x) \pmod{x^{d_i} - 1},
$$

The previous system is equivalent to

$$
F(x) \equiv h_i(x) \pmod{x^{d_i} - 1}, \quad 1 \leq i \leq k.
$$

From hypothesis, $\text{Tr}_{d_i/\gcd(d_i,d_j)}(\beta_i) = \text{Tr}_{d_i/\gcd(d_i,d_j)}(\beta_j)$ for any $1 \leq i < j \leq k$ and this can be rewritten as

$$
\frac{x^n - 1}{x^{\gcd(d_i,d_j)} - 1} \cdot h_i(x) \equiv \frac{x^n - 1}{x^{\gcd(d_i,d_j)} - 1} \cdot h_j(x) \pmod{x^n - 1}, \quad 1 \leq i < j \leq k.
$$

or, equivalently

$$
h_i(x) \equiv h_j(x) \pmod{x^{\gcd(d_i,d_j)} - 1}, \quad 1 \leq i < j \leq k.
$$

From the previous equalities, the Chinese Remainder Theorem entails that Eq. (4.3) has exactly one solution $F(x) = F_0(x)$ modulo $L(x) := \gcd(x^{d_1} - 1,\ldots,x^{d_k} - 1)$ and any other solution is of the form $F_0(x) + L(x) \cdot M(x)$ with $M \in \mathbb{F}_q[x]$. We have seen that $L(x)$ has degree

$$
\lambda(d_1,\ldots,d_k) = \sum_{j=1}^{k} (-1)^{j+1} \sum_{1 \leq i_1 < \cdots < i_j \leq k} \gcd(d_{i_1},\ldots,d_{i_j}).
$$

We observe that our only restriction for Eq. (4.3) is $F \in \mathcal{C}(n)$ and so we conclude that we have exactly $q^{n-\lambda(d_1,\ldots,d_k)}$ distinct solutions for Eq. (4.2).

Acknowledgements. The author was supported by FAPESP 2018/03038-2, Brazil.

References

[1] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, Algebraic curves over a finite field, Princeton Univ. Press, 2008.

[2] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press New York, NY, USA 1986.

[3] G.L. Mullen and D. Panario, Handbook of Finite Fields, Taylor and Francis, Boca Raton, 2013.
[4] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497-508.

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte MG (Brazil), 30123-970

E-mail address: lucasreismat@mat.ufmg.br