AIMS Mathematics, 5(4): 2877–2887.
DOI:10.3934/math.2020185
Received: 04 December 2019
Accepted: 03 February 2020
Published: 18 March 2020

http://www.aimspress.com/journal/Math

Research article

On the number of irreducible polynomials of special kinds in finite fields

Weihua Li, Chengcheng Fang and Wei Cao*

School of Mathematics and Statistics, Ningbo University, Ningbo 315211, P. R. China

* **Correspondence:** Email: caowei@nbu.edu.cn.

Abstract: Let $\mathbb{F}_q$ be the finite field of order q and $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$. For a positive divisor n_1 of n, define the n_1-traces of $f(x)$ to be $\mathrm{Tr}(\alpha; n_1) = \alpha + \alpha^q + \cdots + \alpha^{q^{n_1-1}}$ where α's are the roots of $f(x)$. Let $N_q^*(n; n_1)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ with nozero n_1-traces. Ruskey, Miers and Sawada have found the formula for $N_q^*(n; n)$. Based on the properties of linearized polynomials, we obtain the formula for $N_q^*(n; n_1)$ in the general case, including a new proof to the result by Ruskey, Miers and Sawada.

Keywords: finite field; irreducible polynomial; linearized polynomial
Mathematics Subject Classification: 11T06, 11T55

1. Introduction

The polynomials of special kinds in finite fields have attracted a lot of research interest (see, e.g., [1–3, 6, 9]). Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p and $n \geq 1$ be an integer. Let $I_q(n)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ and $\mu(\cdot)$ the Möbius function. Gauss [4] found that

$$I_q(n) = \sum_{d|n} \mu(d) q^{\frac{n}{d}}/n. \tag{1.1}$$

Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$ be an irreducible polynomial. Suppose that α is a root of $f(x)$, then all the roots of $f(x)$ are $\alpha^{q^i}, i = 0, 1, \ldots, n-1$. The *trace function* of α is defined to be $\mathrm{Tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$. So $-a_1 = \mathrm{Tr}(\alpha)$ and therefore $-a_1$ is also called the *trace* of $f(x)$. Let $N_q(n)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ with nonzero traces. Suppose $n = mp^e$ with $p \nmid m$. Carlitz [1] and Ruskey, Miers and Sawada [12] obtained that:

Theorem 1.1. *The number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ with nonzero traces is given by*

$$N_q(n) = (q-1) \sum_{d|m} \mu(d) q^{\frac{n}{d}}/qn.$$

An irreducible polynomial in $\mathbb{F}_q[x]$ is called a *normal polynomial* if its roots are linearly independent over $\mathbb{F}_q$. All the roots of a normal polynomial of degree n over $\mathbb{F}_q$ form a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Normal bases over finite fields have proved very useful for fast arithmetic computations with potential applications to coding theory and to cryptography (see, e.g., [6] and [7]). It is not easy to determine whether a given irreducible polynomial is normal or not. Let $\phi(\cdot)$ denote the Euler totient function. Using Theorem 1.1 and other results, Huang, Han and Cao [5] showed that:

Theorem 1.2. *The following inequality holds*

$$q^{n-m}\prod_{d|m}(q^{\tau(d)}-1)^{\phi(d)/\tau(d)} \leqslant (q-1)\sum_{d|m}\mu(d)q^{n/d}/q, \tag{1.2}$$

where $\tau(d)$ is the order of q modulo d. Furthermore, the following statements are equivalent:

(i) *Inequality (1.2) becomes an equality.*
(ii) *$n = p^e$, or n is a prime different from p and q is a primitive root modulo n.*
(iii) *Every irreducible polynomial of degree n over $\mathbb{F}_q$ with nonzero trace is a normal polynomial.*

Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ as before. For a positive divisor n_1 of n, define the *n_1-traces* of $f(x)$ to be $\mathrm{Tr}(\alpha; n_1) = \alpha + \alpha^q + \cdots + \alpha^{q^{n_1-1}}$ where α's are the roots of $f(x)$. Let $N_q^*(n; n_1)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ with nozero n_1-traces. Obviously, the function $\mathrm{Tr}(\alpha; n_1)$ generalizes the usual trace function $\mathrm{Tr}(\alpha)$. Gauss's formula (1.1) gives the formula for $N_q^*(n; 1)$ for $n \geq 2$ and Theorem 1.1 gives the formula for $N_q^*(n; n)$. In this paper, we obtain the explicit formula for $N_q^*(n; n_1)$ in the general case, including a new proof to Theorem 1.1.

To state our result, we need to introduce more notation and convention.

- Assume that $n = mp^e$ and $n_1 = m_1 p^{e_1}$ with $n_1 \mid n$ and $p \nmid mm_1$.
- For a positive integer d, let $\mathfrak{P}(d)$ denote the set of all distinct positive prime divisors of d. Assume that $\mathfrak{P}(n) = \{p_1, p_2, \ldots, p_k\}$ and $p_k = p$ if $e \geq 1$.
- Without loss of generality, assume that $\{a \in \mathfrak{P}(n) : a \in \mathfrak{P}(m_1), a \notin \mathfrak{P}(\frac{m}{m_1})\} = \{p_1, \ldots, p_t\}$ with $t \leq k$. Write $m_1' = p_1 \cdots p_t$.

The following is the main theorem of this paper.

Theorem 1.3 (Main Theorem)**.** *With the above notation and convention, we have*

$$N_q^*(n; n_1) = \begin{cases} [\sum_{d|n}\mu(d)q^{\frac{n}{d}} - \sum_{d|m_1'}\mu(d)(q^{\frac{n_1}{d}-1} - q^{\frac{n_1}{pd}})]/n & \text{if } e_1 = e > 0 \text{ and } k = t+1, \\ (\sum_{d|n}\mu(d)q^{\frac{n}{d}} - \sum_{d|m_1'}\mu(d)q^{\frac{n_1}{d}-1})/n & \text{if } e_1 = e = 0 \text{ and } k = t, \\ \sum_{d|n}\mu(d)q^{\frac{n}{d}}/n & \text{otherwise.} \end{cases}$$

In particular, for $n_1 = 1$,

$$N_q^*(n; 1) = \begin{cases} I_q(n) - 1 = q - 1 & \text{if } n = 1, \\ I_q(n) = \sum_{d|n}\mu(d)q^{\frac{n}{d}}/n & \text{if } n > 1, \end{cases}$$

and for $n_1 = n$,

$$N_q^*(n; n) = N_q(n) = (q-1)\sum_{d|m}\mu(d)q^{\frac{n}{d}}/qn.$$

Let $N_q^0(n;n_1)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ with zero n_1-traces. The following corollary is a direct consequence of Theorem 1.3.

Corollary 1.4. *With the above notation and convention, we have*

$$N_q^0(n;n_1)=\begin{cases}[\sum\limits_{d|m_1'}\mu(d)(q^{\frac{n_1}{d}-1}-q^{\frac{n_1}{pd}})]/n & \text{if } e_1=e>0 \text{ and } k=t+1,\\ (\sum\limits_{d|m_1'}\mu(d)q^{\frac{n_1}{d}-1})/n & \text{if } e_1=e=0 \text{ and } k=t,\\ 0 & \text{otherwise.}\end{cases}$$

Since our method is based on the properties of linearized polynomials in finite fields, we will introduce them in the next section. The proof of Theorem 1.3 will be given in Section 3.

2. Linearized polynomials

Linearized polynomials are also called q-polynomials in the literature. Many definitions and results of this section go back to the fundamental papers of Ore [8–11], and we just list them without examples and proofs for the sake of brevity; see [6] for further details.

Let r be a positive integer. A polynomial of the form $L(x)=\sum_{i=0}^{n}c_ix^{q^i}$ with coefficients in an extension filed $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$ is called a *linearized polynomial* over $\mathbb{F}_{q^r}$. The polynomials $l(x)=\sum_{i=0}^{n}c_ix^i$ and $L(x)=\sum_{i=0}^{n}c_ix^{q^i}$ over $\mathbb{F}_{q^r}$ are called *q-associates* of each other. More specially, $l(x)$ is the *conventional q-associate* of $L(x)$ and $L(x)$ is the *linearized q-associate* of $l(x)$. Given two linearized polynomials $L_1(x)$ and $L_2(x)$ over $\mathbb{F}_{q^r}$, we define *symbolic multiplication* by $L_1(x)\otimes L_2(x)=L_1(L_2(x))$. The ordinary product of linearized polynomials need not to be a linearized polynomial. And the set of linearized polynomials over $\mathbb{F}_q$ forms an integral domain under the operations of symbolic multiplication and ordinary addition.

If $L_1(x)$ and $L_2(x)$ are two linearized polynomials over $\mathbb{F}_q$, we say that $L_1(x)$ *symbolically divides* $L_2(x)$ (or that $L_2(x)$ is *symbolically divisible* by $L_1(x)$) if $L_2(x)=L_1(x)\otimes L(x)$ for some linearized polynomial $L(x)$ over $\mathbb{F}_q$. Similarly, one can define *symbolic factorization* and *symbolic irreducibility* for linearized polynomials.

Lemma 2.1. ([6, Lemma 3.59]) *Let $L_1(x)$ and $L_2(x)$ be linearized polynomials over $\mathbb{F}_q$ with conventional q-associates $l_1(x)$ and $l_2(x)$. Then $l(x)=l_1(x)l_2(x)$ and $L(x)=L_1(x)\otimes L_2(x)$ are q-associates of each other.*

The following criterion is an immediate consequence of the lemma above.

Corollary 2.2. *Let $L_1(x)$ and $L(x)$ be linearized polynomials over $\mathbb{F}_q$ with conventional q-associates $l_1(x)$ and $l(x)$. Then $L_1(x)$ symbolically divides $L(x)$ if and only if $l_1(x)$ divides $l(x)$. In particular, $L(x)$ is symbolically irreducible over $\mathbb{F}_q$ if and only if $l(x)$ is irreducible over $\mathbb{F}_q$.*

Let $L(x)$ be a linearized polynomial over $\mathbb{F}_q$ with conventional q-associate $l(x)$. We write $L(x)^{\otimes e}:=\underbrace{L(x)\otimes\cdots\otimes L(x)}_{e}$ for short. Let $L(x)=\otimes_{i=1}^{r}L_i(x)^{\otimes e_i}$ be the symbolic factorization with distinct symbolically irreducible linearized polynomials $L_i(x)$ over $\mathbb{F}_q$, then by Lemma 2.1, $l(x)=\prod_{i=1}^{r}l_i(x)^{e_i}$ is the canonical factorization of $l(x)$ in $\mathbb{F}_q[x]$, where $l_i(x)$ is the conventional q-associate of $L_i(x)$.

3. Proof of main theorem

For a positive integer d, let $\varphi_d(x)$ denote the dth cyclotomic polynomial of degree $\phi(d)$ where $\phi(d)$ is the Euler totient function, and let $\Psi_d(x)$ denote the linearized q-associate of $\varphi_d(x)$. The following lemma is well known.

Lemma 3.1. ([6, Theorems 2.45 and 2.47])

$$x^n - 1 = (x^m - 1)^{p^e} = \prod_{d|m} (\varphi_d(x))^{p^e}.$$

As a direct consequence of Lemmas 2.1 and 3.1, we have

Corollary 3.2.

$$x^{q^n} - x = \bigotimes_{d|m} \Psi_d(x)^{\otimes p^e}.$$

Definition 3.3. We define

$$A = \{\alpha \in \mathbb{F}_{q^n} : \alpha + \alpha^q + \cdots + \alpha^{q^{n_1-1}} = 0\},$$

and for each $p_i \in \mathfrak{P}(n)$, we define

$$A_{p_i} = \mathbb{F}_{q^{n/p_i}} = \{\alpha \in \mathbb{F}_{q^n} : \alpha^{q^{\frac{n}{p_i}}} - \alpha = 0\}.$$

Remark 3.4. (i) From the definition of A_{p_i}, one easily knows that it is just the finite field of size q^{n/p_i}. However, since the sets A and A_{p_i} will be considered together later, we adopt this notation to keep consistency.

(ii) Let $\alpha \in \mathbb{F}_{q^n} \setminus (\bigcup_{p_i \in \mathfrak{P}(n)} A_{p_i} \bigcup A)$. Then from the definition above, we know that the n_1-trace of α over $\mathbb{F}_q$ is nonzero, and that the degree of the minimal polynomial of α over $\mathbb{F}_q$ is just n. So α and all its conjugates in $\mathbb{F}_{q^n}$ form the roots of an irreducible polynomial of degree n over $\mathbb{F}_q$ with nonzero n_1-traces.

To calculate the intersection of A and A_{p_i}'s, we need to factorize the two polynomials $x + x^q + \cdots + x^{q^{n_1-1}}$ and $x^{q^{\frac{n}{p_i}}} - x$ into irreducible linearized polynomials.

Lemma 3.5.

$$A = \{\alpha \in \mathbb{F}_{q^n} : (\alpha^q - \alpha)^{\otimes p^{e_1}-1} \otimes \bigotimes_{1<d|m_1} \Psi_d(\alpha)^{\otimes p^{e_1}} = 0\}, \tag{3.1}$$

and

$$A_{p_i} = \{\alpha \in \mathbb{F}_{q^n} : \bigotimes_{d|\frac{n}{p_i}} \Psi_d(\alpha) = 0\}, \tag{3.2}$$

for $p_i \in \mathfrak{P}(n)$. In particular, if $p_i \neq p$, then

$$A_{p_i} = \{\alpha \in \mathbb{F}_{q^n} : (\alpha^q - \alpha)^{\otimes p^e} \otimes \bigotimes_{1<d|\frac{m}{p_i}} \Psi_d(\alpha)^{\otimes p^e} = 0\}, \tag{3.3}$$

and

$$A_p = \{\alpha \in \mathbb{F}_{q^n} : (\alpha^q - \alpha)^{\otimes p^{e-1}} \otimes \bigotimes_{1<d|m} \Psi_d(\alpha)^{\otimes p^{e-1}} = 0\}. \tag{3.4}$$

Proof. Using Corollary 3.2 and the factorization

$$x^{n_1} - 1 = (x-1)(x-1)^{p^{e_1}-1} \prod_{1<d|m_1} (\varphi_d(x))^{p^{e_1}}$$

that comes from Lemma 3.1, we get (3.1). Similarly, we can get (3.2), (3.3) and (3.4). □

Suppose that $\emptyset \neq J = \{p_{j_1}, \ldots, p_{j_r}\} \subseteq \mathfrak{P}(n)$. Without loss of generality, assume that $\{a \in J : a \in \mathfrak{P}(m_1), a \notin \mathfrak{P}(\frac{m}{m_1})\} = \{p_{j_1}, \ldots, p_{j_t}\}$, and $p = p_{j_r}$ if $p \in J$. Observe that if $p \notin J$, then

$$\gcd(m_1, \frac{m}{p_{j_1} \cdots p_{j_r}}) = \gcd(m_1, \frac{m_1}{p_{j_1} \cdots p_{j_t}} \frac{m}{m_1 p_{j_{t+1}} \cdots p_{j_r}}) = \frac{m_1}{p_{j_1} \cdots p_{j_t}}, \tag{3.5}$$

and if $p = p_{j_r} \in J$, then

$$\gcd(m_1, \frac{m}{p_{j_1} \cdots p_{j_{r-1}}}) = \gcd(m_1, \frac{m_1}{p_{j_1} \cdots p_{j_t}} \frac{m}{m_1 p_{j_{t+1}} \cdots p_{j_{r-1}}}) = \frac{m_1}{p_{j_1} \cdots p_{j_t}}. \tag{3.6}$$

We will use the two observations (3.5) and (3.6) in the lemma below.

Lemma 3.6. (i) *If $p \notin J$ or $p = p_{j_r} \in J$ and $e_1 < e$, then*

$$(\bigcap_{j\in J} A_j) \bigcap A = \{\alpha \in \mathbb{F}_{q^n} : (\alpha^q - \alpha)^{\otimes p^{e_1}-1} \otimes \bigotimes_{1<d|\frac{m_1}{p_{j_1}\cdots p_{j_t}}} \Psi_d(\alpha)^{\otimes p^{e_1}} = 0\}.$$

(ii) *If $p = p_{j_r} \in J$ and $e_1 = e$, then*

$$(\bigcap_{j\in J} A_j) \bigcap A = \{\alpha \in \mathbb{F}_{q^n} : (\alpha^q - \alpha)^{\otimes p^{e_1-1}} \otimes \bigotimes_{1<d|\frac{m_1}{p_{j_1}\cdots p_{j_t}}} \Psi_d(\alpha)^{\otimes p^{e_1-1}} = 0\}.$$

Proof. To calculate $(\bigcap_{j\in J} A_j) \bigcap A$, we first calculate $(\bigcap_{j\in J} A_j)$. By (3.2),

$$\bigcap_{j\in J} A_j = \{\alpha \in \mathbb{F}_{q^n} : \bigotimes_{d|\frac{n}{p_{j_1}\cdots p_{j_r}}} \Psi_d(\alpha) = 0\}. \tag{3.7}$$

If $p \notin J$, then by (3.3) and (3.7),

$$\bigcap_{j\in J} A_j = \{\alpha \in \mathbb{F}_{q^n} : (\alpha^q - \alpha)^{\otimes p^e} \otimes \bigotimes_{1<d|\frac{m}{p_{j_1}\cdots p_{j_r}}} \Psi_d(\alpha)^{\otimes p^e} = 0\}. \tag{3.8}$$

If $p = p_{j_r} \in J$, then by (3.4) and (3.7),

$$\bigcap_{j\in J} A_j = \{\alpha \in \mathbb{F}_{q^n} : (\alpha^q - \alpha)^{\otimes p^{e-1}} \otimes \bigotimes_{1<d|\frac{m}{p_{j_1}\cdots p_{j_{r-1}}}} \Psi_d(\alpha)^{\otimes p^{e-1}} = 0\}. \tag{3.9}$$

Now we calculate $(\bigcap_{j\in J} A_j) \bigcap A$. Recall the observations (3.5) and (3.6) and that $0 \leq e_1 \leq e$ which will be used below. If $p \notin J$, then by (3.1) and (3.8),

$$(\bigcap_{j\in J} A_j) \bigcap A$$

$$=\{\alpha \in \mathbb{F}_{q^n} : (\alpha^q-\alpha)^{\otimes \min\{p^e,p^{e_1}-1\}} \otimes \bigotimes_{1<d|\gcd(m_1,\frac{m}{p_{j_1}\cdots p_{j_r}})} \Psi_d(\alpha)^{\otimes \min\{p^e,p^{e_1}\}} = 0\}$$

$$=\{\alpha \in \mathbb{F}_{q^n} : (\alpha^q-\alpha)^{\otimes p^{e_1}-1} \otimes \bigotimes_{1<d|\frac{m_1}{p_{j_1}\cdots p_{j_t}}} \Psi_d(\alpha)^{\otimes p^{e_1}} = 0\}.$$

If $p = p_{j_r} \in J$, then by (3.1) and (3.9),

$$\begin{aligned}
&(\bigcap_{j\in J} A_j)\bigcap A\\
=&\{\alpha \in \mathbb{F}_{q^n} : (\alpha^q-\alpha)^{\otimes \min\{p^{e-1},p^{e_1}-1\}} \otimes \bigotimes_{1<d|\gcd(m_1,\frac{m}{p_{j_1}\cdots p_{j_{r-1}}})} \Psi_d(\alpha)^{\otimes \min\{p^{e-1},p^{e_1}\}} = 0\}\\
=&\begin{cases}
\{\alpha \in \mathbb{F}_{q^n} : (\alpha^q-\alpha)^{\otimes p^{e_1-1}} \otimes \bigotimes_{1<d|\frac{m_1}{p_{j_1}\cdots p_{j_t}}} \Psi_d(\alpha)^{\otimes p^{e_1-1}} = 0\} & \text{if } e_1 = e,\\
\{\alpha \in \mathbb{F}_{q^n} : (\alpha^q-\alpha)^{\otimes p^{e_1}-1} \otimes \bigotimes_{1<d|\frac{m_1}{p_{j_1}\cdots p_{j_t}}} \Psi_d(\alpha)^{\otimes p^{e_1}} = 0\} & \text{if } e_1 < e.
\end{cases}
\end{aligned}$$

This finishes the proof. □

The following lemma plays a vital role in the proof of our main theorem.

Lemma 3.7. (i) $|A| = q^{n_1-1}$.

(ii) $\left|\bigcap_{j\in J} A_j\right| = q^{\frac{n}{p_{j_1}\cdots p_{j_r}}}$.

(iii) $|(\bigcap_{j\in J} A_j)\bigcap A| = q^{\frac{n_1}{pp_{j_1}\cdots p_{j_t}}}$ *if* $p \in J$ *and* $e_1 = e$.

(iv) $|(\bigcap_{j\in J} A_j)\bigcap A| = q^{\frac{n_1}{p_{j_1}\cdots p_{j_t}}-1}$ *if* $p \notin J$ *or* $e_1 < e$.

Proof. Since (i) and (ii) are trivial, we only need to prove (iii) and (iv). First consider the case $p \notin J$. Set

$$G(x) = (x^q-x)^{\otimes p^{e_1}-1} \otimes \bigotimes_{1<d|\frac{m_1}{p_{j_1}\cdots p_{j_t}}} \Psi_d(x)^{\otimes p^{e_1}}.$$

By Lemma 3.6 (i),

$$(\bigcap_{j\in J} A_j)\bigcap A = \{\alpha \in \mathbb{F}_{q^n} : G(\alpha) = 0\}.$$

Notice that the degree of $G(x)$ is

$$q^{p^{e_1}-1+p^{e_1}(\sum_{d|\frac{m_1}{p_{j_1}\cdots p_{j_t}}}\phi(d)-1)} = q^{\frac{m_1p^{e_1}}{p_{j_1}\cdots p_{j_t}}-1} = q^{\frac{n_1}{p_{j_1}\cdots p_{j_t}}-1},$$

where we use the fact that $\sum_{d|\frac{m_1}{p_{j_1}\cdots p_{j_t}}} \phi(d) = \frac{m_1}{p_{j_1}\cdots p_{j_r}}$. So $G(x)$ has $q^{\frac{n_1}{p_{j_1}\cdots p_{j_t}}-1}$ simple roots. Similarly for the case $p \in J$, and we can get

$$|(\bigcap_{j\in J} A_j)\bigcap A| = \begin{cases}
q^{\frac{m_1p^{e_1-1}}{p_{j_1}\cdots p_{j_t}}} = q^{\frac{n_1}{pp_{j_1}\cdots p_{j_t}}} & \text{if } p = p_{j_r} \in J \text{ and } e_1 = e,\\
q^{\frac{m_1p^{e_1}}{p_{j_1}\cdots p_{j_t}}-1} = q^{\frac{n_1}{p_{j_1}\cdots p_{j_t}}-1} & \text{if } p \notin J \text{ or } e_1 < e.
\end{cases}$$

The result follows. □

Now we are in the position to prove our main theorem.

Proof of Theorem 1.3. Write $A_i = A_{p_i} (i = 1, \ldots, k)$ for short. Let $\alpha \in \mathbb{F}_{q^n} \backslash (\bigcup_{i=1}^{k} A_i \bigcup A)$. By Remark 3.4 (ii), we know that $\mathrm{Tr}(\alpha; n_1) \neq 0$ and that the degree of the minimal polynomial of α over $\mathbb{F}_q$ is n. Since all the conjugates of α have the same property, namely, $\mathrm{Tr}(\alpha^{q^i}; n_1) \neq 0$ and the degree of the minimal polynomial of α^{q^i} over $\mathbb{F}_q$ is n for $i = 0, 1, \ldots, n-1$, we have

$$N_q^*(n; n_1) = \Big|\mathbb{F}_{q^n} \backslash (\bigcup_{i=1}^{k} A_i \bigcup A)\Big|/n. \tag{3.10}$$

We first consider the simplest two cases that $e_1 < e$ and $e_1 = e = 0$, in which Lemma 3.7 (iii) is not used that makes the calculation relatively easy. By the inclusion-exclusion principle and Lemma 3.7,

$$\begin{aligned}
&\Big|\mathbb{F}_{q^n} \backslash (\bigcup_{i=1}^{k} A_i \bigcup A)\Big| \\
= \; & q^n + \sum_{l=1}^{k} (-1)^l \sum_{|I|=l} \Big| \bigcap_{i \in I \subseteq \{1,\ldots,k\}} A_i \Big| + \sum_{l=1}^{k+1} (-1)^l \sum_{l_1+l_2=l-1} \Big| \bigcap_{\substack{i \in I_1 \subseteq \{1,\ldots,t\} \\ |I_1|=l_1}} A_i \bigcap \bigcap_{\substack{j \in I_2 \subseteq \{t+1,\ldots,k\} \\ |I_2|=l_2}} A_j \bigcap A \Big| \\
= \; & q^n + \sum_{l=1}^{k} (-1)^l \sum_{1 \le i_1 < \cdots < i_l \le k} q^{\frac{n}{p_{i_1} \cdots p_{i_l}}} + \sum_{l=1}^{k+1} (-1)^l \sum_{l_1+l_2=l-1} \binom{k-t}{l_2} \sum_{1 \le i_1 < \cdots < i_{l_1} \le t} q^{\frac{n_1}{p_{i_1} \cdots p_{i_{l_1}}} - 1}.
\end{aligned}$$

For a positive integer, let $\omega(d)$ denote the number of distinct prime factors of d. Recall $\mathfrak{P}(n) = \{p_1, p_2, \ldots, p_k\}$ and $m_1' = p_1 \cdots p_t$. Hence the above equation can be rewritten as

$$\Big|\mathbb{F}_{q^n} \backslash (\bigcup_{i=1}^{k} A_i \bigcup A)\Big| = \sum_{d|n} \mu(d) q^{\frac{n}{d}} - \sum_{l=0}^{k} (-1)^l \sum_{d|m_1'} \binom{k-t}{l-\omega(d)} q^{\frac{n_1}{d}-1}. \tag{3.11}$$

Note that

$$\begin{aligned}
&\sum_{l=0}^{k} (-1)^l \sum_{d|m_1'} \binom{k-t}{l-\omega(d)} q^{\frac{n_1}{d}-1} \qquad (3.12) \\
=& q^{n_1-1} - \sum_{i=1}^{t} q^{\frac{n_1}{p_i}-1} - \binom{k-t}{1} q^{n_1-1} + \sum_{1 \le j_1 < j_2 \le t} q^{\frac{n_1}{p_{j_1} p_{j_2}}-1} + \binom{k-t}{1} \sum_{i=1}^{t} q^{\frac{n_1}{p_i}-1} \\
&+ \binom{k-t}{2} q^{n_1-1} - \sum_{1 \le j_1 < j_2 < j_3 \le t} q^{\frac{n_1}{p_{j_1} p_{j_2} p_{j_3}}-1} - \binom{k-t}{1} \sum_{1 \le j_1 < j_2 \le t} q^{\frac{n_1}{p_{j_1} p_{j_2}}-1} \\
&- \binom{k-t}{2} \sum_{i=1}^{t} q^{\frac{n_1}{p_i}-1} - \binom{k-t}{3} q^{n_1-1} + \cdots \\
=& \sum_{d|m_1'} \mu(d) q^{\frac{n_1}{d}-1} - \binom{k-t}{1} \sum_{d|m_1'} \mu(d) q^{\frac{n_1}{d}-1} + \binom{k-t}{2} \sum_{d|m_1'} \mu(d) q^{\frac{n_1}{d}-1} + \cdots \\
=& \begin{cases} \sum\limits_{d|m_1'} \mu(d) q^{\frac{n_1}{d}-1} & \text{if } k = t, \\ 0 & \text{if } k > t. \end{cases}
\end{aligned}$$

By (3.10), (3.11) and (3.12), we get

$$N_q^*(n;n_1)=\begin{cases}\sum\limits_{d|n}\mu(d)q^{\frac{n}{d}}/n & \text{if } e_1<e \text{ or } e_1=e=0 \text{ and } k>t,\\ (\sum\limits_{d|n}\mu(d)q^{\frac{n}{d}}-\sum\limits_{d|m_1'}\mu(d)q^{\frac{n_1}{d}-1})/n & \text{if } e_1=e=0 \text{ and } k=t.\end{cases} \tag{3.13}$$

Next we consider the more complicated case that $e_1=e>0$, in which Lemma 3.7 (iii) is used that makes the calculation relatively lengthy. We omit some detail due to the similar deduction and notation as above. Note that $p_k=p$ in this case by assumption. By the inclusion-exclusion principle,

$$\begin{aligned}&\Big|\mathbb{F}_{q^n}\backslash(\bigcup_{i=1}^{k}A_i\bigcup A)\Big| \qquad (3.14)\\ =\;& q^n+\sum_{l=1}^{k}(-1)^l\sum_{|I|=l}\Big|\bigcap_{i\in I\subseteq\{1,\dots,k\}}A_i\Big|\\ &+\sum_{l=1}^{k}(-1)^l\sum_{l_1+l_2=l-1}\Big|\bigcap_{\substack{i\in I_1\subseteq\{1,\dots,t\}\\|I_1|=l_1}}A_i\bigcap\bigcap_{\substack{j\in I_2\subseteq\{t+1,\dots,k-1\}\\|I_2|=l_2}}A_j\bigcap A\Big|\\ &+\sum_{l=2}^{k+1}(-1)^l\sum_{l_1+l_2=l-2}\Big|\bigcap_{\substack{i\in I_1\subseteq\{1,\dots,t\}\\|I_1|=l_1}}A_i\bigcap\bigcap_{\substack{j\in I_2\subseteq\{t+1,\dots,k-1\}\\|I_2|=l_2}}A_j\bigcap A_k\bigcap A\Big|.\end{aligned}$$

By Lemma 3.7,

$$\begin{aligned}&\sum_{l=1}^{k}(-1)^l\sum_{l_1+l_2=l-1}\Big|\bigcap_{\substack{i\in I_1\subseteq\{1,\dots,t\}\\|I_1|=l_1}}A_i\bigcap\bigcap_{\substack{j\in I_2\subseteq\{t+1,\dots,k-1\}\\|I_2|=l_2}}A_j\bigcap A\Big| \qquad (3.15)\\ =\;&\sum_{l=1}^{k}(-1)^l\sum_{l_1+l_2=l-1}\binom{k-t-1}{l_2}\sum_{1\le i_1<\cdots<i_{l_1}\le t}q^{\frac{n_1}{p_{i_1}\cdots p_{i_{l_1}}}-1}\\ =\;&-\sum_{l=0}^{k-1}(-1)^l\sum_{d|m_1'}\binom{k-t-1}{l-\omega(d)}q^{\frac{n_1}{d}-1},\end{aligned}$$

and

$$\begin{aligned}&\sum_{l=2}^{k+1}(-1)^l\sum_{l_1+l_2=l-2}\Big|\bigcap_{\substack{i\in I_1\subseteq\{1,\dots,t\}\\|I_1|=l_1}}A_i\bigcap\bigcap_{\substack{j\in I_2\subseteq\{t+1,\dots,k-1\}\\|I_2|=l_2}}A_j\bigcap A_k\bigcap A\Big| \qquad (3.16)\\ =\;&\sum_{l=2}^{k+1}(-1)^l\sum_{l_1+l_2=l-2}\binom{k-t-1}{l_2}\sum_{1\le i_1<\cdots<i_{l_1}\le t}q^{\frac{n_1}{pp_{i_1}\cdots p_{i_{l_1}}}}.\\ =\;&\sum_{l=0}^{k-1}(-1)^l\sum_{d|m_1'}\binom{k-t-1}{l-\omega(d)}q^{\frac{n_1}{pd}}.\end{aligned}$$

It follows from (3.14), (3.15) and (3.16) that

$$\left|\mathbb{F}_{q^n}\backslash(\bigcup_{i=1}^{k} A_i \bigcup A)\right| = \sum_{d|n}\mu(d)q^{\frac{n}{d}} - \sum_{l=0}^{k-1}(-1)^l \sum_{d|m_1'}\binom{k-t-1}{l-\omega(d)}(q^{\frac{n_1}{d}-1} - q^{\frac{n_1}{pd}}). \tag{3.17}$$

Similar to (3.12), we have

$$\begin{aligned}&\sum_{l=0}^{k-1}(-1)^l \sum_{d|m_1'}\binom{k-t-1}{l-\omega(d)}(q^{\frac{n_1}{d}-1} - q^{\frac{n_1}{pd}}) \\ &= \begin{cases} \sum\limits_{d|m_1'}\mu(d)q^{\frac{n_1}{d}-1} - \sum\limits_{d|m_1'}\mu(d)q^{\frac{n_1}{pd}} & \text{if } k = t+1, \\ 0 & \text{if } k > t+1, \end{cases}\end{aligned} \tag{3.18}$$

By (3.10), (3.17) and (3.18), we get

$$N_q^*(n;n_1) = \begin{cases} \sum\limits_{d|n}\mu(d)q^{\frac{n}{d}}/n & \text{if } e_1 = e > 0 \text{ and } k > t+1, \\ [\sum\limits_{d|n}\mu(d)q^{\frac{n}{d}} - \sum\limits_{d|m_1'}\mu(d)(q^{\frac{n_1}{d}-1} - q^{\frac{n_1}{pd}})]/n & \text{if } e_1 = e > 0 \text{ and } k = t+1. \end{cases} \tag{3.19}$$

Putting (3.13) and (3.19) together, we obtain

$$N_q^*(n;n_1) = \begin{cases} [\sum\limits_{d|n}\mu(d)q^{\frac{n}{d}} - \sum\limits_{d|m_1'}\mu(d)(q^{\frac{n_1}{d}-1} - q^{\frac{n_1}{pd}})]/n & \text{if } e_1 = e > 0 \text{ and } k = t+1, \\ (\sum\limits_{d|n}\mu(d)q^{\frac{n}{d}} - \sum\limits_{d|m_1'}\mu(d)q^{\frac{n_1}{d}-1})/n & \text{if } e_1 = e = 0 \text{ and } k = t, \\ \sum\limits_{d|n}\mu(d)q^{\frac{n}{d}}/n & \text{otherwise,} \end{cases} \tag{3.20}$$

as desired.

Now suppose that $n_1 = 1$ in which $e_1 = 0$. So the case $e_1 = e > 0$ is excluded. For the case $e_1 = e = 0$ and $k = t$, since $t = 1$, we must have $k = 1$ and hence $n = 1$. By (3.20),

$$N_q^*(1;1) = \sum_{d|1}\mu(d)q^{\frac{1}{d}} - \sum_{d|1}\mu(d)q^{\frac{1}{d}-1} = q - 1 = I_q(1) - 1.$$

For the other cases, by (3.20) we get $N_q^*(n;1) = \sum_{d|n}\mu(d)q^{\frac{n}{d}}/n = I_q(n)$.

Finally suppose that $n_1 = n$ in which $m_1 = m$ and $e = e_1$. There are two subcases: $e = e_1 = 0$ and $e = e_1 > 0$.

- If $e = e_1 = 0$, then $n = m = n_1 = m_1$, and by (3.20) it is easy to verify that

$$N_q^*(n;n) = (\sum_{d|n}\mu(d)q^{\frac{n}{d}} - \sum_{d|m_1'}\mu(d)q^{\frac{n_1}{d}-1})/n = (q-1)\sum_{d|m}\mu(d)q^{\frac{n}{d}}/qn.$$

- If $e = e_1 > 0$, then $k = t+1$ and hence by (3.20),

$$N_q^*(n;n) \;=\; [\sum_{d|n}\mu(d)q^{\frac{n}{d}} - \sum_{d|m_1'}\mu(d)(q^{\frac{n_1}{d}-1} - q^{\frac{n_1}{pd}})]/n$$

$$
\begin{aligned}
&= [\sum_{d|m}\mu(d)q^{\frac{n}{d}} - \sum_{d|m}\mu(d)q^{\frac{n}{pd}} - \sum_{d|m}\mu(d)(q^{\frac{n}{d}-1} - q^{\frac{n}{pd}})]/n \\
&= (\sum_{d|m}\mu(d)q^{\frac{n}{d}} - \sum_{d|m}\mu(d)q^{\frac{n}{d}-1})/n \\
&= (q-1)\sum_{d|m}\mu(d)q^{\frac{n}{d}}/qn.
\end{aligned}
$$

The proof is complete. □

4. Some remarks

The main contribution of this paper is to provide a new proof to Theorem 1.1 and its generalizations. To be precise, based on the properties of linearized polynomials, we count the monic irreducible polynomials of degree n over $\mathbb{F}_q$ with nozero n_1-traces, where n_1 is a divisor of n. Since n_1-traces have the close relationship with the roots (and hence the coefficients) of the associated polynomial, this approach may be adopted to deal with the other enumeration problems concerning the irreducible polynomials with the restricted coefficients in finite fields.

As one reviewer pointed out, the first two cases (i.e. $e_1 = e > 0$ and $k = t + 1$, respectively, $e_1 = e = 0$ and $k = t$) in Theorem 1.3 only occur for $n = n_1$. Thus it remains to consider the case $n < n_1$, which can be deduced from the additive version of Hilbert's Theorem 90. However, if we drop out the restriction that the polynomials must be irreducible, i.e., allowing the degree of α in $\mathrm{Tr}(\alpha; n_1)$ to be less than n, our approach still works while Hilbert's Theorem 90 may not be valid again.

Acknowledgments

The authors sincerely thank the referees for their helpful comments which led to a substantial improvement of this paper. This work was jointly supported by the National Natural Science Foundation of China (Grant No. 11871291) and Ningbo Natural Science Foundation (Grant No. 2019A610035), and sponsored by the K. C. Wong Magna Fund in Ningbo University.

Conflict of interest

The authors declare that there is no conflict of interest.

References

1. L. Carlitz, *A theorem of Dickson on irreducible polynomials*, P. Am. Math. Soc., **3** (1952), 693–700.
2. K. M. Cheng, *Permutational behavior of reversed Dickson polynomials over finite fields II*, AIMS. Math., **2** (2017), 586–609.
3. K. M. Cheng, S. F. Hong, *The first and second moments of reversed Dickson polynomials over finite fields*, J. Number Theory, **187** (2018), 166–188.
4. C. F. Gauss, *Arithmetische Untersuchungen*, Chelsea, 1965.

5. H. Huang, S. M. Han, W. Cao, *Normal bases and irreducible polynomials*, Finite Fields Th. App., **50** (2018), 272–278.
6. R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.
7. G. L. Mullen, D. Panario, *Handbook of Finite Fields*, CRC Press, 2013.
8. O. Ore, *Theory of non-commutative polynomials*, Ann. Math., **34** (1933), 480–508.
9. O. Ore, *On a special class of polynomials*, T. Am. Math. Soc., **35** (1933), 559–584.
10. O. Ore, *Contributions to the theory of finite fields*, T. Am. Math. Soc., **36** (1934), 243–274.
11. O. Ore, *Some studies on cyclic determinants*, Duke Math. J., **18** (1951), 343–354.
12. F. Ruskey, C. R. Miers, J. Sawada, *The number of irreducible polynomials and Lyndon words with given trace*, SIAM J. Discrete Math., **14** (2001), 240–245.

AIMS Press