On the Factorization of Polynomials of the Form $cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}[x]$

Kondwani Magamba[1,2] **and John A. Ryan**[3]

[1]Mzuzu University, Mzuzu, Malawi
[2]Malawi University of Science and Technology, Thyolo, Malawi
[3]Chombe Boole Research Center, Rumphi, Malawi

Abstract

Let n, $r \geq 3$ and s be positive integers where $s \mid nr$. Also, let $\mathbb{F}_{q^n}$ be a finite field with characteristic p. We count the number of irreducible factors of degree r in the factorization of polynomials of the form $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}[x]$ where $ad - bc \neq 0$.

1 Introduction

The polynomial $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_q[x]$ arises in different contexts. For example, in [2], normal and self-dual normal bases are constructed from the factorization of $cx^{q+1} + dx^q - ax - b$ over $\mathbb{F}_q$. In [9], the polynomial $F_s(x)$ crops up in the study of the set $\mathcal{N}_p$ of positive integers which occur as the orders of non-singular derivations of finite-dimensional non-nilpotent Lie algebras of prime characteristic p. Our interest in the factorization of $F_s(x)$ stems from the enumeration of extended and non-extended irreducible Goppa codes. The factorization of polynomials of the form $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_q[x]$ has been covered by a number of papers see [2], [3], [5], [6], [9],[12] and [15]. In [5], Garefalakis uses the action of the general linear group $GL(2, q)$ on irreducible polynomials over $\mathbb{F}_q$ to obtain an explicit formula for the number of irreducible polynomials of a given degree r in the factorization of $x^{q^s} - ax - b \in \mathbb{F}_q[x]$. In [15], Stichtenoth and Topuzoğlu obtain an asymptotic formula on the number of irreducible polynomials in the factorization of $cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_q[x]$ by exploiting the action of the projective linear group $PGL(2, q)$ on non-linear irreducible polynomials over $\mathbb{F}_q$. The polynomial $cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_q[x]$ was also considered in [12] where a complete factorization is obtained using the theory of linearized polynomials.

In this paper, we count the number of irreducible factors of degree r in the factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}[x]$ where $s \mid nr$ and n and $r \geq 3$ are positive integers. The enumeration formulas in [5] only cover matrices whose eigenvalues lie in $\mathbb{F}_q$, our results also cover matrices with eigenvalues in $\mathbb{F}_{q^2}$. Now, since $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ and this paper considers the factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}[x]$ we obtain a generalization of the factorization of $F_s(x)$.

2 Preliminaries

2.1 Some results from polynomial factorization

In this section we state some results from polynomial factorization which we will use.

Theorem 2.1. *[7] Let $v \geq 2$ be an integer and $\beta \in \mathbb{F}_q^*$. Then the binomial $x^v - \beta$ is irreducible in $\mathbb{F}_q[x]$ if and only if the following two conditions are satisfied:*

1. *each prime factor of v divides the order e of β in $\mathbb{F}_q^*$ but not $\frac{q-1}{e}$;*
2. *$q \equiv 1 \pmod 4$ if $v \equiv 0 \pmod 4$.*

Theorem 2.2. *[2] Let $\xi \in \mathbb{F}_q^*$ with multiplicative order v. Then the following factorization over $\mathbb{F}_q$ is complete:*

$$x^{q-1} - \xi = \prod_{j=1}^{\frac{q-1}{v}} (x^v - \beta_j)$$

where β_j runs through the distinct roots of $x^{\frac{q-1}{v}} - \xi$ in $\mathbb{F}_q$.

Theorem 2.3. *[2] For $a, b, c, d \in \mathbb{F}_q$ with $c \neq 0$, $ad - bc \neq 0$ and $\Delta = (a-d)^2 + 4bc \neq 0$ being a quadratic residue in $\mathbb{F}_q$, the following factorization over $\mathbb{F}_q$ is complete:*

$$cx^{q+1} + dx^q - ax - b = (x - x_0)(x - x_1) \prod_{j=1}^{\frac{q-1}{t}} \frac{1}{1 - \beta_j} \left[(x - x_0)^t - \beta_j (x - x_1)^t\right],$$

where $x_0, x_1 \in \mathbb{F}_q$ are the two distinct roots of $cx^2 + (d-a)x - b = 0$, t is the multiplicative order of $\xi = \frac{a - cx_1}{a - cx_0}$ and β_j is a root of $x^{\frac{q-1}{t}} - \xi$ in $\mathbb{F}_q$.

Theorem 2.4. *[2] For $a, b, c, d \in \mathbb{F}_q$ with $c \neq 0$, $ad - bc \neq 0$ and $\Delta = (a-d)^2 + 4bc \neq 0$ being a quadratic nonresidue in $\mathbb{F}_q$, the following factorization over $\mathbb{F}_q$ is complete:*

$$cx^{q+1} + dx^q - ax - b = \prod_{j=1}^{\frac{q+1}{t}} \frac{1}{1 - \beta_j} \left[(x - x_0)^t - \beta_j (x - x_1)^t\right],$$

where $x_0, x_1 \in \mathbb{F}_{q^2}$ are the two distinct roots of $cx^2 + (d-a)x - b = 0$, t is the multiplicative order of $\xi = \frac{a - cx_1}{a - cx_0}$ and β_j is a root of $x^{\frac{q+1}{t}} - \xi$ in $\mathbb{F}_{q^2}$.

Theorem 2.5. *[7] Let $a \in \mathbb{F}_q$ and p be the characteristic of $\mathbb{F}_q$. Then the trinomial $x^p - x - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if $Tr_{\mathbb{F}_q}(a) \neq 0$.*

Theorem 2.6. *[7] For $x^{q^{nr}} - x - \beta$, with β an element of a subfield $\mathbb{F}_s$ of $\mathbb{F}_{q^{nr}}$ we have the following decomposition*

$$x^{q^{nr}} - x - \beta = \prod_{j=1}^{q^{nr}/s} (x^s - x - \gamma_j)$$

where γ_j runs through all the distinct elements of $\mathbb{F}_{q^{nr}}$ with trace $Tr_{\mathbb{F}_{q^{nr}}/\mathbb{F}_s}(\gamma_j) = \beta$.

2.2 Elements of degree r over $\mathbb{F}_{q^n}$

We are interested in counting the number of irreducible factors of degree r in the factorization of $F_s(x)$, so in this section we discuss where elements of degree r lie. We begin with the following definition.

Definition 2.1. The set $\mathbb{S} = \mathbb{S}(n, r)$ is the set of all elements in $\mathbb{F}_{q^{nr}}$ of degree r over $\mathbb{F}_{q^n}$.

Recall that $s \mid nr$. In analysing the factorization of $F_s(x)$ we will make use of the following factorizations of n and r. We define k to be the largest divisor of n that is relatively prime to r and set $\ell_n = \frac{n}{k}$. We will also define m to be the largest divisor of r that is relatively prime to n and set $\ell_r = \frac{r}{m}$. We see that $nr = k\ell_n\ell_r m = k\ell m$ where $\ell = \ell_n\ell_r$. In addition to this, the notation k_1 will be used to mean a divisor of k and we will write $\bar{k}_1 = \frac{k}{k_1}$ etc. With these factorizations of n and r we obtain the following characterization of the elements of $\mathbb{S}$, see [14].

Theorem 2.7. $\mathbb{S}$ contains elements of $\mathbb{F}_{q^{nr}}$ which are roots of irreducible polynomials of degree r over $\mathbb{F}_{q^{k_1\ell_n}}$. Thus, elements of $\mathbb{S}$ lie in subfields of $\mathbb{F}_{q^{nr}}$ of the form $\mathbb{F}_{q^{k_1\ell_n r}}$, for some k_1, but not in any subfield of the form $\mathbb{F}_{q^w}$ where w is not divisible by $\ell_n r$.

For convenience, we will write $n_1 = k_1\ell_n$ and note that $\bar{n}_1 = \frac{n}{n_1} = \bar{k}_1$ and that $(\bar{n}_1, r) = 1$. With this notation we can define, more generally, $\mathbb{S}(n_1, r)$ to be the subset of $\mathbb{S}(n, r)$ of elements that are of degree r over $\mathbb{F}_{q^{n_1}}$.

Now, suppose that $F_s(\alpha) = 0$, where α is an element of order r over $\mathbb{F}_{q^n}$. Then $\alpha^{q^s} = \frac{a\alpha+b}{c\alpha+d}$. We see that if e is the smallest integer such that $\alpha^{q^{es}} = \alpha$, then $e = \bar{\ell}_1\bar{m}_1$ since $s \times \bar{\ell}_1\bar{m}_1 = k_1\ell_1 m_1 \times \frac{\ell}{\ell_1} \times \frac{m}{m_1} = k_1\ell m = k_1\ell_n r = n_1 r$. A natural question that comes up at this point is the form that the right hand side of the equation $\alpha^{q^s} = \frac{a\alpha+b}{c\alpha+d}$ takes when the left hand side is $\alpha^{q^{sk}}$ where k is a positive integer. We address this in the next section.

2.3 Order of a matrix

Recall that $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}$ where $ad - bc \neq 0$. Thus we can take the coefficients $a, b, c, d \in \mathbb{F}_{q^n}$ as entries of a 2×2 non-singular matrix A over $\mathbb{F}_{q^n}$. That is, $A \in GL(2, q^n)$. This enables us to write $\alpha^{q^s} = \frac{a\alpha+b}{c\alpha+d}$ in the form $\alpha^{q^s} = [A](\alpha)$, where $[A](\alpha) = \frac{a\alpha+b}{c\alpha+d}$.

Now, $\alpha^{q^{2s}} = [A]([A](\alpha)) = [A^2](\alpha)$. So by induction we obtain, $\alpha^{q^{sk}} = [A^k](\alpha)$ and if D is the smallest positive integer such that $\alpha^{q^{sD}} = \alpha$ then $\alpha^{q^{sD}} = [A^D](\alpha) = \alpha = [I_2](\alpha)$, where I_2 is the 2×2 identity matrix. Thus $A^D = I_2$ and the order of $A \in GL(2, q^n)$ divides D. We claim that the order of A is D. Suppose the order of A is d, where d is a non-trivial divisor of D. Then $\alpha^{q^{sd}} = [A^d](\alpha) = [I_2](\alpha) = \alpha$. This implies that $\alpha \in \mathbb{F}_{q^{sd}}$ contrary to the fact that D is the least positive integer such that $\alpha \in \mathbb{F}_{q^{sD}}$. Hence the order of A is D. From the previous section, we know that $D = \bar{\ell}_1\bar{m}_1$. We have proved the following.

Lemma 2.1. *Suppose $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}$ where $ad - bc \neq 0$ and $F_s(\alpha) = 0$ where α is an element of degree r over $\mathbb{F}_{q^n}$. Then $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, q^n)$ of order $D = \bar{\ell}_1\bar{m}_1$.*

Clearly, matrices of a given order will play an important role in the factorization of $F_s(x)$. The following theorem gives the relationship between the order of a matrix D, the characteristic of the field and the form that A takes, see [8].

Theorem 2.8. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, q^n)$ *be of order* D *and* $\mathbb{F}_{q^n} = \mathbb{F}_{p^{nt}}$. *Then:*

i. If $D = 1$, *then* A *is similar to a matrix of the form* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

ii. If $D = p^i$, *where* $i \geq 1$, *then* A *is similar to a matrix of the form* $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, *where* $b \neq 0 \in \mathbb{F}_{q^n}$.

iii. If $(p, D) = 1$, $D \mid (q^n - 1)$ *and* A *is not a multiple of* I_2, *then* A *is similar to a matrix of the form* $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, *where* $a \in \mathbb{F}_{q^n} - \{0, 1\}$.

iv. If $(p, D) = 1$ *and* $D \mid (q^n + 1)$ *but* $D \nmid (q^n - 1)$, *then* A *is similar to a matrix of the form* $\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}$ *where* $c, d \in \mathbb{F}_{q^n}$ *and* $c \neq 0$.

Corollary 2.1. *The order of* $A \in GL(2, q^n)$ *divides* $p(q^n - 1)$ *or* $(q^n-)(q^n + 1)$.

Example 2.1. *Let's take* $q = 2$, $n = 5$ *and* $r = 6$. *Suppose we want to factorize* $F_{10}(x) = cx^{2^{10}+1} + dx^{q^{10}} - ax - b$. *Now, if* α *is a root of* $F_{10}(x)$, *then* $\alpha^{2^{10}} = \frac{a\alpha+b}{c\alpha+d}$. *We see that* $D = 3$ *and* $3 \mid (2^5 + 1)$. *So we may take* $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in GL(2, 2^5)$. *Hence, we consider the factorization of* $F_{10}(x) = x^{2^{10}+1} + x^{2^{10}} - 1$.

3 Factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}[x]$

In this section we consider the factorization of the polynomials $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}$ where $s = k_1\ell_1 m_1$. We find the number of irreducible factors of degree r in the factorization of $F_s(x)$. We begin our discussion by looking at the positive integer s.

By definition $s \mid nr$ and we use $s = k_1\ell_1 m_1$ to obtain all factors of nr. We want to break s into a product of factors of n and factors of r. Suppose we can find a positive integer t such that $\mathbb{F}_{q^t} = \mathbb{F}_{q^n} \cap \mathbb{F}_{q^s}$. Then $t = \mathrm{GCD}(n, s) = \mathrm{GCD}(k\ell_n, k_1\ell_1 m_1) = k_1\mathrm{GCD}(\ell_n, \ell_1 m_1) = k_1\mathrm{GCD}(\ell_n, \ell_1) = k_1\ell_d$, where $\ell_d = \mathrm{GCD}(\ell_n, \ell_1)$ and we have used the fact that $\mathrm{GCD}(\ell_n, m_1) = 1$. As such, we can write $s = k_1\ell_1 m_1 = tu$, where $t = k_1\ell_d$. If $\ell_n \mid \ell_1$ then $\ell_d = \ell_n$ and $t = k_1\ell_n$.

Recall that $D = \bar{\ell}_1\bar{m}_1$ and that $\alpha^{q^s} = \frac{a\alpha+b}{c\alpha+d} = [A](\alpha)$ where $\alpha \in \mathbb{F}_{q^{k_1\ell_n r}}$. We see that if $\ell_n \mid \ell_1$ then $\ell_1 = j\ell_n$ and $D = \frac{\ell_n r}{\ell_1 m_1} = \frac{r}{jm_1}$ so $r = Djm_1$ and $D \mid r$. However if $\ell_n \nmid \ell_1$ and we let $\ell_n = \lambda\ell_d$ and $\ell_1 = \gamma\ell_d$, then $D = \frac{\lambda r}{\gamma m_1} = \lambda\nu$, where $\nu = \frac{r}{\gamma m_1}$. Since $\alpha = \alpha^{q^{Ds}} = [A^D](\alpha) = [I_2](\alpha)$ implies that $Ds \equiv 0 \pmod{r}$ we have that $Ds = k_1\ell_n r$. Thus $r = \frac{Ds}{k_1\ell_n} = \frac{\lambda\nu s}{k_1\ell_n} = \frac{\lambda\nu k_1\ell_1 m_1}{k_1\ell_n} = \nu u$ where $u = \gamma m_1 = \frac{\ell_1 m_1}{\ell_d}$. Now, $\ell_1 m_1 = \ell_d u$ implies that $s = k_1\ell_1 m_1 = k_1\ell_d u$. We have proved the following theorem.

Theorem 3.1. *Suppose the order of* A *is* $D = \frac{\lambda r}{\gamma m_1} = \lambda\nu$, *where* $\nu = \frac{r}{\gamma m_1}$. *Let* $P(x) \in \mathbb{F}_{q^{k_1\ell_d}}[x]$ *be a monic irreducible polynomial of degree* $r \geq 3$. *If* $P(x)$ *divides* $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b$ *then*

1. $r = \nu u$, *and* $u \in \mathbb{N}$,

2. $u \mid s$.

Remark 3.1. *We can also take* $s = k_1\ell_1 m_1$ *as* $s = k_1\ell_d u$ *where* $u = \gamma m_1 = \frac{\ell_1 m_1}{\ell_d}$.

Remark 3.2. *Note that if* $n = 1$ *then* $k_1\ell_d = 1$ *and* $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_q[x]$. *Thus the factorization of the form* $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_q[x]$ *considered in [2], [3], [5], [6], [12] and [15] are special cases of our work.*

3.1 Factorization of $F_s(x)$ where $D = 1$

Suppose α is a root of $F_s(x)$ and that $D = 1$. By Theorem 2.8, we may take $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. So $F_s(x) = x^{q^s} - x$. We know that the factorization of $F_s(x) = x^{q^s} - x$ contains irreducible factors of degree r if and only if $s = n_1 r$. We can then use Gauss' formula,

$$\frac{1}{r}\sum_{d|r}\mu(d)q^{\frac{n_1 r}{d}},$$

to count the number of such polynomials.

3.2 Factorization of $F_s(x)$ where $(p, D) = 1$

3.2.1 Factorization of $F_s(x)$ where $(p, D) = 1$, $D \mid (q^n - 1)$ and $\ell_n \mid \ell_1$

Suppose that α is a root of $F_s(x)$ and that $(p, D) = 1$, $D \mid (q^n - 1)$ and $\ell_n \mid \ell_1$. We have $\alpha^{q^s} = [A](\alpha)$. If A is not a multiple of I_2 then by Theorem 2.8, A is conjugate to a matrix of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ where $a \in \mathbb{F}_{q^n} \setminus \{0, 1\}$ is an element of order D. As such, we have $\alpha^{q^s} = a\alpha$ and we may assume that α satisfies an equation of type

$$x^{q^s} - ax = 0. \tag{1}$$

By Theorem 2.2 we have

$$x^{q^s-1} - a = \prod_{i=1}^{\frac{q^s-1}{D}} (x^D - \beta_i)$$

where β_i runs through all the distinct roots of $x^{\frac{q^s-1}{D}} - a$ in $\mathbb{F}_{q^s}$. Now, all the factors in this product are irreducible over $\mathbb{F}_{q^s}$. Hence the corresponding $q^s - 1$ roots lie in $\mathbb{F}_{q^{nr}}$. However, some of the roots may not lie in $\mathbb{S}$. If $\beta_i \in \mathbb{F}_{q^w}$ where $\mathbb{F}_{q^w}$ is a subfield of $\mathbb{F}_{q^s}$ and $Dw = s$ then the roots of $x^D - \beta_i$ lie in $\mathbb{S}$. Now let $r = Du$ and $u = r_1 r_2 \ldots r_w$ where $r_i \neq D$ for all i. If $\beta_i \in \mathbb{F}_{q^t}$ where $t = \frac{s}{r_i}$ then the roots of $x^D - \beta_i$ lie in $\mathbb{F}_{q^{\frac{Ds}{r_i}}}$ and not in $\mathbb{S}$. Thus we obtain the number of roots of $x^{q^s-1} - a = 0$ which are elements of $\mathbb{S}$ by subtracting from $q^s - 1$ the number of elements in any subfield of $\mathbb{F}_{q^s}$ of type $\mathbb{F}_{q^t}$ where $t = \frac{s}{r_i}$. Generally, we find that the number to be subtracted from $q^s - 1$ is

$$\sum_{1\le i\le w}\left(q^{\frac{s}{r_i}} - 1\right) - \sum_{1\le i<j\le w}\left(q^{\frac{s}{r_i r_j}} - 1\right) + \sum_{1\le i<j<k\le w}\left(q^{\frac{s}{r_i r_j r_k}} - 1\right) - \cdots (-1)^{w+1}\left(q^{\frac{s}{r_1\cdots r_w}} - 1\right).$$

Now if $s = k_1\ell_1 m_1$ and $r = Du$ where $u = r_1 r_2 \dots r_w$ then $sD = n_1 r$ and $s = n_1 u$. We have proved the following.

Theorem 3.2. *Let $s = k_1\ell_1 m_1$, $v = \bar{\ell}_1\bar{m}_1 > 1$ and suppose $(p, v) = 1$ and that $v \mid (q^{n_1} - 1)$ where $n_1 = k_1\ell_n$. Let $r = vu, u \in \mathbb{N}$ and $T(k_1, \ell_1 m_1)$ be the set of all roots of irreducible factors of degree r in the factorization of $G_s(x) = x^{q^s-1} - \varepsilon \in \mathbb{F}_{q^n}[x]$, where $\varepsilon \in \mathbb{F}_{q^n} \setminus \{0, 1\}$ is of order v. If $r \not\equiv 0 \pmod v$ then $|T(k_1, \ell_1 m_1)| = 0$. Otherwise*

$$|T(k_1, \ell_1 m_1)| = \frac{1}{vu} \sum_{\substack{d \mid u \\ (d,v)=1}} \mu(d) \left(q^{k_1 \ell_d \frac{u}{d}} - 1 \right).$$

We note that a similar result was found in [5] using the action of the general linear group $GL(2, q)$ on irreducible polynomials over $\mathbb{F}_q$.

Example 3.1. *Consider $q = 2$ and $n = r = 6$. We want to find the number of irreducible polynomials of degree 6 in the factorization of $F_{12}(x) = cx^{2^{12}+1} + dx^{2^{12}} - ax - b \in \mathbb{F}_{2^6}[x]$ where $ad - bc \neq 0$.*
Here $s = k_1\ell_1 m_1 = 12$, $\ell_n = 6$, $\ell_1 = 12$, $v = \bar{\ell}_1\bar{m}_1 = 3$, $r = vu = 3 \times 2$ and $\ell_n \mid \ell_1$. Using the computer algebra system MAGMA, we find that we can take $A = \begin{pmatrix} \zeta^{42} & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, 2^6)$ of order 3 where ζ is a primitive element of $\mathbb{F}_{2^6}$. Thus $F_{12}(x) = x^{4096} + \zeta^{42}x$. By Theorem 3.2, we find that there are 672 polynomials of degree 6 in the factorization of $F_{12}(x) = x^{4096} + \zeta^{42}x$ over $\mathbb{F}_{2^6}$.

3.2.2 Factorization of $F_s(x)$ where $(p, D) = 1$, $D \mid (q^n - 1)$ and $\ell_n \nmid \ell_1$

Suppose that α is a root of $F_s(x)$ and that $(p, D) = 1$, $D \mid (q^n - 1)$ and $\ell_n \nmid \ell_1$. Then we have $\alpha^{q^s} = [A](\alpha)$. By Theorem 2.8, A is conjugate to a matrix of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ where $a \in \mathbb{F}_{q^n} \setminus \{0, 1\}$ is an element of order D. As such, we have $\alpha^{q^s} = a\alpha$ and we may assume that α satisfies an equation of type

$$x^{q^s} - ax = 0. \tag{2}$$

Note that if $\ell_n \mid \ell_1$ then $k_1\ell_n \mid k_1\ell_1 m_1$ and $\mathrm{GCD}(k_1\ell_n, k_1\ell_1 m_1) = k_1\ell_n$ hence $\mathrm{GCD}(q^{k_1\ell_n} - 1, q^{k_1\ell_1 m_1} - 1) = q^{k_1\ell_n} - 1$. This implies that $q^{k_1\ell_n} - 1 \mid q^{k_1\ell_1 m_1} - 1$ and that $D \mid q^s - 1$. However, if $\ell_n \nmid \ell_1$ we know that $\mathrm{GCD}(k_1\ell_n, k_1\ell_1 m_1) = k_1\ell_d$ and that $D = \frac{\lambda r}{\gamma m_1} = \lambda\nu$, where $\nu = \frac{r}{\gamma m_1}$. Now $\frac{r}{\gamma m_1} = \frac{\ell_d \ell_r m}{\ell_1 m_1} = \frac{\ell \bar{m}_1}{\ell_N} = \bar{\ell}_N \bar{m}_1$, where $\ell_N = \mathrm{lcm}(\ell_n, \ell_1)$. So if $\ell_n \nmid \ell_1$ then $D \nmid (q^s - 1)$. We will replace D by ν since if α satisfies $x^{q^s-1} - a$ then α also satisfies $x^{q^{k\ell_N m_1}-1} - \varepsilon = 0$ where ε is of order $\nu = \bar{\ell}_N \bar{m}_1$ and we can show that $\nu \mid (q^s - 1)$. By Theorem 2.2 we obtain

$$x^{q^s-1} - a = \prod_{i=1}^{\frac{q^s-1}{\nu}} (x^\nu - \beta_i) \tag{3}$$

where β_i runs through all the distinct roots of $x^{\frac{q^s-1}{\nu}} - a$ in $\mathbb{F}_{q^s}$. It is shown in [14] that if $q \equiv -1 \pmod 4$ and $k_1\ell_1 m_1$ is odd and $\bar{\ell}_1\bar{m}_1$ is even then we take $D = 2\bar{\ell}_1\bar{m}_1$ otherwise we take $D = \bar{\ell}_1\bar{m}_1$. Now using an argument similar to the one in Section 3.2.1 we obtain the following theorems:

Theorem 3.3. *Let $q \equiv -1 \pmod 4$, $s = k_1\ell_1 m_1$ be odd, $\ell_d = (\ell_n, \ell_1)$ and $v = \bar{\ell}_1\bar{m}_1 = \lambda\nu > 1$ where v is an even integer and $\lambda = \frac{\ell_d}{\ell_n}$. Suppose $(p, v) = 1$ and that $2v \mid (q^{n_1} - 1)$ where $n_1 = k_1\ell_d$. Let $r = \nu u, u \in \mathbb{N}$ and $T^*(k_1, \ell_1 m_1)$ be the set of all roots of irreducible factors of degree r in the factorization of $G_s(x) = x^{q^s-1} - \varepsilon \in \mathbb{F}_{q^n}[x]$, where $\varepsilon \in \mathbb{F}_{q^n} \setminus \{0, 1\}$ is of order 2ν. If $r \not\equiv 0 \pmod \nu$ then $|T^*(k_1, \ell_1 m_1)| = 0$. Otherwise*

$$|T^*(k_1, \ell_1 m_1)| = \frac{1}{\nu u} \sum_{\substack{d \mid u \\ (d,\nu)=1}} \mu(d) \left(q^{n_1 \frac{u}{d}} - 1 \right).$$

In all other cases we have

Theorem 3.4. *Let $s = k_1\ell_1 m_1$, $\ell_d = (\ell_n, \ell_1)$ and $v = \bar{\ell}_1\bar{m}_1 = \lambda\nu > 1$ where $\lambda = \frac{\ell_n}{\ell_d}$. Suppose $(p, v) = 1$ and that $v \mid (q^{n_1} - 1)$ where $n_1 = k_1\ell_d$. Let $r = \nu u, u \in \mathbb{N}$ and $T^{**}(k_1, \ell_1 m_1)$ be the set of all roots of irreducible factors of degree r in the factorization of $G_s(x) = x^{q^s-1} - \varepsilon \in \mathbb{F}_{q^n}[x]$, where $\varepsilon \in \mathbb{F}_{q^n} \setminus \{0, 1\}$ is of order ν. If $r \not\equiv 0 \pmod \nu$ then $|T^{**}(k_1, \ell_1 m_1)| = 0$. Otherwise*

$$|T^{**}(k_1, \ell_1 m_1)| = \frac{1}{\nu u} \sum_{\substack{d \mid u \\ (d,\nu)=1}} \mu(d) \left(q^{n_1 \frac{u}{d}} - 1 \right).$$

Example 3.2. *Consider $q = 2$ and $n = r = 6$. We want to find the number of irreducible polynomials of degree 6 in the factorization of $F_4(x) = cx^{2^4+1} + dx^{2^4} - ax - b \in \mathbb{F}_{2^6}[x]$ where $ad - bc \neq 0$.*
We see that $s = k_1\ell_1 m_1 = 4$, $\ell_n = 6$, $\ell_1 = 4$, $\ell_d = 3$, $\lambda = 2$, $v = \bar{\ell}_1\bar{m}_1 = \lambda\nu = 3 \times 3$, $r = \nu u = 3 \times 2$ and $\ell_n \nmid \ell_1$. Using the computer algebra system MAGMA, we can take $A = \begin{pmatrix} \zeta^{49} & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, 2^6)$ of order 9 where ζ is a primitive element of $\mathbb{F}_{2^6}$. Thus $F_4(x) = x^{16} + \zeta^{49}x$. By Theorem 3.4, we find that there are 2 polynomials of degree 6 in the factorization of $F_4(x) = x^{16} + \zeta^{49}x$ over $\mathbb{F}_{2^6}$.

3.2.3 Factorization of $F_s(x)$ where $(p, D) = 1$ and $D \mid (q^n + 1)$

Suppose that α is a root of $F_s(x)$ and that $(p, D) = 1$ and $D \mid (q^n + 1)$. Then we have $\alpha^{q^s} = [A](\alpha)$. By Theorem 2.8, A is conjugate to a matrix of the form $\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}$ where $c, d \in \mathbb{F}_{q^n}$ and $c \neq 0$. Without loss of generality, we will take $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{F}_{q^n}$, $ad - bc \neq 0$ and the eigenvalues of A lie in $\mathbb{F}_{q^{2n}}$. Thus we have $\alpha^{q^s} = \frac{a\alpha+b}{c\alpha+d}$ and we may assume that α satisfies an equation of type

$$cx^{q^s+1} + dx^{q^s} - ax - b = 0. \tag{4}$$

We begin by considering the factorization of $F_s(x)$ where $(p, D) = 1$, $D \mid (q^n + 1)$ and D is even.

Suppose that α is a root of $F_s(x)$ and that D is even. Then we can take $D = 2d$ where d is a positive integer. Thus we have $\alpha^{q^{sD}} = [A^D](\alpha) = [I_2](\alpha) = \alpha$. So $A^{2d} = (A^d)^2 =$

$B^2 = I_2$, where $B = A^d$. Now, since $B^2 = I_2$, without loss of generality we can take $B = \begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$ since the only elements $\zeta \in \mathbb{F}_{q^n}$ such that $\zeta^2 = 1$ are $\zeta = 1$ and $\zeta = q-1$. Thus α satisfies an equation of the form $F_s(x) = (q-1)(x^{q^s} - x) = 0$. By the argument in Section 3.1 there are no irreducible polynomials of degree r in the factorization of $F_s(x)$.

Example 3.3. *Consider $q = 3$, $n = 5$ and $r = 4$. There are no polynomials of degree 4 in the factorization of $F_5(x) = 2x^{244} + 2 \in \mathbb{F}_{3^5}[x]$ where $A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \in GL(2, 3^5)$ is of order 4.*

Next we consider the factorization of $F_s(x)$ where $(p, D) = 1$, $D \mid (q^n + 1)$ and $d \mid D$ but $d^2 \nmid D$. Suppose that α is a root of $F_s(x)$ and that $d \mid D$ where $1 < d < D$. We have $\alpha^{q^s} = [A](\alpha)$ where A is a matrix of order D. Now, if $d \mid D$ then $\alpha^{q^{sd}} = [A^d](\alpha) = [B](\alpha)$, where $B = A^d$ and the order of B is $\frac{D}{d}$ since $\mathrm{GCD}(D, d) = d$. We see that for α to satisfy $F_{sd}(x)$, d must divide $\frac{D}{d}$. That is α satisfies $F_{sd}(x)$ provided $d^2 \mid D$. We have proved the following theorem.

Theorem 3.5. *Suppose α satisfies $F_s(x)$ and $d \mid D$ where $1 < d < D$. If $d^2 \nmid D$ then α does not satisfy $F_{sd}(x)$.*

This theorem is significant because it tells us when to expect an irreducible polynomial of degree r in the factorization of $F_s(x)$ by looking at the factorization of $F_{sd}(x)$.

Next we consider when an irreducible quadratic polynomial of the form $cx^2 + (d-a)x - b \in \mathbb{F}_{q^{k_1 \ell_d}}[x]$ divides $F_s(x)$.

Proposition 3.1. *If $P(x) = cx^2 + (d-a)x - b \in \mathbb{F}_{q^{k_1 \ell_d}}[x]$ is irreducible, then $P(x) \mid F_s(x)$ if and only if $s = 2k_1 \ell_d w$.*

Proof. Suppose $P(x) = cx^2 + (d-a)x - b \in \mathbb{F}_{q^{k_1 \ell_d}}[x]$ is irreducible and that $P(\alpha) = 0$. Then $\alpha^{q^{2k_1 \ell_d}} = \alpha$. If $s = k_1 \ell_d u$ where u is even then $\mathrm{GCD}(2, k_1 \ell_d u) = 2$ and this implies that $\alpha^{q^{k_1 \ell_d u}} = \alpha$. Thus $F_s(\alpha) = c\alpha^{q^s+1} + d\alpha^{q^s} - a\alpha - b = c\alpha^2 + d\alpha - a\alpha - b = 0$. So $P(x) \mid F_s(x)$. If s is odd and $P(\alpha) = 0$ then $\alpha^{q^s+1} = \alpha^{q+1}$. So $F_s(\alpha) = c\alpha^{q^s+1} + d\alpha^{q^s} - a\alpha - b = c\alpha^{q+1} + d\alpha^q - a\alpha - b = (\alpha^{q-1} - 1)(c\alpha^2 + d\alpha) + c\alpha^2 + d\alpha - a\alpha - b = 0$. We know that $c\alpha^2 + d\alpha - a\alpha - b = 0$ so $F_s(\alpha) = 0 \Leftrightarrow \alpha^{q-1} - 1 = 0$. This means $\alpha \in \mathbb{F}_q$ and $P(x)$ is reducible. $\square$

Consequently, we will divide our analysis according to the parity of u.

Suppose that u is odd, then by Proposition 3.1 there is no quadratic factor in the factorization of $F_s(x)$. By the factorization in Theorem 2.3 we have

$$cx^{q^s+1} + dx^{q^s} - ax - b = \prod_{j=1}^{\frac{q^s+1}{\tau}} \frac{1}{1-\beta_j} \left[(x - x_0)^\tau - \beta_j (x - x_1)^\tau \right] \tag{5}$$

where $x_0, x_1 \in \mathbb{F}_{q^{2k_1 \ell_d}}$ are the two distinct roots of $cx^2 + (d-a)x - b = 0$, τ is the multiplicative order of $\xi = \frac{a - cx_1}{a - cx_0}$ and β_j is a root of $x^{\frac{q^s-1}{\tau}} - \xi$ in $\mathbb{F}_{q^s}$. Note that $\tau = \bar{\ell}_1 \bar{m}_1$.

Now, all the factors of $G_\tau(x) = \frac{1}{1-\beta_j}\left[(x-x_0)^\tau - \beta_j(x-x_1)^\tau\right]$ are irreducible over $\mathbb{F}_{q^s}$ so their corresponding q^s+1 roots lie in $\mathbb{F}_{q^{s\tau}} = \mathbb{F}_{q^{k_1\ell_n r}}$. We consider three cases: $\tau = r$, $\tau = u$ and u is odd where neither $\tau = r$ nor $\tau = u$.

If s is odd and $\tau = r$ then the polynomials $G_\tau(x)$ are of the required degree r and the number of polynomials of degree $r = \nu u$ in the factorization of $F_s(x)$ is $\frac{q^s+1}{r}$.

Next suppose that $\tau = u$. Then $s = k_1\ell_d u = k_1\ell_d\tau$ and if β_j lies in $\mathbb{F}_{q^{k_1\ell_d}}$ then all the roots of $G_\tau(x)$ lie in $\mathbb{F}_{q^{k_1\ell_d\tau}} = \mathbb{F}_{q^s}$. Hence all roots of $G_\tau(x)$ lie in $\mathbb{S}$. So there are $\frac{q^s+1}{r}$ irreducible factors of degree r in the factorization of $F_s(x)$.

Lastly we consider the more general case where s is odd and neither $\tau = r$ nor $\tau = u$. In this case if β_j lies in a subfield of $\mathbb{F}_{q^s}$ of the form $\mathbb{F}_{q^t}$ where $\tau \nmid \frac{s}{t}$ then the roots of $G_\tau(x)$ do not lie in $\mathbb{S}$. Now $r = \nu u$ and if we let $u = r_1r_2\ldots r_w$ where $r_i \neq \nu$ we can use an argument similar to the one in Section 3.2.1 to show that the number roots of $F_s(x)$ which are elements of $\mathbb{S}$ can be found by subtracting from q^s+1 the number

$$\sum_{1\le i\le w}\left(q^{\frac{s}{r_i}}+1\right) - \sum_{1\le i<j\le w}\left(q^{\frac{s}{r_ir_j}}+1\right) + \sum_{1\le i<j<k\le w}\left(q^{\frac{s}{r_ir_jr_k}}+1\right) - \cdots (-1)^{w+1}\left(q^{\frac{s}{r_1\cdots r_w}}+1\right).$$

We have proved the following theorem.

Theorem 3.6. *The number $N_A(\nu u)$ of polynomials of degree νu in the factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b$ where s is odd and the order of A divides q^n+1 is*

$$N_A(\nu u) = \frac{1}{\nu u}\sum_{\substack{d|u \\ d\not\equiv 0 \pmod{\nu}}} \mu(d)(q^{n_1\frac{u}{d}}+1),$$

where $n_1 = k_1\ell_d$.

Next suppose that u is even. Then by Proposition 3.1 there is an irreducible quadratic factor in the factorization of $F_s(x)$. By the factorization in Theorem 2.3 we have

$$cx^{q^s+1} + dx^{q^s} - ax - b = (x-x_0)(x-x_1)\prod_{j=1}^{\frac{q^s-1}{\tau}} \frac{1}{1-\beta_j}\left[(x-x_0)^\tau - \beta_j(x-x_1)^\tau\right] \tag{6}$$

where $x_0, x_1 \in \mathbb{F}_{q^s}$ are the two distinct roots of $cx^2+(d-a)x-b=0$, τ is the multiplicative order of $\xi = \frac{a-cx_1}{a-cx_0}$ and β_j is a root of $x^{\frac{q^s-1}{\tau}} - \xi$ in $\mathbb{F}_{q^s}$. Observe that if $s = 2k_1\ell_d$ then $\mathbb{F}_{q^{k_1\ell_d}}$ is a subfield of $\mathbb{F}_{q^{2k_1\ell_d}}$ and if $\beta_j \in \mathbb{F}_{q^{k_1\ell_d}}$ then the roots of $G_\tau(x)$ do not lie in $\mathbb{S}$. In this case the number of roots of $F_s(x)$ which are elements of $\mathbb{S}$ is $q^{2k_1\ell_d} - q^{k_1\ell_d} - 2$. Thus the number of irreducible factors of degree r in the factorization of $F_s(x)$ is $\frac{1}{r}(q^{2k_1\ell_d} - q^{k_1\ell_d} - 2)$.

More generally, if $s = k_1\ell_d u$ where u is even then there exists a subfield $\mathbb{F}_{q^t}$ of $\mathbb{F}_{q^s}$ such that $2t = k_1\ell_d u$ and the roots of $G_\tau(x)$ over $\mathbb{F}_{q^t}$ do not lie in $\mathbb{S}$. Next note that this result holds for any divisor of u that is not equal to τ. As above we obtain the following result.

Theorem 3.7. *The number $N_A(\nu u)$ of polynomials of degree νu in the factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b$ where $s = k_1\ell_d u$ and u is even and the order of A divides q^n+1 is*

$$N_A(\nu u) = \frac{1}{\nu u}\sum_{\substack{d|u \\ d\not\equiv 0 \pmod{\nu}}} \mu(d)(q^{n_1\frac{u}{d}}-1),$$

where $n_1 = k_1\ell_d$.

Next we combine Theorem 3.6 and Theorem 3.7 to obtain an enumeration formula for the number of irreducible polynomials in the factorization of $F_s(x)$ where $(p, D) = 1$ and $D \mid (q^n + 1)$.

Theorem 3.8. *The number $N_A(\nu u)$ of polynomials of degree νu in the factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b$ where the minimal polynomial of A is an irreducible quadratic polynomial over $\mathbb{F}_{q^{k_1 \ell_d}}$ is*

$$N_A(\nu u) = \frac{1}{\nu u} \sum_{\substack{d|u \\ d \not\equiv 0 \pmod{\nu}}} \mu(d)(q^{n_1 \frac{u}{d}} - (-1)^{\frac{u}{d}}),$$

where $n_1 = k_1 \ell_d$.

A similar result can be found in [11] and [13].

Note that in the discussion leading up to Theorem 3.6 and Theorem 3.7 we implicitly assumed that $\ell_n \mid \ell_1$. Thus $\nu = \bar{\ell}_1 \bar{m}_1$. However, if $\ell_n \nmid \ell_1$ then as we did in Section 3.2.2 we will replace τ in Equation 5 and Equation 6 by $\nu = \frac{r}{\gamma m_1}$.

Example 3.4. *Consider $q = 2$, $n = 5$ and $r = 6$. We want to find the number of irreducible polynomials of degree 6 in the factorization of $F_{10}(x) = x^{2^{10}+1} - x + 1 \in \mathbb{F}_{2^5}[x]$. Suppose α satisfies $F_{10}(x)$. Then $\alpha^{2^{10}+1} - \alpha + 1 = 0$. Thus $\alpha^{2^{10}} = \frac{\alpha - 1}{\alpha} = [A](\alpha)$. So $A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in GL(2, 2^5)$. By direct computation $\alpha^{2^{30}} = \alpha = [A^3](\alpha) = [I_2](\alpha)$. Hence A is a matrix of order 3 and we note that $5 \mid (2^5 + 1)$. Here $\nu = 3$ so $r = \nu u = 3 \times 2$.*

Using Theorem 3.8, with $r = \nu u = 3 \times 2$ we obtain

$$\begin{aligned} N_A(6) &= \tfrac{1}{6} \sum_{\substack{d|2 \\ d \not\equiv 0 \pmod 3}} \mu(d)(2^{5 \cdot \frac{2}{d}} - (-1)^{\frac{2}{d}}) \\ &= \tfrac{1}{6}(2^{10} - 2^5 - 2) \\ &= \tfrac{990}{6} = 165 \end{aligned}$$

So there are 165 polynomials of degree 6 in the factorization of $F_{10}(x) = x^{2^{10}+1} + x + 1$ over $\mathbb{F}_{2^5}$.

Example 3.5. *Consider $q = 5$, $n = 3$ and $r = 6$. We want to find the number of irreducible polynomials of degree 6 in the factorization of $F_2(x) \in \mathbb{F}_{5^2}[x]$. Here $s = k_1 \ell_d u = 2$, $\ell_1 = 1$ and $\ell_n = 3$ so $k_1 \ell_d = 1$ and $u = 2$. Since $\ell_n \nmid \ell_1$ we will take $\nu = 3$. We note that if α is a root of $F_2(x)$ then $\alpha^{5^2} = \frac{a\alpha + b}{c\alpha + d}$. We can take $A = \begin{pmatrix} 0 & 1 \\ 4 & \zeta^{98} \end{pmatrix} \in GL(2, 5^2)$ of order 9 where ζ is a primitive element of $\mathbb{F}_{5^2}$. Thus $F_2(x) = 4x^{5^2+1} + \zeta^{98} x^{25} + 4$. By Theorem 3.8, with $r = \nu u = 3 \times 2$ we find that there are 3 polynomials of degree 6 in the factorization of $F_2(x) = 4x^{26} + \zeta^{98} x^{25} + 4$ over $\mathbb{F}_{5^2}$.*

3.3 Factorization of $F_s(x)$ where GCD$(D, p) = p$

3.3.1 Factorization of $F_s(x)$ where $D = p$

Suppose that α is a root of $F_s(x)$ and that $D = p$. The fact that $D = p$ implies that $s = \frac{n_1 r}{p} = k_1 \frac{\ell m}{p}$. Thus, we have $\alpha^{q^{k_1 \frac{\ell m}{p}}} = [A](\alpha)$. By Theorem 2.8, A is conjugate to a matrix of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ where $b \neq 0 \in \mathbb{F}_{q^n}$. We will take $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ since we can show, by direct computation, that the order of A is p. As such, we have $\alpha^{q^{k_1 \frac{\ell m}{p}}} = \alpha + 1$ and we may assume that α satisfies an equation of type

$$x^{q^{k_1 \frac{\ell m}{p}}} - x - 1 = 0. \tag{7}$$

This polynomial was fully factorized in [14] and an algorithm is given which counts the number of irreducible polynomials of degree r in the factorization of $x^{q^{k_1 \frac{\ell m}{p}}} - x - 1$. However, we will use the methods employed in [14] to find an analytic formula for finding the number of irreducible factors of degree r in the factorization of $x^{p^{k_1 \frac{\ell m j}{p}}} - x - 1$ where p is the characteristic of $\mathbb{F}_q$ and $q = p^j$. We know that

$$x^{p^{k_1 \frac{\ell m j}{p}}} - x - 1 = \prod_{i=1}^{p^{k_1 \frac{\ell m j}{p} - 1}} (x^p - x - \beta_i) \tag{8}$$

where β_i denotes all the elements of $\mathbb{F}_{q^{k_1 \frac{\ell m}{p}}}$ which have trace 1 over $\mathbb{F}_p$, see Theorem 2.6. By Theorem 2.5, the trinomials $x^p - x - \beta_i$ are irreducible over $\mathbb{F}_{q^{k_1 \frac{\ell m}{p}}}$. Now, the $q^{k_1 \frac{\ell m}{p}}$ roots of $x^{p^{k_1 \frac{\ell m j}{p}}} - x - 1 = 0$ lie in $\mathbb{F}_{q^{k_1 \ell m}} - \mathbb{F}_{q^{k_1 \frac{\ell m}{p}}}$. However, some of the roots may not lie in $\mathbb{S}$. If $\beta_i \in \mathbb{F}_{q^{k_1 \ell_1 m_1}}$ where $\ell_1 m_1$ is a proper divisor of $\frac{\ell m}{p}$ then the roots of $x^p - x - \beta_i$ do not lie in $\mathbb{S}$. But if β_i does not lie in any such subfield then the roots of $x^p - x - \beta_i$ do lie in $\mathbb{S}$.

Now if $\beta_i \in \mathbb{F}_{q^w}$ where $\mathbb{F}_{q^w}$ is a proper subfield of $\mathbb{F}_{q^{k_1 \frac{\ell m}{p}}}$ then

$$Tr_{(\mathbb{F}_{q^{k_1 \frac{\ell m}{p}}}/\mathbb{F}_p)}(\beta_i) = \frac{k_1 \ell m}{pw} Tr_{(\mathbb{F}_{q^w}/\mathbb{F}_p)}(\beta_i). \tag{9}$$

So if $\mathrm{GCD}(p, \frac{k_1 \ell m}{pw}) \neq 1$ then $Tr_{(\mathbb{F}_{q^{k_1 \frac{\ell m}{p}}}/\mathbb{F}_p)}(\beta_i) = 0$ and if $\mathrm{GCD}(p, \frac{k_1 \ell m}{pw}) = 1$ then exactly $\frac{1}{p}$ elements of $\mathbb{F}_{q^w}$ have absolute trace equal to 1. In both cases the roots of the corresponding equations $x^p - x - \beta_i$ do not lie in $\mathbb{S}$. Thus we obtain the number of elements of $\mathbb{S}$ which are roots of $x^{q^{k_1 \frac{\ell m}{p}}} - x - 1 = 0$ by subtracting from $q^{k_1 \frac{\ell m}{p}}$ the number of elements in any proper subfield of $\mathbb{F}_{q^{k_1 \frac{\ell m}{p}}}$ of type $\mathbb{F}_{q^{k_1 \ell_1 m_1}}$ where $\ell_1 m_1$ is a divisor of $\frac{\ell m}{p}$ and $p \nmid \frac{\bar{\ell}_1 \bar{m}_1}{p}$. Now, let $r_1, \ldots, r_w$ be the distinct prime factors of r where $r_i \neq p$ for any i, we can use a lattice of subfields of $\mathbb{F}_{q^{k_1 \frac{\ell m}{p}}}$ to show that the number to be subtracted from $q^{k_1 \frac{\ell m}{p}}$ is

$$\sum_{1 \leq i \leq w} q^{\frac{k_1 \ell m}{p r_i}} - \sum_{1 \leq i < j \leq w} q^{\frac{k_1 \ell m}{p r_i r_j}} + \sum_{1 \leq i < j < k \leq w} q^{\frac{k_1 \ell m}{p r_i r_j r_k}} - \cdots (-1)^{w+1} q^{\frac{k_1 \ell m}{p r_1 \cdots r_w}}.$$

Now, if we let $r = pu$ then $u = \frac{r}{p}$. So $k_1 \frac{\ell m}{p} = k_1 \frac{\ell_n \ell_r m}{p} = k_1 \ell_n \frac{r}{p} = k_1 \ell_n u = n_1 u$. Thus, we have proved the following.

Theorem 3.9. *Suppose $F_s(x) = x^{q^{k_1 \frac{\ell m}{p}}} - x - 1$ where $\bar{\ell}_1 \bar{m}_1 = p$. Let $r = pu, u \in \mathbb{N}$, $n_1 = k_1 l_n$ and $V(k_1)$ be the set of roots of irreducible factors of degree r in the factorization of $F_s(x)$. If $r \not\equiv 0 \pmod p$, then $|V(k_1)| = 0$. Otherwise*

$$|V(k_1)| = \sum_{\substack{d|u \\ d \not\equiv 0 \pmod p}} \mu(d) q^{n_1 u/d}.$$

Corollary 3.1. *The number of irreducible factors of degree r in the factorization of $F_s(x) = x^{q^{k_1 \frac{\ell m}{p}}} - x - 1$ is*

$$\frac{1}{r}|V(k_1)|.$$

We note that this result was also found in [5] using the action of the general linear group $GL(2,q)$ on irreducible polynomials over $\mathbb{F}_q$.

Example 3.6. *Consider $q = 2$, $n = r = 6$. We want to find the number of irreducible polynomials of degree 6 in the factorization of $F_{18}(x) \in \mathbb{F}_{2^6}[x]$.*
Here $k_1 = 1$, $\ell_1 = 18$, $m_1 = 1$ so $s = k_1 \ell_1 m_1 = 18$. Also $\ell_n = 6$ and $r = pu = 2 \times 3$. We will take $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL(2, 2^6)$ of order 2. Thus $F_{18}(x) = x^{2^{18}} - x - 1$. By Corollary 3.1, there are 43,080 polynomials of degree 6 in the factorization of $F_{18}(x) = x^{2^{18}} - x - 1$ over $\mathbb{F}_{2^6}$.

Now consider the factorization of $F_s(x)$ where $D = p^2$ and $p^2 \mid r$. The fact that $D = p^2$ implies that $s = \frac{n_1 r}{p^2}$. Thus, we have $\alpha^{q^{\frac{n_1 r}{p^2}}} = [A](\alpha)$. So $\alpha^{q^{n_1 r}} = [A^{p^2}](\alpha)$ and the order of A divides p^2. By Corollary 2.1, matrices of order p^2 do not exist. So we consider matrices of order p. This gives rise to an equation of the form $x^{q^{\frac{n_1 r}{p^2}}} - x - 1 = 0$. By an argument similar to the one in Section 3.3.1, we find that all roots of this polynomial lie in $\mathbb{F}_{q^{\frac{n_1 r}{p}}} - \mathbb{F}_{q^{\frac{n_1 r}{p^2}}}$ and not in $\mathbb{S}$. We have the following theorem.

Theorem 3.10. *There is no polynomial of degree r in the factorization of $F_s(x)$ if $D = p^2$ and $p^2 \mid r$.*

Next suppose that $F_s(x) = x^{q^s} - ax - b \in \mathbb{F}_{q^n}$ is such that $D = pp_1$ where p_1 is some other divisor of r. That is, if $F_s(\alpha) = 0$ then $\alpha^{q^s} = [A](\alpha)$ is such that $\alpha^{q^{spp_1}} = [A^{pp_1}](\alpha) = [I_2](\alpha) = \alpha$. Then $A^{pp_1} = I_2$ and by Corollary 2.1 we know that such a matrix does not exist. Moreover, if we take $B = A^p$ of order p_1 then we have $\alpha^{q^{sp_1}} = [B^{p_1}](\alpha)$ then α satisfies Equation 1 or Equation 3. Also if we take $B = A^{p_1}$ of order p then we have $\alpha^{q^{sp}} = [B^p](\alpha)$ then α satisfies Equation 8 and this is not possible. So there is no irreducible polynomial of degree r in the factorization of $F_s(x)$ in this case.

Finally, we consider the factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}$ where $s = k_1 \ell_1 m$, $D = \bar{\ell}_1 = p^i$, $i > 1$ and $p^2 \nmid r$. Without loss of generality, $s = k_1 \ell_1 m = \frac{nr}{p^i}$ where $p^{i-1} \mid n$. Now, by Theorem 2.8, A is conjugate to a matrix of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ where $b \neq 0 \in \mathbb{F}_{q^n}$. So we have $\alpha^{q^{k_1 \ell_1 m}} = \alpha + b$ and we may assume that α satisfies an equation of type

$$x^{q^{k_1\ell_1 m}} - x - b = 0. \tag{10}$$

This polynomial was fully factorized in [14] by exploiting the decomposition

$$x^{q^{\frac{nr}{p}}} - x - 1 = \prod_{i=1}^{q^{(\frac{\bar{k}_1\bar{\ell}_1}{p}-1)k_1\ell_1 m}} (x^{q^{k_1\ell_1 m}} - x - \beta_i) \tag{11}$$

where β_i runs through all elements of $\mathbb{F}_{q^{\frac{nr}{p}}}$ such that $Tr_{\mathbb{F}_{q^{\frac{nr}{p}}}/\mathbb{F}_{q^{k_1\ell_1 m}}}(\beta_i) = 1$. It is shown in [14] that we obtain the cardinality of the set, $W(k_1\ell_1 m)$, of roots of polynomials of degree r in the factorization of Equation 10 by subtracting from $q^{k_1\ell_1 m}$ the number of elements in any proper subfield of type $\mathbb{F}_{q^{k\ell_2 m_1}}$ where $p \nmid \bar{\ell}_2\bar{m}_1$ but $\bar{\ell}_2\bar{m}_1 > 1$. Furthermore, an algorithm is given in [14] which gives $|W(k_1\ell_1 m)|$. We obtain the following analytic formula from the algorithm in [14].

Theorem 3.11. *Suppose $F_s(x) = x^{q^{k_1\ell_1 m}} - x - b$ where $b \in \mathbb{F}_{q^{\frac{nr}{p}}}$ is such that $Tr_{\mathbb{F}_{q^{\frac{nr}{p}}}/\mathbb{F}_{q^{k_1\ell_1 m}}}(b) = 1$ and $\bar{\ell}_1\bar{m}_1 = p^i$. Let $r = pu, u \in \mathbb{N}$, $n_1 = \frac{n}{p^{i-1}}$ and $W(k_1\ell_1 m)$ be the set of roots of irreducible factors of degree r in the factorization of $F_s(x)$. If $r \not\equiv 0 \pmod p$, then $|W(k_1\ell_1 m)| = 0$. Otherwise*

$$|W(k_1\ell_1 m)| = \sum_{\substack{d|u \\ d\not\equiv 0 \pmod p}} \mu(d) q^{n_1 u/d}.$$

Corollary 3.2. *The number of irreducible factors of degree r in the factorization of $F_s(x) = x^{q^{k_1\ell_1 m}} - x - b$ where $b \in \mathbb{F}_{q^{\frac{nr}{p}}}$ is*

$$\frac{1}{pu}|W(k_1\ell_1 m)|.$$

Example 3.7. *Consider $q = 2$, $n = r = 6$. We want find the number of irreducible polynomials of degree 6 in the factorization of $F_9(x) \in \mathbb{F}_{2^6}[x]$.*
Here $s = 9$ where $k_1 = 1$, $\ell_1 = 9$ and $m_1 = 1$. Also $\ell_n = 6$, $r = pu = 2 \times 3$ and $n_1 = 3$. We will take $A = \begin{pmatrix} 1 & \zeta^{62} \\ 0 & 1 \end{pmatrix} \in GL(2, 2^6)$ where $\zeta \in \mathbb{F}_{2^6}$ is a primitive element. Thus $F_9(x) = x^{2^9} + x + \zeta^{62}$. By Theorem 3.11, there are 84 polynomials of degree 6 in the factorization of $F_9(x) = x^{2^9} + x + \zeta^{62}$.

Finally we bring together all the results we have to obtain enumeration formulas for the number of irreducible polynomials of degree r in the factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b$.

Theorem 3.12. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, q^n)$ be of order $D = \bar{\ell}_1\bar{m}_1$ and $\nu = \frac{r}{\gamma m_1}$ where $\gamma = \frac{\ell_1}{\ell_n}$. Also let $N_A(r)$ be the number of irreducible factors of degree r in the factorization of $F_s(x) = cx^{q^s+1} + dx^{q^s} - ax - b \in \mathbb{F}_{q^n}[x]$. Then the following hold*

1. *If* $D=1$ *and* $s=k_1\ell_n r$ *then*

$$N_A(r)=\frac{1}{r}\sum_{d|r}\mu(d)q^{\frac{k_1\ell_n r}{d}}.$$

2. *If* $GCD(D,p)=1$*,* $D\mid(q^n-1)$*,* $\ell_n\mid\ell_1$*,* $r=\nu u$ *and* $n_1=k_1\ell_d$ *or if* D *is even,* $GCD(D,p)=1$*,* $D\mid(q^n-1)$*,* $\ell_n\nmid\ell_1$*,* $q\equiv-1 \pmod 4$*,* $s=k_1\ell_1 m_1$ *is odd then*

$$N_A(r)=\frac{1}{r}\sum_{\substack{d|u\\(d,\nu)=1}}\mu(d)\left(q^{n_1\frac{u}{d}}-1\right).$$

3. *If* $(p,D)=1$ *and* $D\mid(q^n+1)$*,* $r=\nu u$ *and* $n_1=k_1\ell_d$ *then*

$$N_A(r)=\frac{1}{\nu u}\sum_{\substack{d|u\\d\not\equiv 0 \pmod{\nu}}}\mu(d)(q^{n_1\frac{u}{d}}-(-1)^{\frac{u}{d}}).$$

4. *If* $GCD(D,p)=p$*,* $D=p$*,* $r=pu$ *and* $n_1=k_1\ell_n$ *or if* $D=p^i$ *and* $p^2\nmid r$*,* $r=pu$ *and* $n_1=\frac{n}{p^{i-1}}$ *then*

$$N_A(r)=\frac{1}{r}\sum_{\substack{d|u\\d\not\equiv 0 \pmod{p}}}\mu(d)q^{n_1u/d}.$$

3.4 Counting self-reciprocal irreducible monic polynomials

It is well known that each irreducible factor of $H_s(x)=x^{q^s+1}-1$ of degree ≥ 2 is a self-reciprocal irreducible monic (srim) polynomial of degree $2u$, where $u\mid s$ and $\frac{s}{u}$ is odd, see [10]. Suppose $H_s(\alpha)=0$, then $\alpha^{q^s+1}-1=0$. So $\alpha^{q^s}=[A](\alpha)$ where $A=\begin{pmatrix}0&1\\1&0\end{pmatrix}\in GL(2,q^n)$ is of order 2. We obtain the following result (see [10], [1] and [4]) from Item 2 and Item 4 of Theorem 3.12.

Theorem 3.13. *Let* $N_A(r)$ *be the number of srim polynomials of degree* $2u$ *in the decomposition of* $H_s(x)=x^{q^s+1}-1$*.*

$$N_A(r)=\begin{cases}\frac{1}{2u}(q^s-1), & \text{if } q \text{ is odd and } r=2^i\\ \frac{1}{2u}\sum_{\substack{d|s\\d\not\equiv 0 \pmod 2}}\mu(d)q^{s/d}, & \text{otherwise.}\end{cases}$$

4 Conclusion

In this paper we have obtained enumeration results on the number of irreducible factors of degree r in the factorization of $cx^{q^s+1}+dx^{q^s}-ax-b\in\mathbb{F}_{q^n}[x]$ where $ad-bc\neq 0$. We obtained our results by enumerating the number of roots of polynomials of degree r in the factorization of $cx^{q^s+1}+dx^{q^s}-ax-b\in\mathbb{F}_{q^n}[x]$. We have also obtained a generalization of previous enumeration results which considered this polynomial.

References

[1] L. Carlitz, *Some theorems on irreducible reciprocal polynomials over a finite field*, J. Reine Angew. Math. 227 (1967), pp. 212–220.

[2] I.F. Blake, S. Gao and R.C. Mullin, *Normal and Self-dual Normal Bases from Factorization of* $cx^{q+1} + dx^q - ax - b$, Finite Fields and Their Applications 6 (2000), pp. 255–281, .

[3] I.A.W. Bluher, *On* $x^{q+1} + ax + b$, Finite Fields and Their Applications, 10 (2004), pp. 285-305.

[4] S.D. Cohen, *On irreducible polynomials of certain types in finite fields*, Proc. Cambridge Philos. Soc. 66 (1969), pp. 335344.

[5] T. Garefalakis,*On the action of* $GL_2(\mathbb{F}_q)$ *on Irreducible Polynomials over* $\mathbb{F}_q$, Journal of Pure and Applied Algebra, 215 (2011), pp. 1835-1843.

[6] T. Helleseth and A. Kholosha, *On the equation* $x^{2^l+1} + x + a = 0$, Finite Fields and Their Applications 14 (2008), 159-176 .

[7] R.Lidl, and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1986.

[8] K. Magamba and J.A. Ryan, *Counting Extended Irreducible Codes*, Appl. Algebra Engrg. Comm. Comput. (2018) doi:10.1007/s00200-018-0375-x

[9] S. Mattarei, *The Orders of Nonsingular Derivations of Lie Algebras of Characteristic Two*, J. Austral. Math. Soc. 71 (2006), pp. 299-305.

[10] H. Meyn, *On the construction of irreducible self-reciprocal polynomials over finite fields*, Appl. Algebra Engrg. Comm. Comput., 1 (1990), pp. 4353.

[11] J.F Michon and P. Ravache, *On different families of invariant irreducible polynomials over* $\mathbb{F}_2$. Finite Fields Appl., 16(2010), pp. 163-174.

[12] O. Ore, *Contributions to the Theory of Finite Fields*, Trans. Amer. Math. Soc., Vol. 36 (1934), pp. 243-247.

[13] M. Pizzato, *Some Problems Concerning Polynomials over Finite Fields, or Algebraic Divertissements*, PhD Thesis, University of Trento, 2013.

[14] J.A. Ryan, *Irreducible Goppa Codes*, PhD Thesis, University College Cork, 2004.

[15] H. Stichtenoth and A. Topuzoğlu *Factorization of a Class of Polynomials over Finite Fields*, Finite Fields and Their Applications, 1 (2012), pp. 108-122.