# Self-reciprocal irreducible polynomials with prescribed coefficients

Theodoulos Garefalakis

*Department of Mathematics, University of Crete, 71409 Heraklion, Greece*

---

**Abstract**

We prove estimates for the number of self-reciprocal monic irreducible polynomials over a finite field of odd characteristic, that have the $t$ lower degree coefficients fixed to given values. Our estimates imply that one may specify up to $m/2 - \log_q(2m) - 1$ values in the field and a self-reciprocal monic irreducible polynomial of degree $2m$ exists with its low degree coefficients fixed to those values.

*Keywords:* Self-reciprocal polynomials, irreducible polynomials, finite fields

---

## 1. Introduction

Let $q$ be a prime power and let $\mathbb{F}_q$ be the finite field with $q$ elements. For any $n \in \mathbb{N}$, we denote by $\mathbb{I}_n$ the set of monic irreducible polynomials in $\mathbb{F}_q[X]$. It is well known that the cardinality of $\mathbb{I}_n$, denoted by $\pi_q(n)$, is roughly $q^n/n$. It is of interest, both from a theoretical and a practical point of view, and has been the topic of an active line of research, to compute the cardinalities of various subsets of $\mathbb{I}_n$. Perhaps the earliest result along these lines is Dirichlet's theorem for primes in arithmetic progression for $\mathbb{F}_q[X]$, see [22]. Dirichlet's theorem, applied with modulus $X^t$, implies that the number of monic irreducibles of degree $n$ with the coefficients of the $t$ lowest degree terms fixed to given values (the constant term being non zero) is approximated by $\pi_q(n)/\Phi(X^t)$, where $\Phi(\cdot)$ is Euler's totient function defined in $\mathbb{F}_q[X]$ as $\Phi(F) = \#(\mathbb{F}_q[X]/F\mathbb{F}_q[X])^*$. It should be noted that results as the above require Riemann's Hypothesis for function fields. As a consequence, $t$ has to be taken less than $n/2$.

Dirichlet's theorem has been the starting point for an area of research that has been very active during the past thirty years. For instance, irreducible polynomials with prescribed coefficients [1, 13, 14, 16, 17, 23], and primitive and/or normal

---

*Email address:* `theo@math.uoc.gr` (Theodoulos Garefalakis)

polynomials with prescribed coefficients [5, 6, 7, 8, 9, 10, 11, 12] have been the focus of substantial research.

Irreducible polynomials with additional properties have attracted considerable attention. One class of irreducibles of particular interest has been that of self-reciprocal, monic irreducibles, that is, monic irreducibles $P$ that satisfy $P(X) = X^{\deg(P)}P(1/X)$. The reader is refered to [15, 18] for their applications in coding theory, to [21] for their connection to combinatorics and to [4, 19] for their use in the construction of certain infinite extensions of $\mathbb{F}_q$. Due to their applications, self-reciprocal irreducible polynomials have been studied extensively. In particular, it has been shown that all self-reciprocal monic irreducible polynomials have even degree and their number has been computed in [2, 3, 20].

The subject of the present work is to study the distribution of self-reciprocal monic irreducible polynomials. More precisely, given $t$ values in $\mathbb{F}_q$ we compute the number of self-reciprocal monic irreducibles of degree $2m$ in $\mathbb{F}_q[X]$ with the $t$ low degree coefficients fixed to the given values. We note that the constant term is necessarily fixed to 1. Our approach is based on the work of Carlitz [2].

## 2. Auxiliary lemmata

Let $p$ be an odd prime, $e \geq 1$ and $q = p^e$. We let $\mathbb{A} = \mathbb{F}_q[X]$ be the polynomial ring over $\mathbb{F}_q$. For $m \in \mathbb{N}$, we denote by $\mathbb{I}_m$ the set of monic irreducible polynomials in $\mathbb{A}$ of degree $m$. For a polynomial $F \in \mathbb{A}$, we denote the coefficient of $X^i$ by $F_i$.

**Lemma 1.** *Let $P \in \mathbb{I}_m$, $m \geq 2$, and let $\widetilde{P} = \frac{1}{P_0}X^m P\left(\frac{4}{X}\right)$. Then $\widetilde{P} \in \mathbb{I}_m$ and $\widetilde{\widetilde{P}} = P$.*

Proof. Let $P(X) = \sum_{i=0}^{m} P_i X^i$, where $P_m = 1$ since $P$ is monic. Then

$$\widetilde{P} = \sum_{i=0}^{m} \frac{4^i P_i}{P_0} X^{m-i} = \sum_{i=0}^{m} \frac{4^{m-i} P_{m-i}}{P_0} X^i. \tag{1}$$

Clearly, $\widetilde{P}$ is monic. If $\beta$ is a root of $\widetilde{P}$, then $\beta = 4/\alpha$, where $\alpha$ is a root of $P$. Therefore, $\mathbb{F}_q(\alpha) = \mathbb{F}_q(\beta)$ and $P$ is irreducible if and only if $\widetilde{P}$ is irreducible. Finally, $\widetilde{\widetilde{P}}$ is monic irreducible of degree $m$ and if $\gamma$ is one of its roots, then $\gamma = 4/\beta = \alpha$. It follows that $\widetilde{\widetilde{P}} = P$. □

The polynomial $\widetilde{P}$ has the following important property: it can be easily determined whether or not it is a square modulo $X^2 - 4$ based on whether $P$ is a square modulo $X^2 - 4$. We denote by $(\cdot|X^2 - 4)$ the Legendre symbol modulo $X^2 - 4$ for the ring $\mathbb{A}$.

**Lemma 2.** *Let $P \in \mathbb{I}_m$, $m \geq 2$. Then the following hold.*

1. *If $q \equiv 1 \pmod 4$ or $m$ is even then $(P|X^2-4) = (\widetilde{P}|X^2-4)$.*
2. *If $q \equiv 3 \pmod 4$ and $m$ is odd then $(P|X^2-4) = -(\widetilde{P}|X^2-4)$*

Proof. Let $\alpha$ be a root of $P$ and $\beta = 4/\alpha$ be a root of $\widetilde{P}$. The quadratic reciprocity law for $\mathbb{A}$ [22, Ch. 3] implies that $(P|X^2-4) = (X^2-4|P)$. Further, $(X^2-4|P) = 1$ if and only if $\alpha^2 - 4 = \delta^2$ for some $\delta \in \mathbb{F}_q$. The same reasoning, applied to $\widetilde{P}$ shows that $(\widetilde{P}|X^2-4) = (X^2-4|\widetilde{P})$. Furthermore, $(X^2-4|\widetilde{P}) = 1$ if and only if $\beta^2 - 4$ is a square in $\mathbb{F}_q$. We compute

$$\beta^2 - 4 = \frac{4^2}{\alpha^2} - 4 = -\frac{4}{\alpha^2}(\alpha^2 - 4) = -\left(\frac{2\delta}{\alpha}\right)^2.$$

To finish the proof, it suffices to note that $-1$ is a square in $\mathbb{F}_q$ if and only if either $q \equiv 1 \pmod 4$ or $m$ is even. □

For an abelian group $H$, we denote by $\widehat{H}$ the dual of $H$, that is, the group of characters of $H$. In particular, given a polynomial $F \in \mathbb{A}$, and taking the group $H = (\mathbb{A}/F\mathbb{A})^*$, we note that the dual of $H$ is essentially the group of Dirichlet characters modulo $F$. We will make use of the following simple lemma in Section 4.

**Lemma 3.** *Let $F, G \in \mathbb{A}$ be co-prime polynomials. The map*

$$\begin{array}{rcl} \theta : \widehat{\left(\dfrac{\mathbb{A}}{F\mathbb{A}}\right)^*} \times \widehat{\left(\dfrac{\mathbb{A}}{G\mathbb{A}}\right)^*} & \longrightarrow & \widehat{\left(\dfrac{\mathbb{A}}{FG\mathbb{A}}\right)^*} \\ (\chi, \psi) & \mapsto & \chi\psi, \end{array}$$

*where $\chi\psi(f \bmod FG) = \chi(f \bmod F) \cdot \psi(f \bmod G)$, is a group isomorphism.*

Proof. The statement follows easily from the isomorphism of the Chinese Remainder Theorem $(\mathbb{A}/FG\mathbb{A})^* \to (\mathbb{A}/F\mathbb{A})^* \times (\mathbb{A}/G\mathbb{A})^*$. □

## 3. Outline of method

It is well known, see [2], that every monic self-reciprocal irreducible polynomial has even degree and is of the form $Q(X) = X^m P(X + X^{-1})$, where $P$ is a monic irreducible of degree $m$ such that $X^2 - 4$ is a non-square modulo $P$. The last condition can be written as $(X^2 - 4|P) = -1$, using Legendre's symbol. Conversely, given a monic irreducible polynomial $P$ of degree $m$, that satisfies $(X^2 - 4|P) = -1$, the polynomial $Q(X) = X^m P(X+X^{-1})$ is a monic, irreducible, self-reciprocal polynomial of degree $2m$. Accordingly,

$$\#\{Q \in \mathbb{I}_{2m} \;:\; Q \text{ is self-reciprocal }\} = \#\left\{P \in \mathbb{I}_m \;:\; (P|X^2-4) = -1\right\},$$

where we used the fact that $(X^2-4|P) = (P|X^2-4)$. Our goal is to estimate

$$\#\{Q \in \mathbb{I}_{2m} \;:\; Q \text{ is self-reciprocal \ and } Q_i = c_i,\ i = 1,\dots,t\},$$

where $Q = \sum_{i=0}^{2m} Q_i X^i$ and $c_1,\dots,c_t \in \mathbb{F}_q$ are fixed values.

It is clear that the coefficients of $Q$ depend linearly on the coefficients of $P$. The next lemma makes this dependence explicit.

**Lemma 4.** *Let $P = \sum_{i=0}^m P_i X^i$ and $Q = \sum_{i=0}^{2m} Q_i X^i$ be two polynomials in $\mathbb{A}$ satisfying $Q = X^m P(X+X^{-1})$ and $t \in \mathbb{N}$, $1 \le t \le m-1$. Then there exists a lower triangular matrix $U \in \mathrm{SL}_t(\mathbb{F}_q)$ with all the elements in the diagonal equal to* 1*, such that*

$$(Q_0, Q_1, \dots, Q_t)^T = U \cdot (P_m, P_{m-1}, \dots, P_{m-t})^T.$$

Proof. Let $P = \sum_{i=0}^m P_i X^i = \sum_{i=0}^m a_i X^{m-i}$. Then

$$\begin{aligned} Q &= X^m \sum_{i=0}^{m} a_i (X+X^{-1})^{m-i} = \sum_{i=0}^{m} a_i X^i (X^2+1)^{m-i} = \sum_{i=0}^{m} a_i X^i \sum_{j=0}^{m-i} \binom{m-i}{j} X^{2j} \\ &= \sum_{\substack{0\le i\le m \\ 0 \le j \le m-i}} \binom{m-i}{j} a_i X^{i+2j} = \sum_{k=0}^{2m} \left( \sum_{\substack{0\le i\le m \\ 0 \le j \le m-i \\ k=i+2j}} \binom{m-i}{j} a_i \right) X^k. \end{aligned}$$

It follows that

$$Q_k = \sum_{\substack{0\le i\le m \\ 0 \le j \le m-i \\ k=i+2j}} \binom{m-i}{j} a_i, \quad 0 \le k \le 2m. \tag{2}$$

It is easy to see that $Q_k$ is a linear combination of $a_0,\dots,a_k$ and the coefficient of $a_k$ is $\binom{m-k}{0} = 1$. The statement of the lemma follows once we substitute $P_{m-i}$ for $a_i$ and consider the first $t+1$ equations. □

**Lemma 5.** *Let $m \ge 2$, $t \in \mathbb{N}$, $1 \le t \le m-1$ and $c_1,\dots,c_t \in \mathbb{F}_q$. Then*

$$\begin{aligned} &\#\{Q \in \mathbb{I}_{2m} \;:\; Q \text{ is self-reciprocal and } Q_i = c_i, i = 1,\dots,t\} \\ = &\sum_{c \in \mathbb{F}_q^*} \#\left\{ P \in \mathbb{I}_m \;:\; (P|X^2-4) = \varepsilon, P_0 = \frac{4^m}{c}, P_i = \frac{c_i' 4^{m-i}}{c}, i = 1,\dots,t \right\}, \end{aligned}$$

*where* $(1, c'_1, \ldots, c'_t)^T = U^{-1}(1, c_1, \ldots, c_t)^T$, *U is the matrix of Lemma 4 and*

$$\varepsilon = \begin{cases} -1, & \text{if} \quad q \equiv 1 \pmod 4 \text{ or } m \equiv 0 \pmod 2 \\ 1, & \text{if} \quad q \equiv 3 \pmod 4 \text{ and } m \equiv 1 \pmod 2 \end{cases}$$

Proof. From Lemma 4 and the discussion preceeding it, it follows that

$$\begin{aligned} & \#\{Q \in \mathbb{I}_{2m} \ : \ Q \text{ is self-reciprocal and } Q_i = c_i, i = 1, \ldots, t\} \\ = \ & \#\left\{P \in \mathbb{I}_m \ : \ (P|X^2-4) = -1, P_{m-i} = c'_i, i = 1, \ldots, t\right\}. \end{aligned} \tag{3}$$

We partition the set on the right-hand side as

$$\begin{aligned} & \left\{P \in \mathbb{I}_m \ : \ (P|X^2-4) = -1, P_{m-i} = c'_i, i = 1, \ldots, t\right\} \\ = & \bigcup_{c \in \mathbb{F}_q^*} \left\{P \in \mathbb{I}_m \ : \ (P|X^2-4) = -1, P_0 = c, P_{m-i} = c'_i, i = 1, \ldots, t\right\}. \end{aligned} \tag{4}$$

Let now

$$\mathcal{A}_c = \left\{P \in \mathbb{I}_m \ : \ (P|X^2-4) = -1, P_0 = c, P_{m-i} = c'_i, i = 1, \ldots, t\right\}$$

and

$$\mathcal{B}_c = \left\{P \in \mathbb{I}_m \ : \ (P|X^2-4) = \varepsilon, P_0 = \frac{4^m}{c}, P_i = \frac{c'_i 4^{m-i}}{c}, i = 1, \ldots, t\right\},$$

where $\varepsilon$ is defined in the statement of the Lemma. Clearly the sets $\mathcal{A}_c, c \in \mathbb{F}_q^*$ are pairwise disjoint. The same is true for the sets $\mathcal{B}_c, c \in \mathbb{F}_q^*$. We claim that for every $c \in \mathbb{F}_q^*$, the map

$$\begin{aligned} \vartheta : \mathcal{A}_c & \longrightarrow \mathcal{B}_c \\ P & \mapsto \widetilde{P} \end{aligned}$$

is a bijection. Indeed, from Lemma 1 follows that $\vartheta(P) = \widetilde{P} \in \mathbb{I}_m$ and from Lemma 2 follows that $(\widetilde{P}|X^2-4) = \varepsilon$. Finally, Eq.(1) shows that the coefficients of $\widetilde{P}$ are as required. This shows that the map is well defined. To prove it is injective, note that $\vartheta(P_1) = \vartheta(P_2)$ implies $\widetilde{P_1} = \widetilde{P_2}$. Applying $\vartheta$ again and using Lemma 1 we obtain $P_1 = P_2$. Surjectivity follows from the observation that for $P \in \mathcal{B}_c$, $\widetilde{P} \in \mathcal{A}_c$ and $\vartheta(\widetilde{P}) = P$, that is, $\vartheta$ is its own inverse.

From Eq. (3), Eq. (4) and the fact that $\vartheta$ is bijective, we obtain

$$\#\{Q \in \mathbb{I}_{2m} \ : \ Q \text{ is self-reciprocal and } Q_i = c_i, i = 1, \ldots, t\} = \sum_{c \in \mathbb{F}_q^*} \#\mathcal{B}_c,$$

and the proof is complete. □

Lemma 5 reduces our problem to that of estimating the cardinality of a set of the form

$$\left\{P \in \mathbb{I}_m \ : \ (P|X^2 - 4) = \varepsilon, P_i = c_i, i = 0, \dots, t\right\},$$

for any $c_0, \dots, c_t \in \mathbb{F}_q$, $c_0 \neq 0$. Note that for fixed values $c_i$, $i = 0, \dots, t$, we have

$$\begin{aligned} & \left\{P \in \mathbb{I}_m \ : \ (P|X^2 - 4) = \varepsilon, P_i = c_i, i = 0, \dots, t\right\} \\ = \ & \left\{P \in \mathbb{I}_m \ : \ (P|X^2 - 4) = \varepsilon, \ P \equiv C \pmod{X^{t+1}}\right\}, \end{aligned}$$

where $C = c_t X^t + \cdots + c_1 X + c_0 \in \mathbb{A}$. We denote $\pi_q(m) = \#\mathbb{I}_m$,

$$\pi_q(m, C, \varepsilon) = \#\left\{P \in \mathbb{I}_m \ : \ (P|X^2 - 4) = \varepsilon, \ P \equiv C \pmod{X^{t+1}}\right\},$$

and

$$\pi_q(m, \varepsilon) = \#\left\{P \in \mathbb{I}_m \ : \ (P|X^2 - 4) = \varepsilon\right\}.$$

## 4. Main result

Let $M \in \mathbb{A}$ be a polynomial of degree $k$ and suppose $\rho$ is a non-trivial Dirichlet character modulo $M$. The Dirichlet $L$-function associated with $\rho$ is defined to be

$$\mathcal{L}(s, \rho) = \sum_F \frac{\rho(F)}{|F|^s}, \quad \Re(s) > 1,$$

where $|F| = q^{\deg(F)}$ and the sum is over monic polynomials in $\mathbb{A}$. Making the substitution $u = q^{-s}$, we have

$$\mathcal{L}(s, \rho) = L(u, \rho) = \sum_{n=0}^{\infty} \left( \sum_{\deg(F)=n} \rho(F) \right) u^n.$$

It is not hard to show that $L(u, \rho)$ is a polynomial in $u$ of degree at most $k - 1$. Further, $L(u, \rho)$ has an Euler product,

$$L(u, \rho) = \prod_{d=1}^{\infty} \prod_{\deg(P)=d} \left(1 - \rho(P) u^d\right)^{-1}.$$

Taking the logarithmic derivative of $L(u, \rho)$ and multiplying by $u$, we obtain a series $\sum_{n=1}^{\infty} c_n(\rho) u^n$, with

$$c_n(\rho) = \sum_{d|n} \frac{n}{d} \sum_{\deg(P)=n/d} \rho(P)^d. \tag{5}$$

Weil's theorem of the Riemann hypothesis for function fields implies that

$$|c_n(\rho)| \leq (k-1)q^{\frac{n}{2}}. \tag{6}$$

For a detailed account of the above well known facts, see [22, Ch. 4].

Consider now the quadratic Dirichlet character modulo $X^2-4$, $\psi(F) = (F|X^2-4)$, for $F \in \mathbb{A}$. In [2], Carlitz computed the number of self-reciprocal monic irreducibles in $\mathbb{A}$ using the Dirichlet $L$-function associated with $\psi$.

Let $\chi$ be a Dirichlet character modulo $X^{t+1}$. Since $(X^{t+1}, X^2-4) = 1$, Lemma 3 applies, and there is a non-trivial Dirichlet character modulo $X^{t+1}(X^2-4)$, which we denote by $\chi\psi$ such that $\chi\psi(F) = \chi(F)\psi(F)$. In our case, it is natural to consider the $L$-function associated with the dirichlet character $\chi\psi$. We use the notation $L(u, \chi, \psi)$ for $L(u, \chi\psi)$ and $c_n(\chi, \psi)$ for $c_n(\chi\psi)$.

Applying Eq.(5) and Eq.(6) with $\rho = \chi\psi$, we obtain

$$c_n(\chi, \psi) = \sum_{d|n} \frac{n}{d} \sum_{\deg(P)=n/d} \chi\psi(P)^d \tag{7}$$

and

$$|c_n(\chi, \psi)| \leq (t+2)q^{\frac{n}{2}}. \tag{8}$$

Eq.(6), applied with $\rho = \chi$, for a non-trivial character $\chi$, yields

$$|c_n(\chi)| \leq tq^{\frac{n}{2}}, \quad \text{for } \chi \neq \chi_o. \tag{9}$$

**Proposition 1.** *Let $\chi$ be a non-trivial Dirichlet character modulo $X^{t+1}$. Then the following bounds hold:*

1. *For every $n \in \mathbb{N}$, $n \geq 2$,*

$$\left| \sum_{\substack{\deg(P)=n \\ \psi(P)=-1}} \chi(P) \right| \leq \tfrac{t+5}{n} q^{\frac{n}{2}}.$$

2. *For every $n \in \mathbb{N}$, $n \geq 2$, $n$ odd,*

$$\left| \sum_{\substack{\deg(P)=n \\ \psi(P)=1}} \chi(P) \right| \leq \tfrac{t+5}{n} q^{\frac{n}{2}}.$$

Proof. From Eq. (7), taking into account that $\psi$ is a quadratic character, we have

$$\begin{aligned}
c_n(\chi,\psi) &= \sum_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d\psi(P) + \sum_{\substack{d|n\\ d \text{ even}}} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d \\
&= \sum_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=1}} \chi(P)^d - \sum_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} \chi(P)^d + \\
&\quad \sum_{\substack{d|n\\ d \text{ even}}} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d \\
&= \sum_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d - 2\sum_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} \chi(P)^d + \\
&\quad \sum_{\substack{d|n\\ d \text{ even}}} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d \\
&= \sum_{d|n} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d - 2\sum_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} \chi(P)^d.
\end{aligned}$$

By definition

$$c_n(\chi) = \sum_{d|n} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d$$

and we denote

$$e_n(\chi,\psi,-1) = \sum_{\substack{d|n\\ d \text{ odd}}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} \chi(P)^d,$$

so that

$$c_n(\chi,\psi) = c_n(\chi) - 2e_n(\chi,\psi,-1).$$

From Eq.(8) and Eq.(9) it follows that

$$|e_n(\chi,\psi,-1)| \leq (t+1)q^{\frac{n}{2}}, \quad \text{for } \chi \neq \chi_o. \tag{10}$$

Furthermore,

$$e_n(\chi,\psi,-1) = n \sum_{\substack{\deg(P)=n\\ \psi(P)=-1}} \chi(P) + \sum_{\substack{d|n\\ d \text{ odd}\\ d>1}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} \chi(P)^d.$$

We bound the second summand as follows

$$\left|\sum_{\substack{d|n\\ d\text{ odd}\\ d>1}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} \chi(P)^d\right| \le \sum_{\substack{d|n\\ d\text{ odd}\\ d>1}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} 1 \le \sum_{j=1}^{\lfloor n/3\rfloor} j \sum_{\deg(P)=j} 1,$$

and using the fact that $\sum_{\deg(P)=j} = \pi_q(j) \le q^j/j + 3q^{\frac{j}{2}}/2$ for $q \ge 3$, we have

$$\begin{aligned}
\sum_{j=1}^{\lfloor n/3\rfloor} j \sum_{\deg(P)=j} 1 &\le \sum_{j=1}^{\lfloor n/3\rfloor} \left(q^j + \frac{3j}{2} q^{\frac{j}{2}}\right) \\
&\le \frac{q}{q-1}(q^{\frac{n}{3}} - 1) + \frac{3}{2}\frac{n}{3} \sum_{j=1}^{\lfloor n/3\rfloor} q^{\frac{j}{2}} \\
&\le \frac{3}{2} q^{\frac{n}{3}} + \frac{3n}{2} q^{\frac{n}{6}},
\end{aligned}$$

where we used the fact that $q/(q-1) \le 3/2$ and $\sqrt{q}/(\sqrt{q}-1) \le 3$ for $q \ge 3$. Since $3q^{\frac{n}{3}}/2 \le 2q^{\frac{n}{2}}$ and $3nq^{\frac{n}{6}}/2 \le 2q^{\frac{n}{2}}$ for every $q \ge 3$ and $n \ge 2$, we obtain

$$\left|\sum_{\substack{d|n\\ d\text{ odd}\\ d>1}} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} \chi(P)^d\right| \le 4q^{\frac{n}{2}}.$$

From this bound and Eq. (10) follows that

$$\left|\sum_{\substack{\deg(P)=n\\ \psi(P)=-1}} \chi(P)\right| \le \tfrac{t+5}{n} q^{\frac{n}{2}}. \tag{11}$$

For $n$ odd, we have

$$\begin{aligned}
c_n(\chi,\psi) &= \sum_{d|n} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d \psi(P) \\
&= \sum_{d|n} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=1}} \chi(P)^d - \sum_{d|n} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=-1}} \chi(P)^d \\
&= 2\sum_{d|n} \frac{n}{d} \sum_{\substack{\deg(P)=n/d\\ \psi(P)=1}} \chi(P)^d - \sum_{d|n} \frac{n}{d} \sum_{\deg(P)=n/d} \chi(P)^d.
\end{aligned}$$

Denoting

$$e_n(\chi, \psi, 1) = \sum_{d|n} \frac{n}{d} \sum_{\substack{\deg(P)=n/d \\ \psi(P)=1}} \chi(P)^d,$$

we have

$$c_n(\chi, \psi) = 2e_n(\chi, \psi, 1) - c_n(\chi).$$

It follows that

$$|e_n(\chi, \psi, 1)| \leq (t+1)q^{\frac{n}{2}}$$

and

$$\left| \sum_{\substack{\deg(P)=n \\ \psi(P)=1}} \chi(P) \right| \leq \tfrac{t+5}{n} q^{\frac{n}{2}}. \quad \square$$

Proposition 1 can be used to obtain estimates for $\pi_q(n, C, -1)$.

**Theorem 1.** *Let $q$ be a power of an odd prime and $C \in \mathbb{A}$, co-prime to $X$ of degree at most $t$. Then the following bounds hold:*

1. *For every $n \in \mathbb{N}$, $n \geq 2$,*

$$\left| \pi_q(n, C, -1) - \frac{1}{\Phi(X^{t+1})} \pi_q(n, -1) \right| \leq \tfrac{t+5}{n} q^{\frac{n}{2}}.$$

2. *For every $n \in \mathbb{N}$, $n \geq 2$, $n$ odd,*

$$\left| \pi_q(n, C, 1) - \frac{1}{\Phi(X^{t+1})} \pi_q(n, 1) \right| \leq \tfrac{t+5}{n} q^{\frac{n}{2}}.$$

Proof. For $\varepsilon \in \{-1, 1\}$, we have

$$\begin{aligned} \pi_q(n, C, \varepsilon) &= \sum_{\substack{\deg(P)=n \\ \psi(P)=\varepsilon}} \frac{1}{\Phi(X^{t+1})} \sum_{\chi} \chi(P)\bar{\chi}(C) \\ &= \frac{1}{\Phi(X^{t+1})} \sum_{\chi} \bar{\chi}(C) \sum_{\substack{\deg(P)=n \\ \psi(P)=\varepsilon}} \chi(P), \end{aligned}$$

where $\Phi$ is Euler's totient function on the ring $\mathbb{A}$. Separating the term corresponding to $\chi_o$ we have

$$\pi_q(n, C, \varepsilon) = \frac{1}{\Phi(X^{t+1})} \pi_q(n, \varepsilon) + \frac{1}{\Phi(X^{t+1})} \sum_{\chi \neq \chi_o} \bar{\chi}(C) \sum_{\substack{\deg(P)=n \\ \psi(P)=\varepsilon}} \chi(P),$$

and we obtain

$$\left|\pi_q(n, C, \varepsilon) - \frac{1}{\Phi(X^{t+1})}\pi_q(n, \varepsilon)\right| \leq \frac{1}{\Phi(X^{t+1})} \sum_{\chi \neq \chi_o} \left| \sum_{\substack{\deg(P)=n \\ \psi(P)=\varepsilon}} \chi(P) \right|.$$

The result follows from Proposition 1. □

**Theorem 2.** *Let $t \in \mathbb{N}$, $t \geq 1$, $\mathbf{c} = (c_1, \ldots, c_t) \in \mathbb{F}_q^t$, and denote*

$$N_q(2m, \mathbf{c}) = \#\{Q \in \mathbb{I}_{2m}\ :\ Q \textit{ is self-reciprocal and } Q_i = c_i,\ i = 1, \ldots, t\}.$$

*Then*

$$\left|N_q(2m, \mathbf{c}) - q^{-t}\pi_q(m, -1)\right| \leq \tfrac{t+5}{m}(q-1)q^{\frac{m}{2}}.$$

Proof. From Lemma 5 we know that

$$N_q(2m, \mathbf{c}) = \sum_{c \in \mathbb{F}_q^*} \pi_q(m, C_c, \varepsilon),$$

where $C_c = 4^m/c + \sum_{i=1}^{t}(c_i 4^{m-i}/c)X^i$. For $q \equiv 1 \pmod 4$ or $m$ even, we have $\varepsilon = -1$. For $q \equiv 3 \pmod 4$ and $m$ odd, we have $\varepsilon = 1$. In this case, we see that

$$\pi_q(m, -1) = \frac{1}{2m} \sum_{\substack{d|m \\ d \text{ odd}}} \mu(d) q^{\frac{m}{d}} = \frac{1}{2}\pi_q(m).$$

Since $\pi_q(m, 1) + \pi_q(m, -1) = \pi_q(m)$ for $m \geq 2$, we obtain $\pi_q(m, 1) = \pi_q(m, -1)$. Theorem 1 implies that in every case,

$$\left|\pi_q(m, C_c, \varepsilon) - \frac{1}{\Phi(X^{t+1})}\pi_q(m, -1)\right| \leq \tfrac{t+5}{m} q^{\frac{m}{2}}.$$

It follows that

$$\left|N_q(2m, \mathbf{c}) - \frac{q-1}{\Phi(X^{t+1})}\pi_q(m, -1)\right| \leq \tfrac{t+5}{m}(q-1)q^{\frac{m}{2}}.$$

The result follows by noting that $\Phi(X^{t+1}) = (q-1)q^t$. □

Theorem 2 can be combined with well known formulas for $\pi_q(m, -1)$ to obtain esimates for $N_q(2m, \mathbf{c})$. This is done in the next corollary.

**Corollary 1.** *Let $t \in \mathbb{N}$, $t \geq 1$, $\mathbf{c} = (c_1, \ldots, c_t) \in \mathbb{F}_q^t$. Then*

$$\left| N_q(2m, \mathbf{c}) - \frac{q^{m-t}}{2m} \right| \leq \tfrac{t+5}{m} q^{\frac{m}{2}+1}.$$

*In particular, if $q^{\frac{m}{2}-t-1} > 2t + 10$ then there exists a monic self-reciprocal polynomial $Q$ of degree $2m$ such that $Q_i = c_i$ for $1 \leq i \leq t$.*

Proof. The following enumeration formulas have been known since the work of Carlitz [2] and have been proven by different methods in [3, 19, 20].

$$\pi_q(m, -1) = \begin{cases} \frac{1}{2m}(q^m - 1) & \text{, if } m = 2^s \\ \frac{1}{2m} \sum_{\substack{d \mid m \\ d \text{ odd}}} \mu(d) q^{\frac{m}{d}} & \text{, otherwise} \end{cases} .$$

The formulas imply the estimate

$$\left| \pi_q(m, -1) - \frac{q^m}{2m} \right| \leq \frac{q^{\frac{m}{3}}}{m}.$$

Combining this with Theorem 2, we obtain the stated result. □

## 5. Conclusion

In this work, we have proved estimates for the number of monic irreducible self-reciprocal polynomials of degree $2m$ over a finite field of odd characteristic, that have up to $m/2 - \log_q(2m) - 1$ low degree coefficients prescribed. Our method is based on that of Carlitz [2]. We should emphasize that our results apply to finite fields of odd characteristic. It would be interesting to extend the results of the present work to polynomials over $\mathbb{F}_2$ or, more generaly, over finite fields of characteristic two.

**Acknowlegdments**
This work was done while I was visiting the School of Mathematics and Statistics of Carleton University. I would like to thank Prof. Daniel Panario for the invitation and the School for the hospitality. I would also like to thank the reviewers for carefully reading the manuscript and for providing helpful comments.

[1] M. Car. Distribution des polynomes irreductibles dans $\mathbb{F}[t]$. *Acta Arith.*, 88:141–153, 1999.

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

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

[4] S.D. Cohen. The explicit construction of irreducible polynomials over finite fields. *Designs Codes and Cryptography*, 2:169 – 174, 1992.

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

[6] S.D. Cohen. Primitive polynomials with a prescribed coefficient. *Finite Fields Appl.*, 12(3):425–491, 2006.

[7] S.D. Cohen and D. Hachenberger. Primitive normal bases with prescribed traces. *Appl. Algebra Eng. Comm. Comp.*, 9:383 – 403, 1999.

[8] S.D. Cohen and D. Hachenberger. Primitivity, freeness, norm and trace. *Discrete Math.*, 214:135 – 144, 2000.

[9] S. Fan. Primitive normal polynomials with the last half coefficients prescribed. *Finite Fields Appl.*, 15:604 – 614, 2009.

[10] S.Q. Fan and W.B. Han. $p$-adic formal series and cohen's problem. *Glasg. Math. J.*, 46:47 – 61, 2004.

[11] S.Q. Fan and W.B. Han. Primitive polynomials over finite fields of characteristic two. *Appl. Algebra Eng. Comm. Comp.*, 14:381 – 395, 2004.

[12] S.Q. Fan, W.B. Han, K.Q. Feng, and X.Y. Zhang. Primitive normal polynomials with the first two coefficients prescribed: A revised $p$-adic method. *Finite Fields Appl.*, 13:577 – 604, 2007.

[13] T. Garefalakis. Irreducible polynomials with consecutive zero coefficients. *Finite Fields Appl.*, 14(1):201 – 208, 2008.

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

[15] S.J. Hong and D.C. Bossen. On some properties of self-reciprocal polynomials. *IEEE Trans. Inform. Theory*, IT-21:462 – 464, 1975.

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

[17] E.N. Kuz'min. Irreducible polynomials over finite fields i. *Algebra and Logic*, 33(4):216–232, 1994.

[18] J.L. Massey. Reversible codes. *Information Control*, 7:369 – 380, 1964.

[19] H. Meyn. On the construction of irreducible self-reciprocal polynomials over finite fields. *Appl. Algebra Eng. Comm. Comp.*, 1:43 – 53, 1990.

[20] H. Meyn and W. Götz. Self-reciprocal polynomials over finite fields. volume 413/S-21, pages 82 – 90. Publ. I.R.M.A. Strasbourg, 1990.

[21] R.L. Miller. Necklaces, symmetries and self-reciprocal polynomials. *Discrete Math.*, 22:25 – 33, 1978.

[22] M. Rosen. *Number theory in function fields*. Springer Verlag, 2002.

[23] D. Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.