A generalization of the Hansen–Mullen conjecture on irreducible polynomials over finite fields

Daniel Panario *,1, Georgios Tzanakis

School of Mathematics and Statistics, Carleton University, Ottawa, K1S 5B6, Canada

Article history:
Received 24 May 2011
Revised 28 July 2011
Accepted 5 September 2011
Available online 22 September 2011
Communicated by Stephen D. Cohen

MSC:
11T06
12Y05

Keywords:
Irreducible polynomials
Hansen–Mullen conjecture
Dirichlet characters
Finite fields

1. Introduction

Let q be a prime power, let \( \mathbb{F}_q \) denote the finite field with q elements and set \( \mathbb{A} = \mathbb{F}_q[x] \). Denote by \( \mathcal{I}_n \) the set of monic irreducible polynomials in \( \mathbb{A} \) with degree \( n \) and \( I_n = |\mathcal{I}_n| \). It is well known that

\[
\frac{q^n}{n} - \frac{2q^n}{n} \leq I_n \leq \frac{q^n}{n} - \frac{q}{n}
\]  

(for instance, see [27]). However much less is known about the number or the existence of polynomials of \( \mathcal{I}_n \) with a number of coefficients prescribed.

* Corresponding author.

E-mail addresses: daniel@math.carleton.ca (D. Panario), gtzanaki@math.carleton.ca (G. Tzanakis).

1 This author is partially supported by NSERC of Canada.

© 2011 Elsevier Inc. All rights reserved.

doi:10.1016/j.ffa.2011.09.003
Let \( m, n \) be integers with \( 1 \leq m \leq n \), \( \alpha \in \mathbb{F}_q \) and suppose there exists an irreducible polynomial \( P \) of degree \( n \) over \( \mathbb{F}_q \) with the coefficient of \( x^m \) being \( \alpha \). We say that we prescribe the coefficient of \( x^m \) of \( P \) to \( \alpha \). One aspect of the study of polynomials over finite fields which has been researched extensively is that of the existence and number of irreducible polynomials with prescribed coefficients.

Some of the strongest results in this area follow from the analogue of Dirichlet’s theorem in \( \mathbb{A} \) (see [33]) and generalizations by Car [3] and Hsu [22]; see also [34]. Irreducible polynomials exist with roughly half their coefficients prescribed to any element, subject to them being leading and/or trailing ones. The case of prescribed coefficients in the middle of the polynomial is not covered. Hansen and Mullen [20] conjectured that for any \( n \) there exist polynomials in \( \mathbb{I}_n \) with any one coefficient prescribed. The conjecture was proved by Wan [38] for all but a finite number of cases and was completely settled in [19].

A class of irreducible polynomials that is of practical interest is irreducible polynomials with a large number of consecutive zero coefficients. The generalizations of Dirichlet’s theorem mentioned above also apply in that special case (that is, roughly half the leading and/or trailing coefficients of an irreducible can be prescribed to zero). Garefalakis [16] shows that there also exist polynomials in \( \mathbb{I}_n \) with roughly \( n/3 \) consecutive zero coefficients, covering cases that are not settled by Dirichlet’s theorem. However, it should be pointed out that in some cases we need irreducible polynomials with more than \( n/2 \) zero coefficients. For instance, Coppersmith’s algorithm for discrete logarithm computations requires at least \( n - \log_2 n \) leading zeros [11].

The above mentioned results are based on Weil’s bounds for character sums (these are discussed in Section 2.2). Other results are obtained using completely different tools (like Stickelberger’s theorem and discriminants [35]). For instance, there is active research regarding some interesting special cases of polynomials with many consecutive zero coefficients, such as binomials \([21,31]\), trinomials \([1,2,6,17,28,32,36]\), tetranomials \([18]\), and pentanomials \([23]\), that is, polynomials with two, three, four, and five nonzero coefficients, respectively.

Regarding polynomials with a few coefficients prescribed, current results include the number of irreducible polynomials with their first and last coefficient prescribed [4], the two most significant coefficients prescribed [5,25,26], the three most significant coefficients prescribed, and their trace and constant coefficients prescribed [24,29,30]. We note that some of these results apply only to the finite field with two elements.

We would like to stress that in this work we do not consider primitive or normal polynomials with prescribed coefficients. These have been the focus of substantial recent research (see for instance \([7–10,12–15]\)), but are beyond the scope of this work; we focus on irreducible polynomials only.

The structure of this paper is as follows. In Section 2 we give the preliminaries that are needed for the rest of the paper; we briefly present Dirichlet characters and the bounds for some Dirichlet character sums (Weil bounds), which are the cornerstone of this work. We also discuss Dirichlet’s theorem, which yields some of the strongest results in this area. In Section 3 we prove the main theorem; all the results presented in this paper are consequences of this theorem. Those applications of the main theorem are presented in Section 4 and are divided into two categories: a generalization of the Hansen–Mullen conjecture for irreducible polynomials is presented in Section 4.1, whereas irreducible polynomials with a large number of consecutive zero coefficients are discussed in Section 4.2. Finally, in Section 5 we comment on potential future research.

2. Preliminaries

We first record the following well-known lemma that we use later on.

**Lemma 1.** Let \( n > 1 \). Then, \( \sum_{i=0}^{n} a_i x^i \in \mathbb{I}_n \) if and only if \( \sum_{i=0}^{n} \frac{a_{n-i}}{a_0} x^i \in \mathbb{I}_n \).

2.1. Dirichlet characters

Consider a character \( \chi \) of the multiplicative group \((\mathbb{A}/\mathbb{F})^*\). A Dirichlet character modulo \( f \) is an extension of \( \chi \) to \( \mathbb{A} \) by zero. More precisely, we have the following definition.
Definition 1. Let \( f \in \mathbb{A} \) of positive degree. A Dirichlet character modulo \( f \) is a map \( \chi \) from \( \mathbb{A} \) to \( \mathbb{C} \) such that for all \( a, b \in \mathbb{A} \):

1. \( \chi(a + bf) = \chi(a) \),
2. \( \chi(a) \chi(b) = \chi(ab) \),
3. \( \chi(a) = 0 \iff (a, f) \neq 1 \).

It follows that \( |\chi(a)| = 1 \) when \( \chi(a) \neq 0 \). The Dirichlet character \( \chi_0 \) modulo \( f \) which maps all \( a \in \mathbb{A} \) with \( (a, f) = 1 \) to 1 is called the trivial Dirichlet character. We denote the set of all Dirichlet characters modulo \( f \) as \( X_f \). With each Dirichlet character \( \chi \) modulo \( f \) there is associated the conjugate character \( \chi' \) defined by \( \chi'(a) = \chi(\bar{a}) \) for all \( a \in \mathbb{A} \). We define the product of two Dirichlet characters by setting \( \chi \psi(a) = \chi(a) \psi(a) \) for all \( a \in \mathbb{A} \). This makes \( X_f \) into a group with the trivial Dirichlet character being the neutral element and the conjugate of a Dirichlet character being its inverse.

The following fact about product of Dirichlet characters is easy to prove.

Lemma 2. Let \( \chi_1, \ldots, \chi_r \) be Dirichlet characters modulo \( f_1, f_2, \ldots, f_r \in \mathbb{A} \), respectively. Then the map \( X : \mathbb{A} \to \mathbb{C}^\ast \) such that \( X(h) = \prod_{i=1}^{r} \chi_i(h) \) is a Dirichlet character modulo \( \prod_{i=1}^{r} f_i \).

2.2. Weil bounds

Bounds of certain character sums, often referred to as Weil bounds, are the cornerstones of this work as well as important results, including an asymptotic version of Dirichlet’s theorem in \( \mathbb{A} \) (discussed in the next section) and Wan’s proof of the Hansen–Mullen conjecture. We define

\[
c_n(\chi) = \sum_{d|n} \sum_{P \in I_d} d \chi(P^n) \quad \text{and} \quad c'_n(\chi) = \sum_{P \in I_n} \chi(P).
\]

We define \( I_n \) to be the set of all monic primary polynomials of degree \( n \), that is, monic polynomials of degree \( n \) which are a power of an irreducible. For convenience we write

\[
c_n(\chi) = \sum_{h \in \mathbb{I}_n} \Lambda(h) \chi(h),
\]

where \( \Lambda \) is an analogue of the von Mangolt function in \( \mathbb{A} \) that we define as

\[
\Lambda(h) = \begin{cases} 
\deg P & \text{if } h = aP^e, \text{ some irreducible } P \in \mathbb{A}, \ a \in \mathbb{F}_q^\ast, \ e \in \mathbb{Z}\geq 0, \\
0 & \text{otherwise}.
\end{cases}
\]

Proposition 1. Let \( n \) be a positive integer, \( f \in \mathbb{A} \) and \( \chi \) a non-trivial Dirichlet character modulo \( f \). With \( c_n \) and \( c'_n \) as defined above, we have

\[
|c_n(\chi)| \leq (\deg(f) - 1)q^{n/2} \quad \text{and} \quad |c'_n(\chi)| \leq \frac{\deg(f)}{n} q^{n/2}.
\]

Furthermore, \( c_n(\chi_0) = q^n \) and \( c'_n(\chi_0) = l_n \).

It is important to note that the proofs of the above bounds used the Riemann hypothesis for function fields. For a detailed discussion about these bounds, we refer the interested reader to [33].
2.3. Dirichlet’s theorem and irreducible polynomials with prescribed coefficients

One of the most important results regarding irreducible polynomials with prescribed coefficients follows directly from an asymptotic version of Dirichlet’s theorem for primes in arithmetic progressions in the context of the ring of polynomials over a finite field. For instance, in [38, Theorem 5.1] we find the following effective version of Dirichlet’s theorem in \( \mathbb{A} \).

**Theorem 1.** Let \( f, g \in \mathbb{A} \) be such that \((f, g) = 1\) and \( \pi(n; f, g) \) denote the number of polynomials in \( \mathbb{I}_n \) which are congruent to \( g \) modulo \( f \). Then

\[
\left| \pi(n; f, g) - \frac{q^n}{n \Phi(f)} \right| \leq \frac{1}{n} (\deg(f) + 1) q^n.
\]

(2)

By setting \( f(x) = x^m \) and a suitable choice of \( g \) in Theorem 1, we have the following.

**Corollary 1.** Let \( m, n \) be positive integers and \( \alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_q \). If \( m \leq n/2 - \log_q n \), then there exists a polynomial in \( \mathbb{I}_n \) with its \( m \) least significant coefficients being \( \alpha_0, \ldots, \alpha_{m-1} \).

The following generalization of this result follows from [22] and [3]; see Fig. 1.

**Corollary 2.** Let \( k, m, n \) be positive integers with \( 1 \leq k, m \leq n \) and \( \alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_m \in \mathbb{F}_q \). If \( k + m \leq n/2 - \log_q n \), then there exists a polynomial in \( \mathbb{I}_n \) with its \( k + 1 \) most significant coefficients being \( 1, \alpha_1, \ldots, \alpha_k \) and its \( m \) least significant coefficients being \( \beta_1, \ldots, \beta_m \).

Hansen and Mullen [20] conjectured that given integers \( m, n \) with \( n > m \geq 0 \), there exists a polynomial in \( \mathbb{I}_n \) with the coefficient of \( x^m \) being any given element \( \alpha \in \mathbb{F}_q \), where of course \( \alpha \neq 0 \) if \( m = 0 \). We observe that the above results do not answer the conjecture when \( |m - n/2| < \log_q n \); this was settled in [38] and [19].

3. The main theorem

We use estimates of a product of weighted sums similar to the ones Wan uses in [38] and Garefalakis in [16] to obtain some new results regarding the existence of monic irreducible polynomials with prescribed coefficients.

In Theorem 2 below we consider irreducible polynomials of a general form (see Fig. 2); our main results in the next section all follow from special cases of this theorem.
Theorem 2. Let \( n \geq 3, m_1, \ldots, m_r, l_1, \ldots, l_r \) be integers such that \( n \geq m_1 \geq l_1 > m_2 \geq l_2 > \cdots > m_r \geq l_r \geq 1 \) and \( \alpha_1, \ldots, \alpha_r \in \mathbb{F}_q^* \) with \( \alpha_r \neq 0 \) if \( l_r = 1 \). Set \( m = \sum_{i=1}^r m_i \) and \( l = \sum_{i=1}^r l_i \). If
\[
\sum_{i=1}^n \frac{1}{i} \frac{\Phi(i)}{\Phi(n)} \frac{\chi_1(i)}{\chi_2(i)} \geq \frac{\Phi(m_1)}{\Phi(m)} \sum_{i=1}^m \frac{\chi_1(i)}{\chi_2(i)} \sum_{i=1}^r \frac{\alpha_i}{\alpha_r},
\]
then there exists an irreducible polynomial of the form
\[
x^r + \sum_{i=0}^{n-1} a_i x^i, \quad a_i \in \mathbb{F}_q,
\]
such that \( a_j = 0 \) for all \( m_i > j > l_i, 1 \leq i \leq r \), and \( a_j = \alpha_j \) for \( j = l_1 - 1, \ldots, l_r - 1 \).

For the sake of simplicity and readability, we give the proof for the special case when \( r = 2 \) of Theorem 2; the proof for an arbitrary \( r \) is essentially the same, but only more convoluted. The interested reader is referred to [37] for a complete proof of the general case in full details.

Theorem 3. Let \( n \geq 3, m_1, m_2, l_1, l_2 \) be integers such that \( n \geq m_1 \geq l_1 > m_2 \geq l_2 > 1 \) and \( \alpha_1, \alpha_2 \in \mathbb{F}_q^* \) with \( \alpha_2 \neq 0 \) if \( l_2 = 1 \). Set \( m = m_1 + m_2 \) and \( l = l_1 + l_2 \). If
\[
n - 2(r + 1) \log_q n - 2 \log_q r - r \geq 2m - l,
\]
then there exists a polynomial in \( \mathbb{F}_q \) of the form
\[
x^n + \sum_{i=0}^{n-1} a_i x^i, \quad a_i \in \mathbb{F}_q,
\]
such that \( a_j = 0 \) for all \( m_i > j > l_i, 1 \leq i \leq 2 \), and \( a_j = \alpha_j \) for \( j = l_1 - 1, l_2 - 1 \).

Proof. Let
\[
w = w(n, m_1, m_2, \alpha_1, \alpha_2) = \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1-1}} A(h_1) \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2-1}} A(h_2) \sum_{P \in \mathbb{I}_n} 1,
\]
where the last sum expands over all \( P \in \mathbb{I}_n \) such that \( P \equiv h_i \) (mod \( \mathbb{X}^{m_i} \)), \( i = 1, 2 \). We note that such a \( P \) is of the desired form, and the sums \( \sum_{h_i \in \alpha_i \mathbb{H}_{l_i-1}} A(h_i) \) are non-negative. Thus \( w \) being positive implies the existence of polynomials of the desired form; we prove that when (4) holds, then \( w \) is positive. Using some well-known group theoretical arguments we can rewrite \( w \) as
\[
w = \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1-1}} \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2-1}} A(h_1) A(h_2) \sum_{P \in \mathbb{I}_n} \frac{1}{\Phi(\mathbb{X}^{m_1})} \sum_{\chi_1} \chi_1(P) \frac{\chi_1(h_1)}{\chi_1(h_2)} \frac{1}{\Phi(\mathbb{X}^{m_2})} \sum_{\chi_2} \chi_2(P) \frac{\chi_2(h_2)}{\chi_2(h_1)}
\]
where \( \sum_{(\chi_1, \chi_2)} \) extends over all pairs \( (\chi_1, \chi_2) \in \mathbb{X}^{m_1} \times \mathbb{X}^{m_2} \) (recall that we denote by \( \mathbb{X}_f \) the set of all Dirichlet characters modulo \( f \)) and \( \mathbb{X}_{1,2} \) is the Dirichlet character modulo \( \mathbb{X}^{m_1} \mathbb{X}^{m_2} \) that maps \( P \) to \( \chi_1(P) \chi_2(P) \). (see Lemma 2).
We observe that, for $i = 1, 2$,

$$
\sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(h_i) \chi_i(h_i) = \sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(\alpha_i h_i) \chi_i(\alpha_i h_i) = \sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(h_i) \chi_i(\alpha_i) \chi_i(h_i)
\]

$$

$$
= \chi_1(\alpha_i) \sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(h_i) \chi_i(h_i).
\]

Then, considering $c_n$ and $c_n'$ as defined in Section 2.2, we have

$$
w = \frac{1}{\Phi(x_1) \Phi(x_2)} \sum_{(\chi_1, \chi_2), \chi_1 \neq \chi_0} \chi_1(\alpha_1) \chi_2(\alpha_2)
\]

$$
\cdot \sum_{h_1 \in \mathbb{H}_{1-1}} \Lambda(h_1) \chi_1(h_1) \sum_{h_2 \in \mathbb{H}_{2-1}} \Lambda(h_2) \chi_2(h_2) \sum_{P \in \mathbb{P}} \chi_{1,2}(P)
\]

$$
= \frac{1}{\Phi(x_1) \Phi(x_2)} \sum_{(\chi_1, \chi_2), \chi_1 \neq \chi_0} \chi_1(\alpha_1) \chi_2(\alpha_2) c_{l_1-1}(\chi_1) c_{l_2-1}(\chi_2) c_n'(\chi_{1,2}).
\]

Denote by $\chi_0$ the trivial Dirichlet character modulo $x^m$, $i = 1, 2$, and by $\chi_0$ the trivial Dirichlet character modulo $x_1 x_2 x_3$. Observing that $\chi_0 = \chi_0$, we have

$$
w = \frac{1}{\Phi(x_1) \Phi(x_2)} \sum_{(\chi_1, \chi_2) \neq (\chi_0, \chi_0)} c_{l_1-1}(\chi_0) c_{l_2-2}(\chi_0) c_n'(\chi_0)
\]

$$
+ \frac{1}{\Phi(x_1) \Phi(x_2)} \sum_{(\chi_1, \chi_2) \neq (\chi_0, \chi_0)} \chi_1(\alpha_1) \chi_2(\alpha_2) c_{l_1-1}(\chi_1) c_{l_2-1}(\chi_2) c_n'(\chi_{1,2}),
\]

where the sum runs over all the pairs $(\chi_1, \chi_2) \in X_{x_1} \times X_{x_2}$. From Proposition 1 and from the well-known fact that for any positive integer $m$, $\Phi(x_m) = (q - 1)q^{m-1}$, we have

$$
\frac{c_{l_1-1}(\chi_0) c_{l_2-2}(\chi_0) c_n'(\chi_0)}{\Phi(x_1) \Phi(x_2)} = \frac{q^{l_1-m} I_n}{(q - 1)^2},
\]

so

$$
w - \frac{q^{l_1-m} I_n}{(q - 1)^2} = \frac{1}{\Phi(x_1) \Phi(x_2)} \sum_{(\chi_1, \chi_2) \neq (\chi_0, \chi_0)} \chi_1(\alpha_1) \chi_2(\alpha_2) c_{l_1-1}(\chi_1) c_{l_2-1}(\chi_2) c_n'(\chi_{1,2}).
\]

Taking absolute values, applying triangular inequalities, considering the fact that $|\chi_i(\alpha_i)| = 1$, $i = 1, 2$, and using the bounds given in Proposition 1 and the bounds given in (1), we have that

$$
\left| w - \frac{q^{l_1-m} I_n}{(q - 1)^2} \right| \leq \frac{1}{\Phi(x_1) \Phi(x_2)} \sum_{(\chi_1, \chi_2) \neq (\chi_0, \chi_0)} |c_{l_1-1}(\chi_1)||c_{l_2-1}(\chi_2)||c_n'(\chi_{1,2})|
\]

$$
\leq \frac{M}{n} q^{\frac{n+1}{2}}.
\]
where $M = (m_1 + m_2)(m_1 - 1)(m_2 - 1)$. Hence,

$$W > \frac{q^{l-m}n^r}{(q-1)^2} - \frac{M n^{a+2}}{q^r}.$$ 

It is straightforward to show that when (4) holds, the above lower bound is non-negative. □

4. Applications of the main theorem

4.1. A generalization of the Hansen–Mullen conjecture

Theorem 2 gives conditions under which we can prescribe any coefficient of an irreducible polynomial to any value.

**Corollary 3.** Let $n \geq 3$, $m_1, m_2, \ldots, m_r$ be integers such that $n \geq m_1 > \cdots > m_r \geq 1$ and $\beta_1, \ldots, \beta_r \in \mathbb{F}_q$ with $\beta_r \neq 0$ if $m_r = 1$. If

$$m_1 + m_2 + \cdots + m_r \leq n - 2(r + 1) \log_q n - 2 \log_q r - 3r,$$

then there exists a polynomial in $\mathbb{I}_n$ such that the coefficient of $x^{m_i-1}$ is $\beta_i$, $i = 1, \ldots, r$.

**Proof.** Consider Theorem 2 with $\beta_i = \alpha_i$, $m_i = l_i$ if $\beta_i \neq 0$, and $l_i = m_i - 2$ if $\beta_i = 0$. The value of $\alpha_i$ in that latter case is insignificant, so we may as well ignore it. Since $l_i \geq m_i - 2$ for all $i$, we have that $l \geq m - 2r$ and thus $m + 2r \geq 2m - l$. Thus, instead of (3) we may use the sufficient condition $n - 2(r + 1) \log_q n - 2 \log_q r - r \geq m + 2r$, which can be rewritten as $m_1 + \cdots + m_r \leq n - 2(r + 1) \log_q n - 2 \log_q r - 3r$. We observe that the irreducible polynomial whose existence is yielded in the case described above is of the desired form. □

As we mentioned earlier, it follows from [38, Corollary 5.3] and [19] that the Hansen–Mullen conjecture is true, that is, given an element $\alpha$ of $\mathbb{F}_q$ and $n \in \mathbb{N}$, there exists a polynomial in $\mathbb{I}_n$ with any one of its coefficients being $\alpha$. For $r = 1$, Corollary 3 yields something very similar to Wan’s result for the Hansen–Mullen conjecture.

**Corollary 4.** Let $\alpha \in \mathbb{F}_q$ and $m, n$ be positive integers with $n \geq 3$ and $m \leq n$. If \n
$$q^{n-m-6} \geq n^4,$$

then there exists a polynomial in $\mathbb{I}_n$, such that the coefficient of $x^{m-1}$ is $\alpha$.

It is natural to ask if the above can be generalized to more than one prescribed coefficients. Theorem 2 along with Corollary 2 gives an answer to this question; see Fig. 3.

**Corollary 5.** Let $n \geq 3$, $m_1, \ldots, m_r$ be integers such that $n \geq m_1 > \cdots > m_r \geq 1$ and $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_q$, with $\alpha_r \neq 0$ if $m_r = 1$. If

$$m_2 \leq \frac{n}{2r} - \frac{2r + 3}{r} \log_q n - \frac{2}{r} \log_q r - 3$$

or

$$m_{r-1} \geq \frac{2r - 1}{2r} n + \frac{2r + 3}{r} \log_q n + \frac{2}{r} \log_q r + 3,$$

then there exists a polynomial in $\mathbb{I}_n$ with the coefficient of $x^{m_i-1}$ being $\alpha_i$, $i = 1, \ldots, r$. 

Proof. When \( m_2 + (n - m_1 + 1) \leq n/2 - \log_q n \), or equivalently \( m_1 \geq n/2 + m_2 + \log_q n + 1 \), our corollary is a simple case of Corollary 2. We now consider the case \( m_1 \leq n/2 + m_2 + \log_q n \). Since \( m_1 + m_2 + \cdots + m_r \leq m_1 + (r - 1)m_2 \), from (5) the corollary is settled whenever

\[
m_1 \leq n - (r - 1)m_2 - 2(r + 1) \log_q n - 2 \log_q r - 3r.
\]

Thus, our corollary follows when

\[
\frac{n}{2} + m_2 + \log_q n \leq n - (r - 1)m_2 - 2(r + 1) \log_q n - 2 \log_q r - 3r,
\]

or equivalently,

\[
m_2 \leq \frac{n}{(2r)} - (2r + 3)(\log_q n)/r - (2 \log_q r)/r - 3,
\]

which proves the first case. The case

\[
m_{r-1} \geq (2r - 1)n/(2r) + (2r + 3)(\log_q n)/r + (2 \log_q r)/r + 3
\]

is an immediate consequence of Lemma 1. \( \square \)

Corollary 5 shows that, for sufficiently large \( n \) or \( q \), we can prescribe \( r - 1 \) of the roughly \( n/(2r) \) most or least significant coefficients, and another arbitrary one coefficient, of a polynomial in \( \mathbb{I}_n \). We examine some interesting cases, in particular, when \( r = 2, 3 \).

Corollary 6. Let \( n, m_1, m_2 \) be integers such that \( n \geq m_1 > m_2 \geq 1 \) and \( \alpha_1, \alpha_2 \in \mathbb{F}_q \), with \( \alpha_2 \neq 0 \) if \( m_2 = 1 \). If

\[
m_2 \leq \frac{n}{4} - \frac{7}{2} \log_q n - \log_q 2 - 3
\]

or

\[
m_1 \geq \frac{3n}{4} + \frac{7}{2} \log_q n + \log_q 2 + 3,
\]

then there exists a polynomial in \( \mathbb{I}_n \) such that the coefficients of \( x^{m_1 - 1} \) and \( x^{m_2 - 1} \) are \( \alpha_1 \) and \( \alpha_2 \), respectively.

The above corollary yields that, for sufficiently large \( n \) or \( q \), we can prescribe the trace and any other coefficient of a polynomial in \( \mathbb{I}_n \) to any value.
Table 1
Ranges of \( n \) for \( q < 107 \) in Corollary 6.

<table>
<thead>
<tr>
<th>( q )</th>
<th>( n )</th>
<th>( q )</th>
<th>( n )</th>
<th>( q )</th>
<th>( n )</th>
<th>( q )</th>
<th>( n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( \geq 112 )</td>
<td>13</td>
<td>( \geq 32 )</td>
<td>31</td>
<td>( \geq 27 )</td>
<td>59</td>
<td>( \geq 24 )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 69 )</td>
<td>16</td>
<td>( \geq 31 )</td>
<td>32</td>
<td>( \geq 26 )</td>
<td>61</td>
<td>( \geq 24 )</td>
</tr>
<tr>
<td>4</td>
<td>( \geq 55 )</td>
<td>17</td>
<td>( \geq 30 )</td>
<td>37</td>
<td>( \geq 26 )</td>
<td>64</td>
<td>( \geq 24 )</td>
</tr>
<tr>
<td>5</td>
<td>( \geq 48 )</td>
<td>19</td>
<td>( \geq 29 )</td>
<td>41</td>
<td>( \geq 25 )</td>
<td>67</td>
<td>( \geq 24 )</td>
</tr>
<tr>
<td>7</td>
<td>( \geq 40 )</td>
<td>23</td>
<td>( \geq 28 )</td>
<td>43</td>
<td>( \geq 25 )</td>
<td>71</td>
<td>( \geq 23 )</td>
</tr>
<tr>
<td>8</td>
<td>( \geq 38 )</td>
<td>25</td>
<td>( \geq 28 )</td>
<td>47</td>
<td>( \geq 25 )</td>
<td>73</td>
<td>( \geq 23 )</td>
</tr>
<tr>
<td>9</td>
<td>( \geq 37 )</td>
<td>27</td>
<td>( \geq 28 )</td>
<td>49</td>
<td>( \geq 25 )</td>
<td>79</td>
<td>( \geq 23 )</td>
</tr>
<tr>
<td>11</td>
<td>( \geq 34 )</td>
<td>29</td>
<td>( \geq 27 )</td>
<td>53</td>
<td>( \geq 24 )</td>
<td>81</td>
<td>( \geq 23 )</td>
</tr>
</tbody>
</table>

**Corollary 7.** Let \( \alpha, \beta \in \mathbb{F}_q \). Let \( n \) be a positive integer and \( q \) a prime power such that \( n \geq 22 \) and \( q \geq 107 \), or \( q < 107 \) and \( n \) as in Table 1. Then, there exists a monic irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \) with trace \( \alpha \) and any other coefficient being \( \beta \) (with \( \beta \neq 0 \) when this coefficient is the constant one).

**Proof.** Setting \( m_1 = n \) in Corollary 6 yields that a sufficient condition for the existence of the desired polynomials is

\[
    n \geq 14 \log_q n + \log_q 16 + 12. \quad (6)
\]

Therefore, we examine the values of \( q \) and \( n \) which satisfy (6). Equivalently, we set \( f_q(n) = n - 14 \log_q n - \log_q 16 - 12 \) and we search for the values \( q \) and \( n \) for which \( f_q(n) \geq 0 \). One can find that \( f_q(n) \) is increasing when

\[
    n \geq \frac{14 \ln q}{\ln q}. \quad (7)
\]

We only consider degrees \( n \geq 3 \); since \( 14 / \ln 107 < 3 \), we conclude that for all \( q \geq 107 \), \( f_q(n) \) is increasing. Furthermore, we check that \( f_{107}(22) \geq 0 \) and thus \( f_{107}(n) \geq 0 \) for all \( n \geq 22 \). Lastly, \( f_q(n) \geq f_q'(n) \) if and only if \( q = q' \); we conclude that if \( n \geq 22 \) and \( q \geq 107 \), then \( f_q(n) \geq 0 \).

Finally, for the cases when \( q < 107 \), we compute the single zero of \( f_q(n) \) numerically and conclude that for \( n \) greater or equal to the zero, \( f_q(n) \geq 0 \). Those cases of \( q \), with the corresponding ranges of \( n \), are shown in Table 1.

For the case of three prescribed coefficients, Corollary 5 gives the following.

**Corollary 8.** Let \( n \geq 3 \), \( m_1, m_2, m_3 \) be integers such that \( n \geq m_1 > m_2 > m_3 \geq 1 \), and \( \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q \), with \( \alpha_3 \neq 0 \) if \( m_3 = 1 \). If

\[
    m_2 \leq \frac{n}{6} - 3 \log_q n - \frac{2}{3} \log_q 3 - 3
\]

or

\[
    m_2 \geq \frac{5n}{6} + 3 \log_q n + \frac{2}{3} \log_q 3 + 3,
\]

then there exists a polynomial in \( \mathbb{F}_n \) such that the coefficients of \( x^{m_1-1}, x^{m_2-1} \), and \( x^{m_3-1} \) are \( \alpha_1, \alpha_2, \) and \( \alpha_3 \), respectively.

In that case, considering traces and subtraces with prescribed coefficients, the previous corollary gives the following result.
Table 2
Ranges of \( n \) for \( q < 91 \) in Corollary 9.

<table>
<thead>
<tr>
<th>( q )</th>
<th>( n )</th>
<th>( q )</th>
<th>( n )</th>
<th>( q )</th>
<th>( n )</th>
<th>( q )</th>
<th>( n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( \geq 156 )</td>
<td>3</td>
<td>( \geq 47 )</td>
<td>4</td>
<td>( \geq 78 )</td>
<td>5</td>
<td>( \geq 68 )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 97 )</td>
<td>4</td>
<td>( \geq 45 )</td>
<td>6</td>
<td>( \geq 58 )</td>
<td>7</td>
<td>( \geq 55 )</td>
</tr>
<tr>
<td>4</td>
<td>( \geq 78 )</td>
<td>7</td>
<td>( \geq 41 )</td>
<td>8</td>
<td>( \geq 53 )</td>
<td>9</td>
<td>( \geq 50 )</td>
</tr>
<tr>
<td>5</td>
<td>( \geq 68 )</td>
<td>8</td>
<td>( \geq 43 )</td>
<td>10</td>
<td>( \geq 50 )</td>
<td>11</td>
<td>( \geq 48 )</td>
</tr>
<tr>
<td>6</td>
<td>( \geq 58 )</td>
<td>9</td>
<td>( \geq 44 )</td>
<td>12</td>
<td>( \geq 48 )</td>
<td>13</td>
<td>( \geq 46 )</td>
</tr>
<tr>
<td>7</td>
<td>( \geq 55 )</td>
<td>10</td>
<td>( \geq 47 )</td>
<td>14</td>
<td>( \geq 44 )</td>
<td>15</td>
<td>( \geq 44 )</td>
</tr>
<tr>
<td>8</td>
<td>( \geq 53 )</td>
<td>11</td>
<td>( \geq 49 )</td>
<td>16</td>
<td>( \geq 43 )</td>
<td>17</td>
<td>( \geq 43 )</td>
</tr>
<tr>
<td>9</td>
<td>( \geq 50 )</td>
<td>12</td>
<td>( \geq 51 )</td>
<td>18</td>
<td>( \geq 41 )</td>
<td>19</td>
<td>( \geq 41 )</td>
</tr>
</tbody>
</table>

Fig. 4. The graphical representation of Corollary 10.

**Corollary 9.** Let \( \alpha, \beta, \gamma \in \mathbb{F}_q \). Let \( n \) be a positive integer and \( q \) a prime power such that \( n \geq 33 \) and \( q \geq 91 \), or \( q < 91 \) and \( n \) as in Table 2. Then, there exists a monic irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \) with trace \( \alpha \), subtrace \( \beta \), and any other coefficient being \( \gamma \) (with \( \gamma \neq 0 \) when this coefficient is the constant one).

**Proof.** Setting \( m_1 = n \), \( m_2 = n - 1 \) in Corollary 8 yields that a sufficient condition for the existence of the desired polynomials is \( n \geq 18 \log_q n + 4 \log_q 3 + 18 \). Applying the arguments that we used in the proof of Corollary 7 for the above inequality completes the proof. \( \square \)

4.2. Irreducible polynomials with consecutive zero coefficients

In this section we use Theorem 2 to examine the existence of irreducible polynomials with prescribed coefficients of forms that cannot be obtained from the existing results presented so far. More specifically, we examine the existence of irreducible polynomials with sequences of coefficients prescribed to zero. Focusing on that question, we present the following simpler version of Theorem 2; see Fig. 4.

**Corollary 10.** Let \( n \geq 3, m_1, \ldots, m_r, l_1, \ldots, l_r \) be integers such that \( n \geq m_1 > l_1 \geq m_2 > l_2 \geq \cdots \geq m_r > l_r \geq 1 \). Set \( m = \sum_{i=1}^r m_i, l = \sum_{i=1}^r l_i \). If

\[
 n - 2(r + 1) \log_q n - 2\log_q r - r \geq 2m - l, 
\]

then there exists an irreducible polynomial of the form \( x^n + \sum_{i=0}^{n-1} a_i x^i, a_i \in \mathbb{F}_q \) such that \( a_j = 0 \) for all \( m_i > j \geq l_i, 1 \leq i \leq r \).

It follows from Corollary 2 that we can prescribe roughly half the least or most significant coefficients to zero (see Fig. 1), and from [16] that we can prescribe roughly one third of any coefficients to zero. The following corollary considers irreducible polynomials with a sequence of consecutive zero coefficients and fixed trace; see Fig. 5.

**Corollary 11.** Let \( \alpha \in \mathbb{F}_q \) and \( c \) be a real number such that \( 0 < c < 1/4 \). Then there exist an integer \( n \) and a polynomial in \( \mathbb{I}_n \) with trace \( \alpha \) and a sequence of \( \lfloor cn \rfloor \) consecutive zero coefficients.

**Proof.** Considering Lemma 1, we can equivalently prove that there exist an integer \( n \) and a polynomial in \( \mathbb{I}_n \) with the coefficient of \( x \) being \( \alpha \) and a sequence of \( \lfloor cn \rfloor \) consecutive zero coefficients.
Let $n$ be a positive integer, and consider Theorem 2 with $r = 2$, $m_2 = l_2 = 2$, $\alpha_1 = \alpha$ and set $m_1 - l_1 = \lfloor cn \rfloor$. When $2 + (n - l_1 + 1) \leq n/2 - \log_q n$, or equivalently $l_1 \geq n/2 + \log_q n + 3$, our corollary follows from Corollary 2. Now, let

$$l_1 \leq n/2 + \log_q n + 2.$$  \hfill (8)

From (3), our corollary follows whenever

$$n - 6 \log_q n - 2 \log_q 2 - 2 \geq 2m - l.$$  

We observe that $2m - l \leq m + cn = m_1 + cn + 2$, hence a sufficient condition is given by

$$n - 6 \log_q n - 2 \log_q 2 - 2 \geq m_1 + cn + 2,$$

or equivalently

$$m_1 \leq n(1 - c) - 6 \log_q n - 2 \log_q 2 - 4.$$

Because $m_1 \leq l_1 + cn$, we also have the sufficient condition

$$l_1 + cn \leq n(1 - c) - 6 \log_q n - 2 \log_q 2 - 4,$$

or equivalently,

$$l_1 \leq (1 - 2c)n - 6 \log_q n - 2 \log_q 2 - 4.$$  \hfill (9)

When (9) holds, then there exists an irreducible polynomial of the desired form. From (8) and (9), we have that the corollary follows whenever

$$\frac{n}{2} + \log_q n + 2 \leq (1 - 2c)n - 6 \log_q n - 2 \log_q 2 - 4.$$

or equivalently,

$$\left(\frac{1}{2} - 2c\right)n \geq 7 \log_q n + 2 \log_q 2 + 6.$$  \hfill (10)

Since $0 < c < 1/4$, then $(1/2 - 2c) > 0$. We observe that $n$ can be chosen sufficiently large so that (10) holds. That completes the proof of the corollary. \hfill \square

Corollary 11 shows that, for any $\varepsilon > 0$ and large enough $q$ or $n$, there exist irreducible polynomials of degree $n$ with up to $\lfloor (1/4 - \varepsilon)n \rfloor$ consecutive coefficients fixed to zero and its trace fixed to any element. For instance, setting $c = 1/5$ in Corollary 11 yields the following corollary.
Corollary 12. Let $q$ be a prime power and $n$ a positive integer. Let $\alpha \in \mathbb{F}_q$. If $n \geq 70 \log_q n + 20 \log_q 2 + 60$ then there exists a monic irreducible polynomial of degree $n$ over $\mathbb{F}_q$ with any $\lfloor n/5 \rfloor$ consecutive coefficients fixed to zero and its trace fixed to $\alpha$.

5. Conclusion

In this paper we consider the existence of irreducible polynomials with prescribed coefficients. The main results are presented in Section 4 and include a generalization of the Hansen–Mullen conjecture and the asymptotical existence of irreducible polynomials with trace and any other one coefficients prescribed to any value.

It would be interesting to improve these results; it is natural to ask if the restrictions that appear in (3) of Theorem 2 can be weakened. Any improvement to this restriction will reflect accordingly to all the results of Section 4.

Another particularly interesting improvement would be to show results similar to Corollaries 7 and 9, but not restricting one of the prescribed coefficients to be the trace; that would show that a generalization of the Hansen–Mullen conjecture holds asymptotically.

We thank the anonymous referee for correcting an error in the statement of Lemma 1 in the first version of the paper.

References