Finite Fields and Their Applications 18 (2012) 303–315

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

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 INFO

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

ABSTRACT

Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. We examine the existence of irreducible polynomials with prescribed coefficients over $\mathbb{F}_q$. We focus on a conjecture by Hansen and Mullen which states that for $n \geqslant 3$, there exist irreducible polynomials over $\mathbb{F}_q$ of degree n, with any *one* coefficient prescribed to any element of $\mathbb{F}_q$ (this being nonzero when the constant coefficient is being prescribed) and was proved by Wan. We introduce a variation of Wan's method to give restrictions subject to which this result can be extended to more than one prescribed coefficient; for example we show the asymptotical existence of irreducible polynomials with trace and any other one coefficient prescribed to any value. It also follows from our generalization the existence of irreducible polynomials with sequences of consecutive zero coefficients.

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 $\mathbb{I}_n$ the set of monic irreducible polynomials in $\mathbb{A}$ with degree n and $I_n = |\mathbb{I}_n|$. It is well known that

$$\frac{q^n}{n} - \frac{2q^{\frac{n}{2}}}{n} \leqslant I_n \leqslant \frac{q^n}{n} - \frac{q}{n} \tag{1}$$

(for instance, see [27]). However much less is known about the number or the existence of polynomials of $\mathbb{I}_n$ 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.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.09.003

Let m, n be integers with $1 \leqslant m \leqslant n$, $\alpha \in \mathbb{F}_q$ and suppose there exists an irreducible polynomial P of degree n over $\mathbb{F}_q$ with the coefficient of x^m being α. We say that *we prescribe the coefficient of x^m of P to α*. 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 χ of the multiplicative group $(\mathbb{A}/f\mathbb{A})^*$. A *Dirichlet character* modulo f is an extension of χ 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 χ 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. $\chi(a) = 0 \Leftrightarrow (a, f) \neq 1$.

It follows that $|\chi(a)| = 1$ when $\chi(a) \neq 0$. The Dirichlet character χ_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 χ modulo f there is associated the *conjugate* character $\overline{\chi}$ defined by $\overline{\chi}(a) = \overline{\chi(a)}$ 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 $\mathcal{X} : \mathbb{A} \longrightarrow \mathbb{C}^*$ such that $\mathcal{X}(h) = \prod_{i=1}^{r} \chi_i(h)$ 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

$$c_n(\chi) = \sum_{d|n} \sum_{P \in \mathbb{I}_d} d\chi\left(P^{\frac{n}{d}}\right) \quad \text{and} \quad c'_n(\chi) = \sum_{P \in \mathbb{I}_n} \chi(P).$$

We define $\mathbb{H}_n$ 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

$$c_n(\chi) = \sum_{h \in \mathbb{H}_n} \Lambda(h)\chi(h),$$

where Λ is an analogue of the von Mangolt function in $\mathbb{A}$ that we define as

$$\Lambda(h) = \begin{cases} \deg P & \text{if } h = aP^e, \text{ some irreducible } P \in \mathbb{A},\ a \in \mathbb{F}_q^*, \text{ and } e \in \mathbb{Z}_{\geqslant 0}, \\ 0 & \text{otherwise.} \end{cases}$$

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

$$\left|c_n(\chi)\right| \leqslant \left(\deg(f) - 1\right)q^{\frac{n}{2}} \quad \textit{and} \quad \left|c'_n(\chi)\right| \leqslant \frac{\deg(f)}{n} q^{\frac{n}{2}}.$$

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

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].

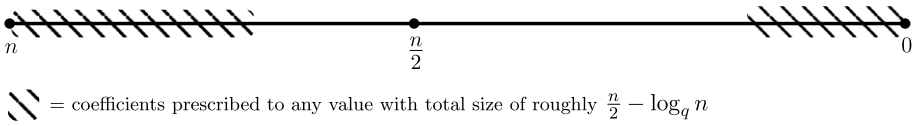

Fig. 1. The graphical representation of Corollary 2.

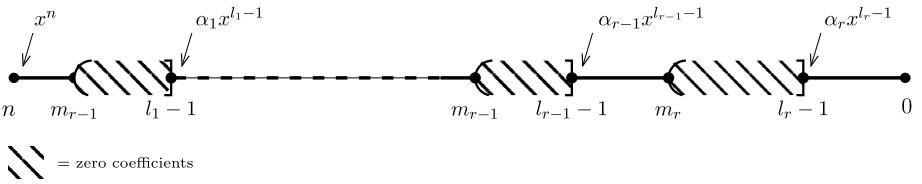

Fig. 2. The graphical representation of Theorem 2.

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*

$$\left|\pi(n; f, g) - \frac{q^n}{n\Phi(f)}\right| \leqslant \frac{1}{n}\big(\deg(f) + 1\big)q^{\frac{n}{2}}. \tag{2}$$

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 $m \leqslant n/2 - \log_q n$, 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 $1 \leqslant k, m \leqslant n$ and $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_m \in \mathbb{F}_q$. If $k + m \leqslant \frac{n}{2} - \log_q n$, 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 $n > m \geqslant 0$, 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 $n \geqslant 3$, $m_1, \ldots, m_r, l_1, \ldots, l_r$ be integers such that $n \geqslant m_1 \geqslant l_1 > m_2 \geqslant l_2 > \cdots > m_r \geqslant l_r \geqslant 1$ 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*

$$n - 2(r+1)\log_q n - 2\log_q r - r \geqslant 2m - l, \tag{3}$$

then there exists an irreducible polynomial 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 $m_i > j \geqslant l_i$, $1 \leqslant i \leqslant r$, 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 $n \geqslant 3$, m_1, m_2, l_1, l_2 be integers such that $n \geqslant m_1 \geqslant l_1 > m_2 \geqslant l_2 \geqslant 1$ and $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$ with $\alpha_2 \neq 0$ if $l_2 = 1$. Set $m = m_1 + m_2$, $l = l_1 + l_2$. If*

$$n - 6\log_q n - 2\log_q 2 - 2 \geqslant 2m - l, \tag{4}$$

then there exists a polynomial in $\mathbb{I}_n$ 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 $m_i > j \geqslant l_i$, $i = 1, 2$, and $a_j = \alpha_j$ for $j = l_1 - 1, l_2 - 1$.

Proof. Let

$$w = w(n, m_1, m_2, \alpha_1, \alpha_2) = \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1 - 1}} \Lambda(h_1) \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2 - 1}} \Lambda(h_2) \sum_P 1,$$

where the last sum expands over all $P \in \mathbb{I}_n$ such that $P \equiv h_i \pmod{x^{m_i}}$, $i = 1, 2$. We note that such a P is of the desired form, and the sums $\sum_{h_i \in \alpha_i \mathbb{H}_{l_i - 1}} \Lambda(h_i)$ 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

$$\begin{aligned} w = & \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1 - 1}} \Lambda(h_1) \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2 - 1}} \Lambda(h_2) \\ & \cdot \sum_{P \in \mathbb{I}_n} \left(\frac{1}{\Phi(x^{m_1})} \sum_{\chi_1} \chi_1(P) \overline{\chi_1(h_1)} \right) \left(\frac{1}{\Phi(x^{m_2})} \sum_{\chi_2} \chi_2(P) \overline{\chi_2(h_2)} \right) \\ = & \frac{1}{\Phi(x^{m_1})} \frac{1}{\Phi(x^{m_2})} \sum_{(\chi_1, \chi_2)} \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1 - 1}} \Lambda(h_1) \overline{\chi_1(h_1)} \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2 - 1}} \Lambda(h_2) \overline{\chi_2(h_2)} \sum_{P \in \mathbb{I}_n} \mathcal{X}_{1,2}(P) \end{aligned}$$

where $\sum_{(\chi_1, \chi_2)}$ extends over all pairs $(\chi_1, \chi_2) \in X_{x^{m_1}} \times X_{x^{m_2}}$ (recall that we denote by X_f the set of all Dirichlet characters modulo f) and $\mathcal{X}_{1,2}$ is the Dirichlet character modulo $x^{m_1} x^{m_2}$ that maps P to $\chi_1(P)\chi_2(P)$ (see Lemma 2).

We observe that, for $i = 1, 2$,

$$\sum_{h_i \in \alpha_i \mathbb{H}_{l_i-1}} \Lambda(h_i)\overline{\chi_i(h_i)} = \sum_{h_i \in \mathbb{H}_{l_i-1}} \Lambda(\alpha_i h_i)\overline{\chi_i(\alpha_i h_i)} = \sum_{h_i \in \mathbb{H}_{l_i-1}} \Lambda(h_i)\overline{\chi_i(\alpha_i)}\,\overline{\chi_i(h_i)}$$
$$= \overline{\chi_i(\alpha_i)} \sum_{h_i \in \mathbb{H}_{l_i-1}} \Lambda(h_i)\overline{\chi_i(h_i)}.$$

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

$$w = \frac{1}{\Phi(x^{m_1})\Phi(x^{m_2})} \sum_{(\chi_1,\chi_2)} \overline{\chi_1(\alpha_1)}\,\overline{\chi_2(\alpha_2)}$$
$$\cdot \sum_{h_1 \in \mathbb{H}_{l_1-1}} \Lambda(h_1)\overline{\chi_1(h_1)} \sum_{h_2 \in \mathbb{H}_{l_2-1}} \Lambda(h_2)\overline{\chi_2(h_2)} \sum_{P \in \mathbb{I}_n} \mathcal{X}_{1,2}(P)$$
$$= \frac{1}{\Phi(x^{m_1})\Phi(x^{m_2})} \sum_{(\chi_1,\chi_2)} \overline{\chi_1(\alpha_1)}\,\overline{\chi_2(\alpha_2)} c_{l_1-1}(\overline{\chi_1}) c_{l_2-1}(\overline{\chi_2}) c'_n(\mathcal{X}_{1,2}).$$

Denote by χ_{0i} the trivial Dirichlet character modulo x^{m_i}, $i = 1, 2$, and by $\mathcal{X}_0$ the trivial Dirichlet character modulo $x^{m_1}x^{m_2}$. Observing that $\overline{\chi_{0i}} = \chi_{0i}$, we have

$$w = \frac{1}{\Phi(x^{m_1})\Phi(x^{m_2})} c_{l_1-1}(\chi_{01}) c_{l_2-1}(\chi_{02}) c'_n(\mathcal{X}_0)$$
$$+ \frac{1}{\Phi(x^{m_1})\Phi(x^{m_2})} \sum_{\substack{(\chi_1,\chi_2) \\ \neq(\chi_{01},\chi_{02})}} \overline{\chi_1(\alpha_1)}\,\overline{\chi_2(\alpha_2)} c_{l_1-1}(\overline{\chi_1}) c_{l_2-1}(\overline{\chi_2}) c'_n(\mathcal{X}_{1,2}),$$

where the sum runs over all the pairs $(\chi_1, \chi_2) \in X_{m_1} \times X_{m_2}$ with $(\chi_1, \chi_2) \neq (\chi_{01}, \chi_{02})$. 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

$$\frac{c_{l_1-1}(\chi_{01}) c_{l_2-2}(\chi_{02}) c'_n(\mathcal{X}_0)}{\Phi(x^{m_1})\Phi(x^{m_2})} = \frac{q^{l-m} I_n}{(q-1)^2},$$

so

$$w - \frac{q^{l-m} I_n}{(q-1)^2} = \frac{1}{\Phi(x^{m_1})\Phi(x^{m_2})} \sum_{\substack{(\chi_1,\chi_2) \\ \neq(\chi_{01},\chi_{02})}} \overline{\chi_1(\alpha_1)}\,\overline{\chi_2(\alpha_2)} c_{l_1-1}(\overline{\chi_1}) c_{l_2-1}(\overline{\chi_2}) c'_n(\mathcal{X}_{1,2}).$$

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

$$\left| w - \frac{q^{l-m} I_n}{(q-1)^2} \right| \leqslant \frac{1}{\Phi(x^{m_1})\Phi(x^{m_2})} \sum_{\substack{(\chi_1,\chi_2) \\ \neq(\chi_{01},\chi_{02})}} \left|c_{l_1-1}(\overline{\chi_1})\right| \left|c_{l_2-1}(\overline{\chi_2})\right| \left|c'_n(\mathcal{X}_{1,2})\right|$$
$$\leqslant \frac{M}{n} q^{\frac{n+l-2}{2}},$$

where $M = (m_1 + m_2)(m_1 - 1)(m_2 - 1)$. Hence,

$$w > \frac{q^{l-m} I_n}{(q-1)^2} - \frac{M}{n} q^{\frac{n+l-2}{2}}.$$

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

$$m_1 + m_2 + \cdots + m_r \leqslant n - 2(r+1)\log_q n - 2\log_q r - 3r, \tag{5}$$

then there exists a polynomial in $\mathbb{I}_n$ such that the coefficient of $x^{m_i - 1}$ is β_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 α_i in that latter case is insignificant, so we may as well ignore it. Since $l_i \geqslant m_i - 2$ for all i, we have that $l \geqslant m - 2r$ and thus $m + 2r \geqslant 2m - l$. Thus, instead of (3) we may use the sufficient condition $n - 2(r+1)\log_q n - 2\log_q r - r \geqslant m + 2r$, which can be rewritten as $m_1 + \cdots + m_r \leqslant n - 2(r+1)\log_q n - 2\log_q r - 3r$. 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 α of $\mathbb{F}_q$ and $n \in \mathbb{N}$, there exists a polynomial in $\mathbb{I}_n$ with any *one* of its coefficients being α. 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 $n \geqslant 3$ and $m \leqslant n$. If*

$$q^{n-m-6} \geqslant n^4,$$

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

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

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

or

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

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

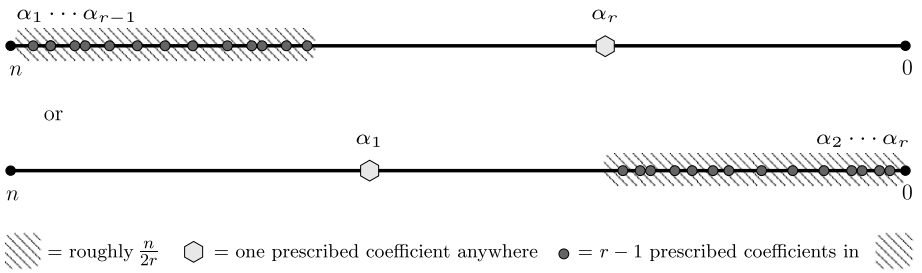

Fig. 3. The graphical representation of Corollary 5.

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

$$m_1\leqslant n-(r-1)m_2-2(r+1)\log_q n-2\log_q r-3r.$$

Thus, our corollary follows when

$$\frac{n}{2}+m_2+\log_q n\leqslant n-(r-1)m_2-2(r+1)\log_q n-2\log_q r-3r,$$

or equivalently,

$$m_2\leqslant n/(2r)-(2r+3)(\log_q n)/r-(2\log_q r)/r-3,$$

which proves the first case. The case

$$m_{r-1}\geqslant(2r-1)n/(2r)+(2r+3)(\log_q n)/r+(2\log_q r)/r+3$$

is an immediate consequence of Lemma 1. □

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 $n\geqslant m_1>m_2\geqslant 1$ and $\alpha_1,\alpha_2\in\mathbb{F}_q$, with $\alpha_2\neq 0$ if $m_2=1$. If*

$$m_2\leqslant\frac{n}{4}-\frac{7}{2}\log_q n-\log_q 2-3$$

or

$$m_1\geqslant\frac{3n}{4}+\frac{7}{2}\log_q n+\log_q 2+3,$$

then there exists a polynomial in $\mathbb{I}_n$ such that the coefficients of x^{m_1-1} and x^{m_2-1} are α_1 and α_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.

q	n	q	n	q	n	q	n	q	n
2	$\geqslant 112$	13	$\geqslant 32$	31	$\geqslant 27$	59	$\geqslant 24$	83	$\geqslant 23$
3	$\geqslant 69$	16	$\geqslant 31$	32	$\geqslant 26$	61	$\geqslant 24$	89	$\geqslant 23$
4	$\geqslant 55$	17	$\geqslant 30$	37	$\geqslant 26$	64	$\geqslant 24$	97	$\geqslant 23$
5	$\geqslant 48$	19	$\geqslant 29$	41	$\geqslant 25$	67	$\geqslant 24$	101	$\geqslant 22$
7	$\geqslant 40$	23	$\geqslant 28$	43	$\geqslant 25$	71	$\geqslant 23$	103	$\geqslant 22$
8	$\geqslant 38$	25	$\geqslant 28$	47	$\geqslant 25$	73	$\geqslant 23$		
9	$\geqslant 37$	27	$\geqslant 28$	49	$\geqslant 25$	79	$\geqslant 23$		
11	$\geqslant 34$	29	$\geqslant 27$	53	$\geqslant 24$	81	$\geqslant 23$		

Corollary 7. *Let $\alpha, \beta \in \mathbb{F}_q$. Let n be a positive integer and q a prime power such that $n \geqslant 22$ and $q \geqslant 107$, 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 α and any other coefficient being β (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

$$n \geqslant 14 \log_q n + \log_q 16 + 12. \tag{6}$$

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 $f_q(n) \geqslant 0$. One can find that $f_q(n)$ is increasing when

$$n \geqslant \frac{14}{\ln q}. \tag{7}$$

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

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

$$m_2 \leqslant \frac{n}{6} - 3 \log_q n - \frac{2}{3} \log_q 3 - 3$$

or

$$m_2 \geqslant \frac{5n}{6} + 3 \log_q n + \frac{2}{3} \log_q 3 + 3,$$

then there exists a polynomial in $\mathbb{I}_n$ such that the coefficients of x^{m_1-1}, x^{m_2-1}, and x^{m_3-1} are α_1, α_2, and α_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.

q	n	q	n	q	n	q	n	q	n
2	$\geqslant 156$	13	$\geqslant 47$	31	$\geqslant 39$	59	$\geqslant 35$	83	$\geqslant 34$
3	$\geqslant 97$	16	$\geqslant 45$	32	$\geqslant 39$	61	$\geqslant 35$	89	$\geqslant 34$
4	$\geqslant 78$	17	$\geqslant 44$	37	$\geqslant 38$	64	$\geqslant 35$		
5	$\geqslant 68$	19	$\geqslant 43$	41	$\geqslant 37$	67	$\geqslant 35$		
7	$\geqslant 58$	23	$\geqslant 41$	43	$\geqslant 37$	71	$\geqslant 34$		
8	$\geqslant 55$	25	$\geqslant 40$	47	$\geqslant 36$	73	$\geqslant 34$		
9	$\geqslant 53$	27	$\geqslant 40$	49	$\geqslant 36$	79	$\geqslant 34$		
11	$\geqslant 50$	29	$\geqslant 39$	53	$\geqslant 36$	81	$\geqslant 34$		

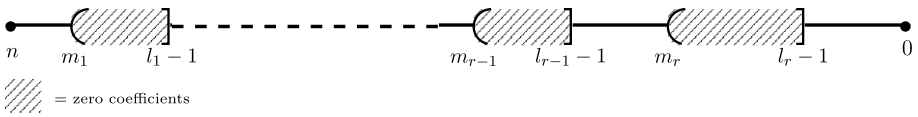

Fig. 4. The graphical representation of Corollary 10.

Corollary 9. *Let $\alpha, \beta, \gamma \in \mathbb{F}_q$. Let n be a positive integer and q a prime power such that $n \geqslant 33$ and $q \geqslant 91$, 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 α, subtrace β, and any other coefficient being γ (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 $n \geqslant 18 \log_q n + 4 \log_q 3 + 18$. Applying the arguments that we used in the proof of Corollary 7 for the above inequality completes the proof. □

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

$$n - 2(r+1)\log_q n - 2\log_q r - r \geqslant 2m - l,$$

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 $m_i > j \geqslant l_i$, $1 \leqslant i \leqslant r$.

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 α 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 α and a sequence of $\lfloor cn \rfloor$ consecutive zero coefficients.

Fig. 5. The graphical representation of Corollary 11.

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 $2 + (n - l_1 + 1) \leqslant n/2 - \log_q n$, or equivalently $l_1 \geqslant n/2 + \log_q n + 3$, our corollary follows from Corollary 2. Now, let

$$l_1 \leqslant n/2 + \log_q n + 2. \tag{8}$$

From (3), our corollary follows whenever

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

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

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

or equivalently

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

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

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

or equivalently,

$$l_1 \leqslant (1 - 2c)n - 6\log_q n - 2\log_q 2 - 4. \tag{9}$$

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

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

or equivalently,

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

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. □

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 $n \geqslant 70 \log_q n + 20 \log_q 2 + 60$ 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 α.*

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

[1] O. Ahmadi, On the distribution of irreducible trinomials over $\mathbb{F}_3$, Finite Fields Appl. 13 (2007) 659–664.
[2] R. Brent, P. Zimmerman, Ten new primitive binary trinomials, Math. Comp. 78 (2009) 1197–1199.
[3] M. Car, Distribution des polynomes irreductibles dans $\mathbb{F}_q[t]$, Acta Arith. 88 (1999) 141–153.
[4] L. Carlitz, A theorem of Dickson on irreducible polynomials, Proc. Amer. Math. Soc. 3 (1952) 693–700.
[5] K. Cattell, C.R. Miers, F. Ruskey, J. Sawada, M. Serra, The number of irreducible polynomials over $GF(2)$ with given trace and subtrace, J. Combin. Math. Combin. Comput. 47 (2003) 31–64.
[6] S.D. Cohen, The distribution of polynomials over finite fields, Acta Arith. 17 (1970) 255–271.
[7] S.D. Cohen, Explicit theorems on generator polynomials, Finite Fields Appl. 11 (3) (2005) 337–357.
[8] S.D. Cohen, Primitive polynomials with a prescribed coefficient, Finite Fields Appl. 12 (3) (2006) 425–491.
[9] S.D. Cohen, D. Hachenberger, Primitive normal bases with prescribed traces, Appl. Algebra Engrg. Comm. Comput. 9 (1999) 383–403.
[10] S.D. Cohen, D. Hachenberger, Primitivity, freeness, norm and trace, Discrete Math. 214 (2000) 135–144.
[11] D. Coppersmith, Fast evaluation of logarithms in fields of characteristic two, IEEE Trans. Inform. Theory 30 (4) (1984) 587–594.
[12] S.Q. Fan, Primitive normal polynomials with the last half coefficients prescribed, Finite Fields Appl. 15 (2009) 604–614.
[13] S.Q. Fan, W.B. Han, p-Adic formal series and Cohen's problem, Glasg. Math. J. 46 (2004) 47–61.
[14] S.Q. Fan, W.B. Han, Primitive polynomials over finite fields of characteristic two, Appl. Algebra Engrg. Comm. Comput. 14 (2004) 381–395.
[15] R.W. Fitzgerald, J.L. Yucas, Irreducible polynomials over $GF(2)$ with three prescribed coefficients, Finite Fields Appl. 9 (2003) 286–299.
[16] T. Garefalakis, Irreducible polynomials with consecutive zero coefficients, Finite Fields Appl. 14 (1) (2008) 201–208.
[17] J. von zur Gathen, Irreducible trinomials over finite fields, Math. Comp. 72 (2003) 1987–2000.
[18] A. Hales, D. Newhart, Swan's theorem for binary tetranomials, Finite Fields Appl. 12 (2006) 301–311.
[19] K.H. Ham, G.L. Mullen, Distribution of irreducible polynomials of small degrees over finite fields, Math. Comp. 67 (221) (1998) 337–341.
[20] T. Hansen, G.L. Mullen, Primitive polynomials over finite fields, Math. Comp. 59 (1992) 639–643.
[21] B. Hanson, D. Panario, D. Thomson, Swan-like results for binomials and trinomials over finite fields of odd characteristic, Des. Codes Cryptogr. (2011) 1–11, doi:10.1007/s10623-010-9476-7.
[22] C.N. Hsu, The distribution of irreducible polynomials in $\mathbb{F}_q[t]$, J. Number Theory 61 (1) (1996) 85–96.
[23] R. Kim, W. Koepf, The parity of the number of irreducible factors for some pentanomials, Finite Fields Appl. 15 (2009) 585–603.
[24] K. Kononen, M. Moisio, M. Rinta-aho, K. Väänänen, Irreducible polynomials with prescribed trace and restricted norm, JP J. Algebra Number Theory Appl. 11 (2009) 223–248.
[25] E.N. Kuz'min, A class of irreducible polynomials over a finite field, Dokl. Akadad. Nauk SSSR 313 (1990) 552–555 (in Russian).
[26] E.N. Kuz'min, Irreducible polynomials over a finite field and an analogue of Gauss sums over a field of characteristic 2, Sibirsk. Mat. Zh. 32 (1991) 100–108 (in Russian).
[27] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, 1983.
[28] P. Loidreau, On the factorization of trinomials over $\mathbb{F}_3$, INRIA Rapport de Recherche 3918, 2000.
[29] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, Acta Arith. 132 (2008) 329–350.

[30] B. Omidi Koma, D. Panario, Q. Wang, The number of irreducible polynomials of degree n over $\mathbb{F}_q$ with given trace and constant terms, Discrete Math. 310 (2010) 1282–1292.
[31] D. Panario, D. Thomson, Efficient p-th root computations in finite fields of characteristic p, Des. Codes Cryptogr. 50 (3) (2009) 351–358.
[32] R. Ree, Proof of a conjecture of S. Chowla, J. Number Theory 1 (61) (1971) 210–212.
[33] M. Rosen, Number Theory in Function Fields, Grad. Texts in Math., vol. 210, 2002.
[34] I.E. Shparlinski, Coefficients of primitive polynomials, Mat. Zametki 38 (1985) 810–815, 956 (in Russian).
[35] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Verh. 1 Internat. Math. Kongresses (1897) 182–193.
[36] R. Swan, Factorization of polynomials over finite fields, Pacific J. Math. 12 (1962) 1099–1106.
[37] G. Tzanakis, On the existence of irreducible polynomials with prescribed coefficients over finite fields, Master's thesis, Carleton University, 2010, http://www.math.carleton.ca/~gtzanaki/mscthesis.pdf.
[38] D. Wan, Generators and irreducible polynomials over finite fields, Math. Comp. 66 (219) (1997) 1195–1212.