Improved Error Bounds for the Number of Irreducible Polynomials and Self-Reciprocal Irreducible Monic Polynomials with Prescribed Coefficients over a Finite Field

Zhicheng Gao
School of Mathematics and Statistics, Carleton University, Canada

Abstract

A polynomial is called self-reciprocal (or palindromic) if the sequence of its coefficients is palindromic. In this paper we obtain improved error bounds for the number of irreducible polynomials and self-reciprocal irreducible monic polynomials with prescribed coefficients over a finite field. The improved bounds imply that self-reciprocal irreducible monic polynomials with degree $2d$ and prescribed ℓ leading coefficients always exist provided that ℓ is slightly less than $d/2$.

2012 ACM Subject Classification Mathematics of computing → Generating functions; Mathematics of computing → Enumeration

Keywords and phrases finite fields, irreducible polynomials, prescribed coefficients, generating functions, Weil bounds, self-reciprocal

Digital Object Identifier 10.4230/LIPIcs.AofA.2022.9

Funding Research supported by NSERC (RGPIN 04010-2015) and Carleton University Development Grant (189035).

Acknowledgements I would like to thank the referees for their helpful comments which improve the presentation of the paper.

1 Introduction

The existence of irreducible polynomials over finite fields with restricted coefficients play important roles in coding theory and information theory (see, e.g., [13, 10]). The main objective of this paper is to improve some well-known error bounds on the number of irreducible polynomials and self-reciprocal irreducible monic polynomials with prescribed coefficients. Asymptotic formulas with good error bounds played essential roles in proving the existence of irreducible polynomials and self-reciprocal irreducible monic polynomials with prescribed coefficients. For example, the famous Hansen-Mullen conjecture on the existence of irreducible polynomials with one prescribed coefficient was proved asymptotically by Wan [14] using the Weil bound on character sums. Practical error bounds allow Ham and Mullen [7] to confirm the conjecture for small degrees and finite fields. Panario and Tzanakis [11] used Wan's approach to study the extended Hansen-Mullen conjecture by considering several prescribed coefficients. Garefalakis and Kapetanakis [5] used Wan's approach to prove the existence of self-reciprocal irreducible monic polynomials with one prescribed coefficient. Ha and Pollack [6, 12] obtained bounds for several prescribed coefficients using a different approach based on the circle method. Our approach uses generating functions whose coefficients are from the group algebra defined in terms of the prescribed coefficients.

Throughout the paper, we shall use the following notations.

- $\mathbb{F}_q$ denotes the finite field with q elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.
- $\mathcal{M}_q$ denotes the set of monic polynomials over $\mathbb{F}_q$ and $\mathcal{M}_q(d) = \{f : f \in \mathcal{M}_q, \deg(f) = d\}$.

- For a polynomial f, $\deg(f)$ denotes the degree of f, and $f^*(x) = x^{\deg(f)} f(1/x)$ is the *reciprocal* of f. If $f^* = f$, then f is called *self-reciprocal* or *palindromic*.
- $\mathcal{I}_q \subseteq \mathcal{M}_q$ denotes the set of irreducible monic polynomials and $\mathcal{I}_q(d) = \mathcal{I}_q \cap \mathcal{M}_q(d)$.
- $\mathcal{S}_q \subseteq \mathcal{I}_q$ denotes the set of self-reciprocal irreducible monic polynomials. Since every odd-degree self-reciprocal polynomial contains the factor $x+1$, we only need to consider $\mathcal{S}_q(d) = \{f : f \in \mathcal{S}_q, \deg(f) = 2d\}$.
- For a generating function F, $[\,]F$ extracts the relevant coefficient from F.

Given non-negative integers ℓ, t, we say that two polynomials $f, g \in \mathcal{M}_q$ are *equivalent* with respect to ℓ, t if

$$\left[x^{\deg(f)-j}\right] f(x) = \left[x^{\deg(g)-j}\right] g(x), 1 \le j \le \ell,$$
$$\left[x^{j}\right] f(x) = \left[x^{j}\right] g(x), 0 \le j \le t-1.$$

Let $\langle f \rangle$ denote the equivalence class represented by f. It is known [15, 8, 9] that the set $\mathcal{E}^{\ell,t}$ of all equivalence classes forms an abelian group under the multiplication $\langle f\rangle\langle g\rangle = \langle fg\rangle$. (When $t > 0$, it is assumed that the constant term is nonzero.)

Given $\varepsilon \in \mathcal{E}^{\ell,t}$ and $\delta \in \mathcal{E}^{\ell,0}$, define

$$I_q(d;\varepsilon) = \left|\{f \in \mathcal{I}_q(d) : \langle f\rangle = \varepsilon\}\right|, \quad S_q(d;\delta) = \left|\{f \in \mathcal{S}_q(d) : \langle f\rangle = \delta\}\right|.$$

The rest of the paper is organized as follows. In Section 2 we state our main results about the bounds for $I_q(d;\varepsilon)$ and $S_q(d;\varepsilon)$. In Section 3 we sketch the proofs of our main results. Section 4 gives some examples to demonstrate the improvement of our bounds over those in [2, 9]. Section 5 concludes the paper.

2 Main results

In the rest of the paper, we shall use the Iverson bracket $[\![P]\!]$ which has value 1 if the predicate P is true and value 0 otherwise. It is easy to see [15, 9] that

$$\left|\mathcal{E}^{\ell,t}\right| = (q - [\![t > 0]\!])q^{\ell+t-1}.$$

For typographical convenience, we shall use $\mathcal{E}^{\ell}$ to denote $\mathcal{E}^{\ell,0}$. For any given q, the following observation [9, Lemma 1.1] will be useful:

$$\mathcal{E}^{\ell,t} \cong \mathcal{E}^{\ell} \times \mathcal{E}^{t-1} \times \mathbb{F}_q^*, \quad t \ge 1. \tag{1}$$

Thus we may focus on the group $\mathcal{E}^{\ell}$. When $t > 0$ and $\varepsilon \in \mathcal{E}^{\ell,t}$, we also write $\varepsilon = (\varepsilon_1, \gamma^m, \varepsilon_2)$ with $\varepsilon_1 \in \mathcal{E}^{\ell}$, $\varepsilon_2 \in \mathcal{E}^{t-1}$, and $1 \le m \le q-1$.

Since $\mathcal{E}^{\ell}$ is abelian, it is isomorphic to a direct product of cyclic groups. Let $\xi_{\ell,1}, \ldots, \xi_{\ell,u_\ell}$ be a fixed minimal set of generators of $\mathcal{E}^{\ell}$, and denote their orders by $r_{\ell,1}, \ldots, r_{\ell,u_\ell}$, respectively. In the rest of the paper, γ denotes a fixed generator of the multiplicative group $\mathbb{F}_q^*$. By (1), each $\varepsilon \in \mathcal{E}^{\ell,t}$ can be written uniquely as

$$\varepsilon = \gamma^{e_0(\varepsilon)} \prod_{h=1}^{u_\ell} \xi_{\ell,h}^{e_{\ell,h}(\varepsilon)} \prod_{i=1}^{u_{t-1}} \xi_{t-1,i}^{e_{t-1,i}(\varepsilon)}, 1 \le e_0(\varepsilon) \le q-1, 1 \le e_{\ell,h}(\varepsilon) \le r_{\ell,u_\ell}, 1 \le e_{t-1,i}(\varepsilon) \le r_{\ell,u_{t-1}}.$$

Thus each $\varepsilon \in \mathcal{E}^{\ell,t}$ can be represented uniquely by either a monic polynomial of degree $\ell + t$ or the *exponent vector* $\vec{e}(\varepsilon) = (e_0(\varepsilon), e_{\ell,1}(\varepsilon), \ldots, e_{\ell.u_\ell}, e_{t-1,1}, \ldots, e_{t-1,u_{t-1}})$. When $t = 0$, it is understood that e_0 is ignored.

Let $\omega_r = \exp(2\pi i/r)$ and $\varepsilon, \varepsilon' \in \mathcal{E}^{\ell,t}$. Define

$$\{\varepsilon^{1/k}\} = \{\delta \in \mathcal{E}^{\ell,t} : \delta^k = \varepsilon\}, \tag{2}$$

$$\mathcal{E}^{\ell,t}(d) = \{\langle f\rangle : f \in \mathcal{M}_q(d)\},$$

$$a(\varepsilon,\varepsilon') = \omega_{q-1}^{e_0(\varepsilon)e_0(\varepsilon')} \prod_{h=1}^{u_\ell} \omega_{r_{\ell,h}}^{e_{\ell,h}(\varepsilon)e_{\ell,h}(\varepsilon')} \prod_{i=1}^{u_{t-1}} \omega_{r_{t-1,i}}^{e_{t-1,i}(\varepsilon)e_{t-1,i}(\varepsilon')}, \tag{3}$$

$$c(d;\varepsilon) = \sum_{\varepsilon' \in \mathcal{E}^{\ell,t}(d)} a(\varepsilon,\varepsilon'), \tag{4}$$

$$P(z;\varepsilon) = 1 + \sum_{d=1}^{\ell+t-1} c(d;\varepsilon) z^d, \tag{5}$$

$$D = \sum_{\varepsilon \neq \langle 1\rangle} \deg(P(z;\varepsilon)). \tag{6}$$

Define

$$D' = \sum_{\delta \in \mathcal{E}^\ell \setminus \{\langle 1\rangle\}} \deg(P(z;\delta,1,\delta)).$$

Since $\deg(P(z;\varepsilon)) \le \ell + t - 1$ and $\deg(P(z;\delta,1,\delta)) \le 2\ell$, we have

$$D \le (\ell + t - 1)(\left|\mathcal{E}^{\ell,t}\right| - 1), \tag{7}$$

$$D' \le 2\ell \left(q^\ell - 1\right). \tag{8}$$

With the above notations, we now state our main results.

▶ **Theorem 1.** *Let $\mathcal{E}$ denote the group $\mathcal{E}^{\ell,t}$ and $\varepsilon \in \mathcal{E}$.*

(a) *We have the following upper bounds:*

$$I_q(d;\varepsilon) \le \frac{1}{|\mathcal{E}|}\frac{q^d - [\![t>0]\!]}{d} + \frac{D}{|\mathcal{E}|}\frac{q^{d/2}}{d} \tag{9}$$

$$\le \frac{1}{|\mathcal{E}|}\frac{q^d}{d} + \frac{(|\mathcal{E}|-1)(\ell+t-1)}{|\mathcal{E}|}\frac{q^{d/2}}{d}. \tag{10}$$

(b) *Assume $\ell + t \le \lceil d/2\rceil - 1$ and let $e_1(q,d) = \min\left\{3.4q^{-d/6}, 0.8\right\}$. We have the following lower bounds:*

$$I_q(d;\varepsilon) \ge \frac{1}{|\mathcal{E}|}\frac{q^d - [\![t>0]\!]}{d} - \left(\frac{D + \left|\{\varepsilon^{1/2}\}\right| [\![2 \mid d]\!]}{|\mathcal{E}|} + e_1(q,d)\right)\frac{q^{d/2}}{d} \tag{11}$$

$$\ge \frac{1}{|\mathcal{E}|}\frac{q^d}{d} - (\ell + t + 1)\frac{q^{d/2}}{d}. \tag{12}$$

▶ Remark.

- The upper bound (10) is given in [9, Theorem 2.4], which follows immediately from (9) and (7). The lower bound (12) is given in [2, Theorem 2.1], which follows immediately from (11), (7) and $|\{\varepsilon^{1/2}\}| \le |\mathcal{E}|$.
- We also note that the upper bound given in [2, Theorem 2.1] is slightly weaker than (10), and the lower bound in [9, Theorem 2.4] is slightly weaker than (12).
- Recall $|\mathcal{E}| = (q - [\![t>0]\!])q^{\ell+t-1}$. When $2 \nmid q$, we also have $\left|\{\varepsilon^{1/2}\}\right| \le 1 + [\![t>0]\!]$.

By (7) and (8), our next theorem improves the error bound in [4, Theorem 3] by a factor of q^ℓ. This improvement enables us to essentially extend the range of ℓ from $d/4$ to $d/2$.

▶ **Theorem 2.** *Let $\varepsilon \in \mathcal{E}^\ell$ and $e_2(q,d) = \min\{7q^{-d/6}, 2\}$. Assume $\ell \le \lceil d/2 \rceil - 1$.*

(a) *We have the following upper bounds:*

$$S_q(d;\varepsilon) \le \frac{1}{2d}q^{d-\ell} + \left(\frac{D'+2D+3[\![2 \mid d]\!]\left|\{\varepsilon^{1/2}\}\right|}{2q^\ell} + e_2(q,d)\right)\frac{q^{d/2}}{d} \tag{13}$$

$$\le \frac{1}{2d}q^{d-\ell} + (2\ell+2.5)\frac{q^{d/2}}{d}. \tag{14}$$

(b) *We have the following lower bounds:*

$$S_q(d;\varepsilon) \ge \frac{1}{2d}q^{d-\ell} - \left(\frac{D'+2D}{2q^\ell} + [\![2 \mid d]\!]\frac{\left|\{\langle 1\rangle^{1/2}\}\right|}{q^\ell} + e_2(q,d)\right)\frac{q^{d/2}}{d} \tag{15}$$

$$\ge \frac{1}{2d}q^{d-\ell} - (2\ell+2)\frac{q^{d/2}}{d}. \tag{16}$$

Consequently $S_q(d;\varepsilon) > 0$ whenever

$$\ell \le \min\left\{\left\lceil\frac{d}{2}\right\rceil - 1, \frac{d}{2} - \log_q(2d+2)\right\}.$$

3 Outline of proofs

Fix ℓ, t and consider the group $\mathcal{E} := \mathcal{E}^{\ell,t}$. In the following, when $t > 0$ and $f(0) = 0$, it is understood that $\langle f\rangle = 0$. Define

$$F(z) = \sum_{f\in\mathcal{M}_q}\langle f\rangle z^{\deg(f)} = \langle 1\rangle + \sum_{d\ge 1}\sum_{f\in\mathcal{M}_q(d)}\langle f\rangle z^d,$$
$$F_q(d;\varepsilon) = d\left[z^d\varepsilon\right]\ln F(z),\ \varepsilon\in\mathcal{E},$$

where

$$\ln F(z) = \sum_{k\ge 1}\frac{(-1)^{k-1}}{k}\left(\sum_{d\ge 1}\sum_{f\in\mathcal{M}_q(d)}\langle f\rangle z^d\right)^k.$$

We note that $F(z)$ is a generating function with coefficients from the group algebra $\mathbb{C}[\mathcal{E}]$. Using the fact that every polynomial is uniquely factored into irreducible polynomials and $\langle f\rangle\langle g\rangle = \langle fg\rangle$, one can obtain [15, Proposition 2] the following equations:

$$F_q(d;\varepsilon) = \sum_{k\mid d}\frac{d}{k}\sum_{\varepsilon_1\in\{\varepsilon^{1/k}\}} I_q(d/k;\varepsilon_1), \tag{17}$$

$$I_q(d;\varepsilon) = \frac{1}{d}\sum_{k\mid d}\mu(k)\sum_{\varepsilon_1\in\{\varepsilon^{1/k}\}} F_q(d/k;\varepsilon_1). \tag{18}$$

We need a few more notations before stating a formula for $F_q(d;\varepsilon)$ derived in [15]. If $\{\varepsilon^{1/k}\} \ne \emptyset$, we let $\varepsilon^{1/k}$ denote any particular element in $\{\varepsilon^{1/k}\}$. The following simple observations are immediate from (2) and (3).

$$\left\{\varepsilon^{1/k}\right\} = \varepsilon^{1/k}\left\{\langle 1\rangle^{1/k}\right\},$$
$$\left|\left\{\varepsilon^{1/k}\right\}\right| = \left|\left\{\langle 1\rangle^{1/k}\right\}\right| \left[\!\left[\left\{\varepsilon^{1/k}\right\} \neq \emptyset\right]\!\right],$$
$$a(\varepsilon^{-1}, \delta) = a(\varepsilon, \delta^{-1}), \tag{19}$$
$$a(\delta, \varepsilon_1\varepsilon_2) = a(\delta, \varepsilon_1)a(\delta, \varepsilon_2). \tag{20}$$

Set

$$\rho_d(g) := \sum_{\rho} \rho^{-d},$$

where the sum is over all the nonzero roots (with multiplicity) of the polynomial $g \in \mathbb{C}[z]$. Theorem 3 in [15] gives the following formula (written in slightly different notation).

▶ **Proposition 3.** *Let $\mathcal{E}$ denote the group $\mathcal{E}^{\ell,t}$ and let $\varepsilon \in \mathcal{E}$. We have*

$$F_q(d;\varepsilon) = \frac{q^d - [\![t>0]\!]}{|\mathcal{E}|} - \frac{1}{|\mathcal{E}|}\sum_{\delta\in\mathcal{E}\setminus\{\langle 1\rangle\}} a\left(\delta, \varepsilon^{-1}\right)\rho_d(P(z;\delta)). \tag{21}$$

The following lemma simplifies sums involving $F_q(d;\varepsilon)$ over some subgroups of $\mathcal{E}^{\ell,t}$, which play a crucial role in the proofs of Theorems 1 and 2.

▶ **Lemma 4.** *Let $\mathcal{E}$ denote the group $\mathcal{E}^{\ell,t}$.*

(a) *For each $\varepsilon \in \mathcal{E}$, we have*

$$\begin{aligned}
&\sum_{\varepsilon_1\in\{\varepsilon^{1/k}\}} F_q\left(d/k;\varepsilon_1\right)\\
&= \frac{\left|\{\varepsilon^{1/k}\}\right|}{|\mathcal{E}|}\left(q^{d/k} - [\![t>0]\!]\right)\\
&\quad - \frac{\left|\{\varepsilon^{1/k}\}\right|}{|\mathcal{E}|}\sum_{\delta\in\mathcal{E}\setminus\{\langle 1\rangle\}} \left[\!\left[\{\delta^{1/k}\} \neq \emptyset\right]\!\right] a\left(\delta, \varepsilon^{-1/k}\right)\rho_{d/k}(P(z;\delta)) \qquad (22)\\
&\leq \frac{\left|\{\varepsilon^{1/k}\}\right|}{|\mathcal{E}|}\left(q^{d/k} - [\![t>0]\!]\right) + (\ell+t-1)q^{d/2k}. \qquad (23)
\end{aligned}$$

(b) *Fix a generator γ of $\mathbb{F}_q^*$ and recall that $\mathcal{E}^\ell$ denotes the group $\mathcal{E}^{\ell,0}$. For each $\varepsilon \in \mathcal{E}^\ell$, we have*

$$\begin{aligned}
&\sum_{m=1}^{q-1}\sum_{\delta\in\mathcal{E}^\ell} F_q\left(d;\varepsilon\delta^{-1},\gamma^m,\delta\right)\\
&= \frac{q^d-1}{q^\ell} - \frac{1}{q^\ell}\sum_{\delta\neq\langle 1\rangle} a\left(\delta,\varepsilon^{-1/k}\right)\rho_d\left(P(z;\delta,1,\delta)\right), \qquad (24)\\
&\sum_{\varepsilon_1\in\{\varepsilon^{1/k}\}}\sum_{m=1}^{q-1}\sum_{\delta\in\mathcal{E}^\ell} F_q\left(d/k;\varepsilon_1\delta^{-1},\gamma^m,\delta\right)\\
&= \frac{\left|\{\varepsilon^{1/k}\}\right|}{q^\ell}\left(q^{d/k} - 1 - \sum_{\delta\neq\langle 1\rangle,\{\delta^{1/k}\}\neq\emptyset} a\left(\delta,\varepsilon^{-1/k}\right)\rho_{d/k}\left(P(z;\delta,1,\delta)\right)\right). \qquad (25)
\end{aligned}$$

Proof. (a) The well-known identity

$$\sum_{s=0}^{r-1} \omega_r^{sj} = r[\![r \mid j]\!]$$

immediately leads to

$$\sum_{\delta \in \mathcal{E}} a(\delta, \varepsilon) = |\mathcal{E}|[\![\varepsilon = \langle 1 \rangle]\!], \tag{26}$$

$$\sum_{\varepsilon_1 \in \{\varepsilon^{1/k}\}} a(\varepsilon_1, \delta) = \left|\left\{\varepsilon^{1/k}\right\}\right| a(\varepsilon^{1/k}, \delta)[\![\{\delta^{1/k}\} \neq \emptyset]\!]. \tag{27}$$

where $a(\varepsilon^{1/k}, \delta)$ is interpreted as 0 if $\{\varepsilon^{1/k}\} = \emptyset$. It follows from (21) and (27) that

$$\begin{aligned}
&\sum_{\varepsilon_1 \in \{\varepsilon^{1/k}\}} F_q\left(d/k; \varepsilon_1\right) \\
&= \frac{\left|\{\varepsilon^{1/k}\}\right|}{|\mathcal{E}|}\left(q^{d/k} - [\![t > 0]\!]\right) \\
&\quad - \frac{1}{|\mathcal{E}|} \sum_{\delta \in \mathcal{E} \setminus \{\langle 1 \rangle\}} \sum_{\varepsilon_1 \in \{\varepsilon^{1/k}\}} a(\varepsilon_1, \delta^{-1}) \rho_{d/k}(P(z; \delta)) \\
&= \frac{\left|\{\varepsilon^{1/k}\}\right|}{|\mathcal{E}|}\left(q^{d/k} - [\![t > 0]\!]\right) \\
&\quad - \frac{\left|\{\varepsilon^{1/k}\}\right|}{|\mathcal{E}|} \sum_{\delta \in \mathcal{E} \setminus \{\langle 1 \rangle\}} \left[\!\left[\{\delta^{1/k}\} \neq \emptyset\right]\!\right] a\left(\delta, \varepsilon^{-1/k}\right) \rho_{d/k}(P(z; \delta)),
\end{aligned}$$

which is (22). Now (23) follows by noting

$$\sum_{\delta \in \mathcal{E} \setminus \{\langle 1 \rangle\}} \left[\!\left[\{\delta^{1/k}\} \neq \emptyset\right]\!\right] = \frac{|\mathcal{E}|}{\left|\{\langle 1 \rangle^{1/k}\}\right|} - 1. \tag{28}$$

To prove part (b), we use (19), (20), (21), and (26) to obtain

$$\begin{aligned}
&\sum_{m=1}^{q-1} \sum_{\delta \in \mathcal{E}^\ell} F_q\left(d; \varepsilon\delta^{-1}, \gamma^m, \delta\right) \\
&= \frac{(q-1)q^\ell}{|\mathcal{E}^{\ell,\ell+1}|}\left(q^d - 1\right) \\
&\quad - \frac{1}{|\mathcal{E}^{\ell,\ell+1}|} \sum_{(\varepsilon_1, \gamma^n, \varepsilon_2) \neq \langle 1 \rangle} a\left(\varepsilon, \varepsilon_1^{-1}\right) \rho_d\left(P(z; \varepsilon_1, \gamma^n, \varepsilon_2)\right) \sum_{m=1}^{q-1} \omega_{q-1}^{-nm} \sum_{\delta \in \mathcal{E}^\ell} a\left(\delta, \varepsilon_1 \varepsilon_2^{-1}\right) \\
&= \frac{1}{q^\ell}\left(q^d - 1\right) - \frac{1}{q^\ell} \sum_{\delta \neq \langle 1 \rangle} a(\varepsilon^{-1}, \delta) \rho_d\left(P(z; \delta, 1, \delta)\right).
\end{aligned}$$

Now (25) follows from (27). ◀

Proof of Theorem 1. Hsu [9, Theoem 1.3] showed that each (complex) root ρ of $P(z; \delta)$ satisfies

$$|\rho| \geq q^{-1/2}.$$

It follows from (21) that

$$\left|F_q(d;\varepsilon) - \frac{1}{|\mathcal{E}|}\left(q^d - [\![t>0]\!]\right)\right| \le \frac{D}{|\mathcal{E}|}q^{d/2}. \tag{29}$$

By (17), we have

$$I_q(d;\varepsilon) \le \frac{1}{d}F_q(d;\varepsilon).$$

It follows from (29) that

$$I_q(d;\varepsilon) \le \frac{1}{d|\mathcal{E}|}\left(q^d - [\![t>0]\!]\right) + \frac{D}{d|\mathcal{E}|}q^{d/2},$$

which establishes the desired upper bound.

To prove the lower bound, we define

$$\begin{aligned} L_q(d,\ell,t) = {} & \sum_{k\ge 3}[\![k \mid d, \mu(k)=-1]\!]\frac{\left|\{\langle 1\rangle^{1/k}\}\right|}{|\mathcal{E}|}q^{d/k-d/2} \\ & + (\ell+t-1)\sum_{k\ge 2}[\![k \mid d, \mu(k)=-1]\!]\left(1-\frac{\left|\{\langle 1\rangle^{1/k}\}\right|}{|\mathcal{E}|}\right)q^{d/2k-d/2}. \end{aligned} \tag{30}$$

Using (18), (23), and (29), we obtain

$$\begin{aligned} I_q(d;\varepsilon) &\ge \frac{1}{d}F_q(d;\varepsilon) - \frac{1}{d}\sum_{k\mid d}[\![\mu(k)=-1]\!]\sum_{\delta\in\{\varepsilon^{1/k}\}}F_q(d/k;\delta) \\ &\ge \frac{q^d - [\![t>0]\!]}{d|\mathcal{E}|} - \left(\frac{D+\left|\{\varepsilon^{1/2}\}\right|[\![2\mid d]\!]}{|\mathcal{E}|} + L_q(d,\ell,t)\right)\frac{q^{d/2}}{d}. \end{aligned}$$

We now estimate $L_q(d,\ell,t)$ by truncating the sums in (30) and bounding the remainders by geometric sums. For our purpose, we use

$$\begin{aligned} L_q(d;\ell,t) \le {} & \sum_{k=3}^{29}[\![k \mid d, \mu(k)=-1]\!]\frac{\left|\{\langle 1\rangle^{1/k}\}\right|}{|\mathcal{E}|}q^{d/k-d/2} \\ & + (\ell+t-1)\left(1-\frac{1}{|\mathcal{E}|}\right)\sum_{k=2}^{29}[\![k \mid d, \mu(k)=-1]\!]q^{d/2k-d/2} \\ & + [\![d\ge 30]\!]q^{-d/2}\sum_{1\le j\le d/30}\left(q^j + (\ell+t-1)\left(1-\frac{1}{|\mathcal{E}|}\right)q^{j/2}\right). \end{aligned} \tag{31}$$

Using (31), $\ell+t \le \lceil d/2\rceil - 1$, and

$$1-\frac{1}{|\mathcal{E}|}<1,\ \frac{1}{|\mathcal{E}|} \le \frac{\left|\{\langle 1\rangle^{1/k}\}\right|}{|\mathcal{E}|} \le 1,\ \sum_{1\le j\le d/30}q^j \le \frac{q}{q-1}\left(q^{d/30}-1\right),$$

we obtain (with the help of Maple) $L_q(d,\ell,t) \le \min\{2.8q^{-d/6}, 0.6\}$ when $q\ge 3$.

The case $q=2$ can be treated similarly by observing $|\mathcal{E}| = 2^{\ell+t-1}$ and $|\{\langle 1\rangle^{1/k}\}| = 1$ when k is not a powe of 2. ◀

The following bijection ϕ_d from $\mathcal{E}^\ell$ to itself is used to express $S_q(d;\varepsilon)$ in terms of $I_q(d;\varepsilon)$ [1, 3, 4].

Set $g_0 = 1$. For each positive integer d, let $\phi_d : (g_1, \ldots, g_\ell) \mapsto (f_1, \ldots, f_\ell)$ be defined by

$$f_k = \sum_{j \le k/2} \binom{d+2j-k}{j} g_{k-2j}, \quad 1 \le k \le \ell.$$

The following is [4, Theorem 1], rewritten in more compact notation.

▶ **Proposition 5.** *Suppose $d > 1$ and $\varepsilon \in \mathcal{E}^\ell$. Then*

$$S_q(d;\varepsilon) = \frac{1}{2} \sum_{\varepsilon_1 \in \{\varepsilon^{1/2}\}} S_q(d/2;\varepsilon_1) + I_q(d;\phi_d^{-1}(\varepsilon)) - \frac{1}{2} \sum_{n=0}^{q-2} \sum_{\delta \in \mathcal{E}^\ell} I_q\left(d;\varepsilon\delta^{-1},\gamma^n,\delta\right).$$

Proof of Theorem 2. We first use Theorem 3 and (28) to simplify the following sum:

$$\begin{aligned}
&\sum_{m=1}^{q-1} \sum_{\delta \in \mathcal{E}} I_q(d;\varepsilon\delta^{-1},\gamma^m,\delta) \\
&= \sum_{k \mid d} \frac{\mu(k)}{d} \sum_{m,\delta} \sum_{m_1,\delta_1,\varepsilon_1} F_q(d/k;\varepsilon_1\delta_1^{-1},\gamma^{m_1},\delta_1) [\![\gamma^{km_1} = \gamma^m, \delta_1^k = \delta, \varepsilon_1^k = \varepsilon]\!] \\
&= \sum_{k \mid d} \frac{\mu(k)}{d} \sum_{\varepsilon_1 \in \{\varepsilon^{1/k}\}} \sum_{m_1=1}^{q-1} \sum_{\delta_1 \in \mathcal{E}} F_q(d/k;\varepsilon_1\delta_1^{-1},\gamma^{m_1},\delta_1). \qquad (32)
\end{aligned}$$

Applying Theorem 5, (32), and noting

$$S_q(d/2;\delta) \le I_q(d/2;\delta) \le \frac{2}{d} F_q(d/2;\delta),$$

we obtain

$$\begin{aligned}
S_q(d;\varepsilon) \le{}& \frac{1}{d} \sum_{\varepsilon_1 \in \{\varepsilon^{1/2}\}} F_q(d/2;\varepsilon_1) + I_q(d;\phi_d^{-1}(\varepsilon)) \\
&- \frac{1}{2d} \sum_{m=1}^{q-1} \sum_{\delta \in \mathcal{E}} F_q(d;\varepsilon\delta^{-1},\gamma^m,\delta) \\
&+ \sum_{k \ge 2} \frac{[\![k \mid d, \mu(k) = -1]\!]}{2d} \sum_{\varepsilon_1 \in \{\varepsilon^{1/k}\}} \sum_{m=1}^{q-1} \sum_{\delta \in \mathcal{E}} F_q(d/k;\varepsilon_1\delta^{-1},\gamma^m,\delta).
\end{aligned}$$

It follows from (9), (25), and (27) that

$$\begin{aligned}
S_q(d;\varepsilon) &\le [\![2 \mid d]\!]\frac{\left|\{\varepsilon^{1/2}\}\right|}{q^\ell}\frac{q^{d/2}}{d} + [\![2 \mid d]\!](\ell-1)\left(1-\frac{1}{q^\ell}\right)\frac{q^{d/4}}{d} \\
&\quad + \frac{1}{dq^\ell}\left(q^d + Dq^{d/2}\right) - \frac{1}{2dq^\ell}\left(q^d-1\right) + \frac{D'}{2dq^\ell}q^{d/2} \\
&\quad + [\![2 \mid d]\!]\frac{\left|\{\varepsilon^{1/2}\}\right|}{2q^\ell}\frac{q^{d/2}}{d} + [\![2 \mid d]\!]\ell\left(1-\frac{1}{q^\ell}\right)\frac{q^{d/4}}{d} \\
&\quad + \frac{1}{2dq^\ell}\sum_{k\ge 3}[\![k \mid d, \mu(k)=-1]\!]\left|\{\varepsilon^{1/k}\}\right| q^{d/k} \\
&\quad + \frac{\ell}{d}\sum_{k\ge 3}[\![k \mid d, \mu(k)=-1]\!]\left(1-\frac{1}{q^\ell}\right)q^{d/2k} \\
&\le \frac{1}{d}q^{d-\ell} + \left(\frac{D'+2D+3[\![2 \mid d]\!]\left|\{\varepsilon^{1/2}\}\right|}{2q^\ell} + U_q(d;\ell)\right)\frac{q^{d/2}}{d},
\end{aligned}$$

where

$$\begin{aligned}
U_q(d;\ell) &= \frac{1}{2}q^{-\ell-d/2} + [\![2 \mid d]\!](2\ell-1)\left(1-\frac{1}{q^\ell}\right)q^{-d/4} \\
&\quad + \frac{1}{2q^\ell}\sum_{k\ge 3}[\![k \mid d, \mu(k)=-1]\!]\left|\{\varepsilon^{1/k}\}\right| q^{d/k-d/2} \\
&\quad + \ell\left(1-\frac{1}{q^\ell}\right)\sum_{k\ge 3}[\![k \mid d, \mu(k)=-1]\!]q^{d/2k-d/2}.
\end{aligned}$$

Simple calculations as in the proof of Theorem 1 give $U_q(d;\ell) \le \min\{6.6q^{-d/6}, 1.5\}$. This establishes (13). The bound (14) follows immediately from (13) and (7).

For the lower bound, we use Proposition 5 and (32) to obtain

$$\begin{aligned}
S_q(d;\varepsilon) &\ge I_q(d;\phi_d^{-1}(\varepsilon)) \\
&\quad - \sum_{k\mid d}\frac{[\![k \mid d]\!]}{2d}\sum_{\varepsilon_1\in\{\varepsilon^{1/k}\}}\sum_{m=1}^{q-1}\sum_{\delta\in\mathcal{E}^\ell}F_q(d/k;\varepsilon_1\delta^{-1},\gamma^m,\delta) \\
&\ge \frac{1}{d}q^{d-\ell} - \left(\frac{D+\left|\{\langle 1\rangle^{1/2}\}\right|[\![2 \mid d]\!]}{q^\ell} + L_q(d;\ell,0)\right)\frac{q^{d/2}}{d} \\
&\quad - \frac{1}{2d}\sum_{m=1}^{q-1}\sum_{\delta\in\mathcal{E}}F_q(d;\varepsilon\delta^{-1},\gamma^m,\delta) \\
&\quad - \frac{1}{2d}\sum_{k\ge 3}[\![k \mid d, \mu(k)=1]\!]\sum_{\varepsilon_1\in\{\varepsilon^{1/k}\}}\sum_{m=1}^{q-1}\sum_{\delta\in\mathcal{E}}F_q(d/k;\varepsilon_1\delta^{-1},\gamma^m,\delta).
\end{aligned}$$

Applying (24) and (28) again, we obtain

$$\begin{aligned} S_q(d;\varepsilon) \geq \frac{1}{d}q^{d-\ell} - \left(\frac{D + \left|\{\langle 1\rangle^{1/2}\}\right| [\![2 \mid d]\!]}{q^\ell} + L_q(d;\ell,0)\right)\frac{q^{d/2}}{d} \\ - \frac{1}{2dq^\ell}\left(q^d - 1 + D'q^{d/2}\right) \\ - \frac{1}{2d}\sum_{k\geq 6}[\![k \mid d, \mu(k) = 1]\!]\frac{\left|\{\langle 1\rangle^{1/k}\}\right|}{q^\ell}q^{d/k} \\ - \frac{\ell}{d}\left(1 - \frac{1}{q^\ell}\right)\sum_{k\geq 6}[\![k \mid d, \mu(k) = 1]\!]q^{d/2k}. \end{aligned}$$

Define

$$\begin{aligned} L'_q(d;\ell) = L_q(d;\ell,0) + \frac{1}{2}\sum_{k\geq 6}[\![k \mid d, \mu(k) = 1]\!]\frac{\left|\{\langle 1\rangle^{1/k}\}\right|}{q^\ell}q^{d/k-d/2} \\ + \ell\left(1 - \frac{1}{q^\ell}\right)\sum_{k\geq 6}[\![k \mid d, \mu(k) = 1]\!]q^{d/2k-d/2}. \end{aligned}$$

We then have

$$S_q(d;\varepsilon) \geq \frac{1}{2d}q^{d-\ell} - \left(\frac{D'}{2q^\ell} + \frac{D + \left|\{\langle 1\rangle^{1/2}\}\right| [\![2 \mid d]\!]}{q^\ell} + L'_q(d;\ell)\right)\frac{q^{d/2}}{d}. \tag{33}$$

Similar calculations give

$$L'_q(d;\ell) \leq \min\{7q^{-d/6}, 2\}.$$

Now (15) follows from (33). The bound (16) follows immediately from (15), (7), (8), and

$$\left|\{\langle 1\rangle^{1/2}\}\right| \leq q^\ell.$$

Hence $S_q(d;\varepsilon) > 0$ when

$$q^{d/2} > 2(2\ell + 2)q^\ell.$$

Using $2\ell \leq d - 1$ and taking $\log_q$ on both sides, we complete the proof. ◀

4 Examples

In this section, we use some examples to demonstrate that $\frac{D}{|\mathcal{E}^\ell|-1}$ is smaller than $\ell - 1$. For $P(z;\varepsilon)$ defined in (5), let

$$d_j = |\{\varepsilon \in \mathcal{E}^\ell \setminus \{\langle 1\rangle\} : \deg(P(z;\varepsilon)) = j\}|, \quad \vec{d} = (d_1, d_2, \ldots d_{\ell-1}).$$

We note

$$D = \sum_{j=1}^{\ell-1} j d_j.$$

▶ **Example 6.** Consider $q = 2$ and $\ell = 4$. From [15, Example 4], we have

$$\vec{d} = (2, 4, 8),$$
$$D = 2 + 2 \times 4 + 3 \times 8 = 34,$$
$$\frac{D}{|\mathcal{E}^4| - 1} = \frac{34}{2^4 - 1} < 2.3.$$

▶ **Example 7.** Consider $q = 2$ and $\ell = 5$. From [15, Example 6], we have

$$\vec{d} = (2, 4, 8, 16),$$
$$D = 2 + 2 \times 4 + 3 \times 8 + 4 \times 16 = 98,$$
$$\frac{D}{|\mathcal{E}^5| - 1} = \frac{98}{2^5 - 1} < 3.2.$$

▶ **Example 8.** Consider $q = 3$ and $\ell = 3$. From [15, Example 5], we have

$$\vec{d} = (6, 18),$$
$$D = 6 + 2 \times 18 = 42,$$
$$\frac{D}{|\mathcal{E}^3| - 1} = \frac{42}{3^3 - 1} < 1.62.$$

We use the following result from [15, Lemma 1] to produce a few more examples.

▶ **Lemma 9.** *Let $q = p$ be a prime number. The generators of $\mathcal{E}^\ell$ are*

$$\left\{\langle x^j + 1\rangle : \gcd(p, j) = 1, 1 \le j \le \ell\right\},$$

and the order of $\langle x^j + 1\rangle$ is equal to p^{s_j}, where s_j is the smallest positive integer such that $jp^{s_j} > \ell$.

The degree sequence $\vec{d}$ in the following examples are calculated using (3)–(6) with the help of the computer algebra system *Maple*.

▶ **Example 10.** Consider $q = 2$ and $\ell = 6$. By Lemma 9, the group $\mathcal{E}^6$ is generated by $\langle x + 1\rangle$, $\langle x^3 + 1\rangle$, $\langle x^5 + 1\rangle$, of orders 8,4,2, respectively. Hence

$$\vec{d} = (2, 4, 8, 16, 32),$$
$$D = 2 + 2 \times 4 + 3 \times 8 + 4 \times 16 + 5 \times 32 = 258,$$
$$\frac{D}{|\mathcal{E}^6| - 1} = \frac{258}{2^6 - 1} < 4.1.$$

▶ **Example 11.** Consider $q = 2$ and $\ell = 7$. By Lemma 9, the group $\mathcal{E}^7$ is generated by $\langle x + 1\rangle$, $\langle x^3 + 1\rangle$, $\langle x^5 + 1\rangle$, $\langle x^7 + 1\rangle$, of orders 8,4,2,2, respectively. Hence

$$\vec{d} = (2, 4, 8, 16, 32, 64),$$
$$D = 2 + 2 \times 4 + 3 \times 8 + 4 \times 16 + 5 \times 32 + 6 \times 64 = 642,$$
$$\frac{D}{|\mathcal{E}^7| - 1} = \frac{642}{2^7 - 1} < 5.1.$$

▶ **Example 12.** Consider $q = 3$ and $\ell = 4$. By Lemma 9, the group $\mathcal{E}^4$ is generated by $\langle x + 1\rangle$, $\langle x^2 + 1\rangle$, $\langle x^4 + 1\rangle$, of orders 9,3,3, respectively. Hence

$$\vec{d} = (6, 18, 54),$$
$$D = 6 + 2 \times 18 + 3 \times 54 = 204,$$
$$\frac{D}{|\mathcal{E}^4| - 1} = \frac{204}{3^4 - 1} < 2.6.$$

▶ **Example 13.** Consider $q = 3$ and $\ell = 5$. By Lemma 9, the group $\mathcal{E}^5$ is generated by $\langle x+1\rangle$, $\langle x^2+1\rangle$, $\langle x^4+1\rangle$, $\langle x^5+1\rangle$, of orders 9,3,3,3, respectively. Hence

$$\begin{aligned}\vec{d} &= (6, 18, 54, 162),\\ D &= 6 + 2\times 18 + 3\times 54 + 4\times 162 = 852,\\ \frac{D}{|\mathcal{E}^5| - 1} &= \frac{852}{3^5 - 1} < 3.6.\end{aligned}$$

▶ **Example 14.** Consider $q = 3$ and $\ell = 6$. By Lemma 9, the group $\mathcal{E}^6$ is generated by $\langle x+1\rangle$, $\langle x^2+1\rangle$, $\langle x^4+1\rangle$, $\langle x^5+1\rangle$, of orders 9,9,3,3, respectively. Hence

$$\begin{aligned}\vec{d} &= (6, 18, 54, 162, 486),\\ D &= 6 + 2\times 18 + 3\times 54 + 4\times 162 + 5\times 486 = 3282,\\ \frac{D}{|\mathcal{E}^6| - 1} &= \frac{3282}{3^6 - 1} < 4.51.\end{aligned}$$

▶ **Observation.** *The above examples suggest that the degree sequence $\vec{d}$ for the group $\mathcal{E}^\ell$ satisfies*

$$d_j = (q-1)q^j.$$

5 Conclusion

We derived new error bounds for the number of irreducible monic polynomials with prescribed leading and ending coefficients. These bounds improve the bounds in [2, 9]. The new bounds are then used to obtain bounds for the number $S_q(d;\varepsilon)$ of self-reciprocal irreducible monic polynomials of degree $2d$ with ℓ prescribed leading coefficients. The new lower bound for $S_q(d;\varepsilon)$ significantly improves the one obtained in [4] and it implies $S_q(d;\varepsilon) > 0$ when

$$\ell \le \min\left\{\left\lceil\frac{d}{2}\right\rceil - 1, \frac{d}{2} - \log_q(2d+2)\right\}.$$

Some examples are given to demonstrate the improvement of our bounds in Theorem 1 over those in [2, 9]. Our examples show a pattern about the degree sequence $\vec{d}$, which can be used to calculate D exactly.

References

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

2 S. D. Cohen. On irreducible polynomials of certain types in finite fields. *Proc. Camb. Phil. Soc.*, 66:335–344, 1969.

3 S. D. Cohen. Explicit theorems on generator polynomials. *Finite Fields Appl.*, 11:337–357, 2005.

4 Z.C. Gao. Counting self-reciprocal irreducible monic polynomials with prescribed coefficients over a finite field. `arXiv:2109.09006`.

5 T. Garefalakis and G. Kapetanakis. On the hansen-mullen conjecture for self-reciprocal irreducible polynomials. *Finite Fields Appl.*, 69:832–841, 2012.

6 J Ha. Irreducible polynomials with several prescribed coefficients. *Finite Fields Appl.*, 40:10–25, 2016.

7 K.H. Ham and G.L. Mullen. Distribution of irreducible polynomials of small degrees over finite fields. *Math. Comp.*, 67(221):337–341, 1998.

8 D. R. Hayes. The distribution of irreducibles in GF$[q, x]$. *Trans. Amer. Math. Soc.*, 117:101–127, 1965.

9 C.N. Hsu. The distribution of irreducible polynomials in $\mathbb{F}_q[t]$. *J. Number Theory*, 61(1):85–96, 1996.

10 D. Panario. Open problems for polynomials over finite fields and applications. In *Chapter 5 of Proceedings on the Open Problems in Mathematics and Computer Science Conference*, pages 111–126. Springer, 2015.

11 D. Panario and G. Tzanakis. A generalization of the hansen-mullen conjecture on irreducible polynomials over finite fields. *Finite Fields Appl.*, 18:303–315, 2012.

12 P. Pollack. Irreducible polynomials with several prescribed coefficients. *Finite Fields Appl.*, 22:70–78, 2013.

13 D. Bossen S. Hong. On some properties of self-reciprocal polynomials. *IEEE Trans. Inform. Theory*, 21(4):462–464, 1975.

14 D. Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 219:1195–1212, 1997.

15 S. Kuttner Z. Gao and Q. Wang. Counting irreducible polynomials with prescribed coefficients over a finite field. *Finite Fields Appl.*, 80(102023), 2022. doi:10.1016/j.ffa.2022.102023.