On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials

Theodoulos Garefalakis, Giorgos Kapetanakis[1,*]

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

Abstract

Let q be a power of an odd prime and let $k, n \in \mathbb{N}$ such that $1 < k \leq n$. We investigate the existence of self-reciprocal irreducible monic polynomials over $\mathbb{F}_q$, of degree $2n$ and their k-th coefficient prescribed.

Keywords: Self-reciprocal polynomials, Hansen-Mullen conjecture, Character sums
2010 MSC: 12E05, 12E10, 11T06

1. Introduction

The properties of irreducible polynomials over finite fields have proved to be of great theoretical and practical interest. Such properties, that have been investigated, include primitivity, normality, having certain coefficients fixed to given values and combinations of those properties. For a survey of results in this line of research, we refer to [4] and the references therein.

Hansen and Mullen [10] conjectured that there exists an irreducible polynomial over $\mathbb{F}_q$ with an arbitary coefficient prescribed, with a couple of obvious exceptions.

Conjecture 1.1 (Hansen-Mullen). *Let $a \in \mathbb{F}_q$, let $n \geq 2$ and fix $0 \leq j < n$. Then there exists an irreducible polynomial $P(X) = X^n + \sum_{k=0}^{n-1} P_k X^k$ over $\mathbb{F}_q$ with $a_j = a$ except when $j = a = 0$ or q even, $n = 2$, $j = 1$, and $a = 0$.*

By considering primitive polynomials with given trace, Cohen [2] proves that the conjecture is true for $j = n - 1$. Hansen and Mullen proved their conjecture for $j = 1$. Wan [17] proved that the conjecture holds, for $q > 19$ or $n \geq 36$ and Ham and Mullen [9] proved the remaining cases with the help of computers. Those cases have also been settled theoretically by Cohen and Prešern [5, 6]. Several extensions of this result have been shown [7, 8, 15].

*Corresponding author
Email addresses: theo@math.uoc.gr (Theodoulos Garefalakis), gkapet@math.uoc.gr (Giorgos Kapetanakis)
[1]Tel: (+30) 2810 393821, Fax: (+30) 2810 393881

Given a polynomial $Q \in \mathbb{F}_q[X]$, its *reciprocal* Q^R is defined as $Q^R(X) = X^{\deg(Q)}Q(1/X)$. One class of polynomials that has been investigated [1, 3, 8, 13, 14] is that of *self-reciprocal irreducible polynomials*, that is, irreducible polynomials that satisfy $Q^R(X) = Q(X)$. Besides the theoretical interest in their existence and density, self-reciprocal irreducible polynomials have been useful in application, and in particular in the construction of error-correcting codes [11, 12].

It is natural to expect that self-reciprocal monic irreducible polynomials over finite fields, with some coefficient fixed, exist. In this work we restrict ourselves to the case where q is odd and prove that there exists a self-reciprocal irreducible monic polynomial over $\mathbb{F}_q$, of degree n with its k-th coefficient prescribed, provided that

$$q^{\frac{n-k-1}{2}} \geq \frac{16}{5}k(k+5) + \frac{1}{2}.$$

The proof of the main theorem is based on an estimate of a weighted sum, which is very similar to the one that Wan considers [17]. Our main tools are Weil's bound for character sums, Carlitz's [1] characterization of self-reciprocal irreducible monic polynomials over $\mathbb{F}_q$ and a character sum estimate proved in [8].

2. Preliminaries

Let q be a power of an odd prime and let $\mathbb{F}_q$ be the finite field with q elements. We denote by $\mathbb{I}_n$ the set of monic irreducible polynomials of degree n and by $\mathbb{J}_n$ the set of irreducible polynomials of degree n and constant term h_0 equal to 1. Further, we set $\mathbb{G}_k = \{h \in \mathbb{F}_q[X] \ : \ \deg(h) \leq k \text{ and } h_0 = 1\}$.

It is well known, see [1], that if Q is a self-reciprocal monic irreducible polynomial over $\mathbb{F}_q$, then $\deg(Q)$ is even and $Q(X) = X^n P(X + X^{-1})$ for some $P \in \mathbb{I}_n$ such that $\psi(P) = -1$, where $\psi(P) = (P|X^2 - 4)$, the Jacobi symbol of P modulo $X^2 - 4$. Conversely, if $P \in \mathbb{I}_n$, with $\psi(P) = -1$, and $Q = X^n P(X + X^{-1})$, then Q is a self-reciprocal monic irreducible.

We denote $P = \sum_{i=0}^{n} P_i X^i$ and $Q = \sum_{i=0}^{2n} Q_i X^i$, and we compute

$$\begin{aligned} Q(X) = X^n P(X + X^{-1}) &= \sum_{i=0}^{n} P_i X^{n-i}(X^2+1)^i \\ &= \sum_{i=0}^{n} P_i X^{n-i} \left(\sum_{j=0}^{i} \binom{i}{j} X^{2j} \right) = \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{i}{j} P_i X^{n-i+2j}. \end{aligned}$$

Since Q is monic and self-reciprocal, $Q_0 = 1$ and $Q_{2n-i} = Q_i$, so we may restrict ourselves to $1 \leq k \leq n$. The last equation implies that

$$Q_k = \sum_{\substack{0 \leq j \leq i \leq n \\ n-i+2j=k}} \binom{i}{j} P_i = \sum_{\substack{n-k \leq i \leq n \\ k-n+i \in 2\mathbb{Z}}} \binom{i}{\frac{k-n+i}{2}} P_i,$$

and by making the variable change $j = n - i$ we have

$$Q_k = \sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} P_{n-j}.$$

The coefficient Q_k is expressed in terms of the coefficients of the k largest degree terms of P. In order to express Q_k in terms of the coefficients of low degree terms of a polynomial related to P, we define the polynomial $\hat{P}$ as follows.

Definition 2.1. Let $g \in \mathbb{F}_q[X]$, $\deg(g) = n$. We define $\hat{g} = X^n g\left(\frac{4}{X}\right)$.

The following lemma summarizes the properties of the transformation.

Lemma 2.2. *Let $P \in \mathbb{J}_n$, $n \ge 2$. Then $\hat{P} \in \mathbb{I}_n$, $\hat{P}_i = 4^{n-i} P_{n-i}$. Further, $\psi(P) = -\varepsilon\psi(\hat{P})$, where*

$$\varepsilon := \begin{cases} -1, & \text{if } q \equiv 1 \pmod 4 \text{ or } n \text{ is even.} \\ 1, & \text{otherwise.} \end{cases}$$

Proof. Since P is irreducible of degree $n \ge 2$, we see that $\hat{P}$ is of degree n. The irreducibility of $\hat{P}$ follows from the fact that if θ is a root of P, then $4/\theta$ is a root of $\hat{P}$, and $\mathbb{F}_q(\theta) = \mathbb{F}_q(4/\theta)$. The statement regarding the coefficients of $\hat{P}$ is easily verified and the one regarding $\psi(\hat{P})$ is proven in [8, Lemma 2]. □

Let $a \in \mathbb{F}_q$ and suppose that there exists an irreducible polynomial $P \in \mathbb{J}_n$, such that $\psi(P) = \varepsilon$ and $\sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} 4^j P_j = a$. Then Lemma 2.2 implies that $\hat{P} \in \mathbb{I}_n$ and $\psi(\hat{P}) = -1$. If we let $Q = X^n \hat{P}(X + X^{-1})$, we have

$$Q_k = \sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} \hat{P}_{n-j} = \sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} 4^j P_j = a.$$

For convenience, we define

$$\delta_j = \begin{cases} \binom{n-j}{\frac{k-j}{2}} 4^j, & \text{if } k - j \equiv 0 \pmod 2, \\ 0, & \text{if } k - j \equiv 1 \pmod 2. \end{cases}$$

We note that $\delta_k = 4^k \ne 0$. If we let $P \equiv h \pmod{X^{k+1}}$, for a polynomial h of degree at most $k-1$, the condition $\sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} 4^j P_j = a$ becomes

$$\sum_{j=0}^{k} \delta_j h_j = a.$$

This leads us to define the following map.

Definition 2.3. For $n, k \in \mathbb{N}$ with $1 \leq k \leq n$, we define

$$\begin{aligned} \tau_{n,k} : \mathbb{G}_k &\longrightarrow \mathbb{F}_q, \\ h &\mapsto \sum_{j=0}^{k} \delta_j h_j. \end{aligned}$$

Our observations are summarized in the following proposition.

Proposition 2.4. *Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. Suppose that there exists an irreducible polynomial $P \in \mathbb{J}_n$, such that $\psi(P) = \varepsilon$ and $P \equiv h \pmod{X^{k+1}}$ for some $h \in \mathbb{G}_k$ with $\tau_{n,k}(h) = a$. Then there exists a self-reciprocal monic irreducible polynomial Q, of degree $2n$, with $Q_k = a$.*

In the proceeding sections we will need to correlate the inverse image of $\tau_{n,k}$ with $\mathbb{G}_{k-1}$. This is achieved in the proposition below.

Proposition 2.5. *Let $a \in \mathbb{F}_q$, $n, k \in \mathbb{N}$, $n \geq 2$ and $1 \leq k \leq n$. Let $f = \sum_{i=0}^{k} f_i X^i \in \mathbb{F}_q[X]$, with $f_0 = 1$ and $f_i = \delta_{k-i}\delta_k^{-1}$, $1 \leq i \leq k-1$, and $f_k = \delta_k^{-1}(\delta_0 - a)$. Then the map $\sigma_{n,k,a} : \tau_{n,k}^{-1}(a) \to \mathbb{G}_{k-1}$ defined by $\sigma_{n,k,a}(h) = hf \pmod{X^{k+1}}$ is a bijection.*

Proof. We start by showing that the map is well-defined. The polynomial $\sigma_{n,k,a}(h)$, by its definition, is of degree at most k and has constant term equal to 1. The coefficient of X^k of $\sigma_{n,k,a}(h)$ is $h_k + f_k + \sum_{j=1}^{k-1} h_j f_{k-j}$. Noting that $\tau_{n,k}(h) = a$, we compute

$$\begin{aligned} f_k + h_k + \sum_{j=1}^{k-1} h_j f_{k-j} &= -a\delta_k^{-1} + \delta_0\delta_k^{-1} + h_k\delta_k\delta_k^{-1} + \sum_{j=1}^{k-1} h_j\delta_j\delta_k^{-1} \\ &= -a\delta_k^{-1} + \delta_k^{-1}\left(\sum_{j=0}^{k} h_j\delta_j\right) \\ &= -a\delta_k^{-1} + \delta_k^{-1}\tau_{n,k}(h) = 0. \end{aligned}$$

This shows that $\deg(\sigma_{n,k,a}(h)) \leq k-1$, and the map is well-defined.

To see that the map is one-to-one, consider $h_1, h_2 \in \tau_{n,k}^{-1}(a)$ such that $\sigma_{n,k,a}(h_1) = \sigma_{n,k,a}(h_2)$. This implies that

$$h_1 f \equiv h_2 f \pmod{X^{k+1}}.$$

Since f is invertible modulo X^{k+1}, we obtain $h_1 \equiv h_2 \pmod{X^{k+1}}$, which implies $h_1 = h_2$ since $\deg(h_1), \deg(h_2) \leq k$.

It is trivial that $\#\mathbb{G}_{k-1} = q^{k-1}$. The proof will be complete once we show that $\#\tau_{n,k}^{-1}(a) = q^{k-1}$. It is clear that $\tau_{n,k}$ is linear and surjective, therefore, the dimension of its kernel is equal to $k-1$. It follows that the kernel, and therefore the fibers of $\tau_{n,k}$, have cardinality q^{k-1}. □

Remark. We easily check that in the above proof we could substitude $\tau_{n,k}$ with an arbitary $\mathbb{F}_q$-linear $\tau : \mathbb{G}_k \to \mathbb{F}_q$, such that $\tau(X^k) \neq 0$, since this is the only property of $\tau_{n,k}$ we actually used.

3. Character sums

Let $M \in \mathbb{F}_q[X]$ be a polynomial of degree at least 1 and suppose χ is a non-trivial Dirichlet character modulo M. The Dirichlet L-function associated with χ is defined to be

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

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

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

It turns out that $L(u,\chi)$ is a polynomial in u of degree at most $\deg(M) - 1$. Further, $L(u,\chi)$ has an Euler product,

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

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

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

where the inner sum runs over monic irreducible polynomials of degree d, i.e., over the set $\mathbb{I}_d$. Weil's theorem of the Riemann hypothesis for function fields implies (see [17] and the references therein) the following theorem.

Theorem 3.1. *Let χ be a Dirichlet character modulo M. Then*

1. *If $\chi \neq \chi_o$ then*
$$|c_n(\chi)| \leq (\deg(M) - 1)q^{\frac{n}{2}}.$$
2. *If $\chi \neq \chi_o$ and $\chi(\mathbb{F}_q^*) = 1$, then*
$$|1 + c_n(\chi)| \leq (\deg(M) - 2)q^{\frac{n}{2}}.$$

For a detailed account of the above well-known facts, see [16, Chapter 4]. We will also need the following result of [8].

Theorem 3.2. *Let χ be a non-trivial Dirichlet character modulo X^{k+1}. Then the following bounds hold:*

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

$$\left| \sum_{\substack{P \in \mathbb{I}_n \\ \psi(P)=-1}} \chi(P) \right| \leq \tfrac{k+5}{n} q^{\frac{n}{2}}.$$

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

$$\left| \sum_{\substack{P \in \mathbb{I}_n \\ \psi(P)=1}} \chi(P) \right| \leq \tfrac{k+5}{n} q^{\frac{n}{2}}.$$

Let Λ be the von Mangoldt function on $\mathbb{F}_q[X]$, which is defined as follows: $\Lambda(h) = \deg(P)$, if h is a power of the irreducible polynomial P, and is zero otherwise. We also let $\Lambda(1) = 1$. Then one can see that

$$c_n(\chi) = \sum_{\deg(h)=n} \Lambda(h)\chi(h)$$

where the sum runs over monic polynomials of degree n.

We will encounter character sums, which involve a character χ that is trivial on $\mathbb{F}_q^*$, and where the sums run over polynomials with constant term equal to 1 (not necessarily monic). Estimates for such character sums, follow directly from the estimates of the related sums that run over monic polynomials. Since our focus will be on Dirichlet characters modulo X^{k+1}, we state our proposition accordingly.

Proposition 3.3. *Let* $n, k \in \mathbb{N}$, $1 \leq k \leq n$ *and let* $\chi \neq \chi_o$ *be a Dirichlet character modulo* X^{k+1}, *such that* $\chi(\mathbb{F}_q^*) = 1$.

$$\left| \sum_{\substack{\deg(h)=n \\ h_0=1}} \Lambda(h)\chi(h) \right| \leq 1 + kq^{\frac{n}{2}}, \quad \textit{for } n \geq 1. \tag{1}$$

$$\left| \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P)=\varepsilon}} \chi(P) \right| \leq \tfrac{k+5}{n} q^{\frac{n}{2}}, \quad \textit{for } n \geq 2, \tag{2}$$

where either $\varepsilon = -1$, *or* $\varepsilon = 1$ *and* n *is odd.*

Proof. For Eq. (1), we note that as h runs over the polynomials of degree n with constant term 1, h/h_n runs over the monic polynomials of degree n. Taking into account that $\chi(\mathbb{F}_q^*) = 1$, we have

$$\left| \sum_{\substack{\deg(h)=n \\ h_0=1}} \Lambda(h)\chi(h) \right| = \left| \sum_{\substack{\deg(h)=n \\ h_0=1}} \Lambda(h)\chi\left(\frac{h}{h_n}\right) \right| = \left| \sum_{\substack{\deg(h)=n \\ h \text{ monic}}} \Lambda(h)\chi(h) \right|$$

and the bound follows from Theorem 3.1. For Eq. (2) the same observation applies, that is, as P runs over $\mathbb{J}_n$, P/P_n runs over $\mathbb{I}_n$. Further, for any constant $c \in \mathbb{F}_q^*$, $\psi(c) = 1$. The bound in Eq. (2) now follows from Theorem 3.2. $\square$

4. Weighted sum

Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$ and $a \in \mathbb{F}_q$. Inspired by Wan's work [17] we introduce the following weighted sum.

$$w_a(n,k) = \sum_{h \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(h)) \sum_{\substack{P \in \mathbb{J}_n, \psi(P)=\varepsilon \\ P \equiv h \pmod{X^{k+1}}}} 1. \tag{3}$$

It is clear that if $w_a(n,k) > 0$, then there exists some $P \in \mathbb{J}_n$ such that $P \equiv h \pmod{X^{k+1}}$ for some $h \in \mathbb{G}_k$, with $\tau_{n,k}(h) = a$ and $\psi(P) = \varepsilon$. Then Proposition 2.4 implies that there exists a self-reciprocal, monic irreducible polynomial Q, of degree n with $Q_k = a$.

Let U be the subgroup of $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ that contains classes of polynomials with constant term equal to 1. Then $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ is the direct sum of U and $\mathbb{F}_q^*$. The set $\mathbb{G}_{k-1}$ is a set of representatives of U. Further, the group of characters of U consists exactly of those characters of $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ that are trivial on $\mathbb{F}_q$, that is, $\widehat{U} = \{\chi \in \widehat{(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*} \ : \ \chi(\mathbb{F}_q^*) = 1\}$. Using these observations and with the help of the orthogonality relations, Eq. (3) can be rewritten as

$$w_a(n,k) = \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P)=\varepsilon}} \chi(P) \sum_{h \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(h)) \bar{\chi}(h),$$

If we denote by g the inverse of f modulo X^{k+1}, where f as defined in Proposition 2.5, and using Proposition 2.5, we obtain

$$\begin{aligned} w_a(n,k) &= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P)=\varepsilon}} \chi(P) \sum_{h \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(h)) \bar{\chi}(\sigma_{n,k,a}(h)g) \\ &= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P)=\varepsilon}} \chi(P)\bar{\chi}(g) \sum_{h \in \mathbb{G}_{k-1}} \Lambda(h)\bar{\chi}(h). \end{aligned}$$

Separating the term that corresponds to χ_o, we have

$$\left| w_a(n,k) - \frac{\pi_q(n,\varepsilon)}{q^k} \sum_{h \in \mathbb{G}_{k-1}} \Lambda(h) \right| \leq \frac{1}{q^k} \sum_{\chi \neq \chi_o} \left| \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P)=\varepsilon}} \chi(P) \right| \left| \sum_{h \in \mathbb{G}_{k-1}} \Lambda(h)\bar{\chi}(h) \right|,$$

where $\pi_q(n,\varepsilon) = \#\{P \in \mathbb{I}_n : \psi(P) = \varepsilon\}$. It is computed in [1],

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

If n is not a power of 2, we have

$$\left|\pi_q(n,-1) - \frac{q^n}{2n}\right| \leq \frac{1}{2n}\frac{q}{q-1} q^{\frac{n}{3}}. \tag{4}$$

Note that the bound remains true in the case that n is a power of 2. If n is even, then $\varepsilon = -1$. If n is odd then $\pi_q(n,-1) = \frac{1}{2n}\sum_{d|n}\mu(d)q^{\frac{n}{d}} = \frac{1}{2}\pi_q(n)$. Since $\pi_q(n,-1) + \pi_q(n,1) = \pi_q(n)$, we conclude that $\pi_q(n,1) = \pi_q(n,-1)$. Thus, in every case, $\pi_q(n,\varepsilon) = \pi_q(n,-1)$. Furthermore,

$$\sum_{h \in \mathbb{G}_{k-1}} \Lambda(h) = \sum_{m=0}^{k-1} \sum_{\substack{\deg(h)=m \\ h_0=1}} \Lambda(h) = \sum_{m=0}^{k-1} q^m = \frac{q^k-1}{q-1}.$$

Eq.(1) of Proposition 3.3 implies that

$$\left|\sum_{h \in \mathbb{G}_{k-1}} \Lambda(h)\bar{\chi}(h)\right| \leq 1 + \sum_{m=1}^{k-1}(1 + kq^{\frac{m}{2}}) = k\frac{q^{\frac{k}{2}}-1}{\sqrt{q}-1}.$$

Putting everything together, and using Eq.(2) we have

$$\left|w_a(n,k) - \frac{q^k-1}{q^k(q-1)}\pi_q(n,-1)\right| \leq \frac{k(k+5)}{n}\frac{(q^k-1)(q^{\frac{k}{2}}-1)q^{\frac{n}{2}}}{q^k(\sqrt{q}-1)}. \tag{5}$$

The following theorem follows directly from this bound.

Theorem 4.1. *Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a monic, self-reciprocal irreducible polynomial $Q \in \mathbb{F}_q[X]$, of degree n with $Q_k = a$ if the following bound holds.*

$$\pi_q(n,-1) \geq \frac{k(k+5)}{n}(\sqrt{q}+1)q^{\frac{n+k}{2}}.$$

Proof. From our previous discussion, it suffices to show that $w_a(n,k) > 0$. Eq. (5) implies that a sufficient condition is

$$\frac{q^k-1}{q^k(q-1)}\pi_q(n,-1) > \frac{k(k+5)}{n}\frac{(q^k-1)(q^{\frac{k}{2}}-1)q^{\frac{n}{2}}}{q^k(\sqrt{q}-1)},$$

that is,

$$\pi_q(n,-1) > \frac{k(k+5)}{n}(\sqrt{q}+1)(q^{\frac{k}{2}}-1)q^{\frac{n}{2}}. \tag{6}$$

The stated condition follows easily. □

Substituting the bound of Eq. (4) in Theorem 4.1, we obtain the following.

Theorem 4.2. *Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a monic, self-reciprocal irreducible polynomial $Q \in \mathbb{F}_q[X]$, of degree n with $Q_k = a$ if the following bound holds.*

$$q^{\frac{n-k-1}{2}} \geq \frac{16}{5}k(k+5) + \frac{1}{2}.$$

PROOF. From Theorem 4.1 and Eq. (4), we see that a sufficient condition is

$$\frac{q^n}{2n} - \frac{q}{q-1}\frac{q^{\frac{n}{3}}}{2n} \geq \frac{k(k+5)}{n}(\sqrt{q}+1)q^{\frac{n+k}{2}}.$$

Using the fact that $\frac{q}{q-1} \leq \frac{3}{2}$ and $\sqrt{q}+1 \leq \frac{16\sqrt{q}}{10}$ for $q \geq 3$, we obtain the sufficient condition

$$q^{\frac{n-k+1}{2}} \geq \frac{16k(k+5)}{5} + \frac{3}{2}q^{-\frac{n}{6}-\frac{k}{2}-\frac{1}{2}}.$$

Since $\frac{3}{2}q^{-\frac{n}{6}-\frac{k}{2}+\frac{1}{2}} \leq \frac{1}{2}$, the condition in the statement follows. □

REMARK. As pointed out at the Remark after Proposition 2.5 we could have more general results by choosing an arbitary $\mathbb{F}_q$-linear $\tau : \mathbb{G}_k \to \mathbb{F}_q$, such that $\tau(X^k) \neq 0$. In this case, if the bounds of Theorems 4.1 or 4.2 hold, then there exists some $P \in \mathbb{I}_n$, with $\psi(P) = -1$ and $\hat{P} \equiv h \bmod X^{k+1}$ for some $h \in \tau^{-1}(a)$, for any $a \in \mathbb{F}_q$.

5. An example

If we content ourselves to any $k \leq n/2$, Eq. (6) gives us that there exists a monic irreducible self-reciprocal polynomial over $\mathbb{F}_q$, where q a power of an odd prime, of degree $2n$ with it's k-th coefficient prescribed, if

$$\pi_q(n, -1) > \frac{\lfloor n/2 \rfloor(\lfloor n/2 \rfloor + 5)}{n}(\sqrt{q}+1)(q^{\lfloor n/2 \rfloor/2} - 1)q^{n/2}. \tag{7}$$

With the help of computers (using Maple) we can use Eq. (7) to find pairs (q, n) such that if q is a power of an odd prime and n an integer, then there exists some monic irreducible self-reciprocal polynomial over $\mathbb{F}_q$ of degree $2n$ such that any of its $\lfloor n/2 \rfloor$ low degree coefficients is prescribed. Such pairs are illustrated in Table 1.

Corollary 5.1. *If $n \geq 3$ an integer and q a power of an odd prime, then there exists a monic irreducible self-reciprocal polynomial over $\mathbb{F}_q$ of degree $2n$ such that any of its $\lfloor n/2 \rfloor$ low degree coefficients is prescribed, if either $n \geq 27$ or $q \geq 839$.*

Table 1: Pairs (q, n) that satisfy Eq. (7).

n	3	4	5	6	7	8	9	10
q	≥ 149	≥ 839	≥ 37	≥ 59	≥ 17	≥ 23	≥ 11	≥ 13
n	11	12	13	14	15	16	17	18
q	≥ 9	≥ 9	≥ 7	≥ 7	≥ 5	≥ 7	≥ 5	≥ 5
n	19	20	21	22	23	24	25	26
q	≥ 5	≥ 5	≥ 5	≥ 5	≥ 5	≥ 5	≥ 3	≥ 5

PROOF. It is clear that if the bound of Theorem 4.2 holds for some q_o and $k = n/2$, then it still holds for any $q \geq q_o$ and $1 \leq k \leq n/2$. Also it is not hard to see that

$$3^{\frac{n-\frac{n}{2}-1}{2}} \geq \frac{16}{5}\frac{n}{2}\left(\frac{n}{2}+5\right)+\frac{1}{2}$$

for all $n \geq 27$, since the function

$$g(n) = 3^{\frac{n-2}{4}} - \frac{4}{5}n(n+10) + \frac{1}{2}$$

is increasing for $n \geq 27$ and $g(27) > 0$. Further, from Table 1, we see that our statement is true for $q \geq 839$. □

Acknowledgments
We would like to thank the anonymous reviewers for carefully reading the paper and for providing useful comments.

References

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

[2] S. D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.

[3] S. D. Cohen. The explicit construction of irreducible polynomials over finite fields. *Des. Codes Cryptogr.*, 2(2):169–174, 1992.

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

[5] S. D. Cohen and M. Prešern. Primitive polynomials with prescribed second coefficient. *Glasgow Math. J.*, 48:281–307, 2006.

[6] S. D. Cohen and M. Prešern. The Hansen-Mullen primitivity conjecture: completion of proof. In *Number theory and polynomials*, volume 352 of *LMS Lecture notes*, pages 89–120. Cambridge University Press, Cambridge, 2008.

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

[8] T. Garefalakis. Self-reciprocal irreducible polynomials with prescribed coefficients. *Finite Fields Appl.*, 17(2):183–193, 2011.

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

[10] T. Hansen and G. L. Mullen. Primitive polynomials over finite fields. *Math. Comp.*, 59(200):639–643, 1992.

[11] S. Hong and D. Bossen. On some properties of self-reciprocal polynomials. *IEEE Trans. Information Theory*, 21(4):462–464, 1975.

[12] J. L. Massey. Reversible codes. *Information and Control*, 7(3):369–380, 1964.

[13] H. Meyn. On the construction of irreducible self-reciprocal polynomials over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):43–53, 1990.

[14] H. Meyn and W. Götz. Self-reciprocal polynomials over finite fields. *Publ. Inst. Rech. Math. Av.*, 413/S-21:82–90, 1990.

[15] D. Panario and G. Tzanakis. A generalization of the Hansen-Mullen conjecture on irreducible polynomials over finite fields. To appear.

[16] M. Rosen. *Number Theory in Function Fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

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