# IRREDUCIBLE POLYNOMIALS WITH SEVERAL PRESCRIBED COEFFICIENTS

PAUL POLLACK

*In memory of David Hayes*

Abstract. We study the number of monic irreducible polynomials of degree $n$ over $\mathbf{F}_q$ having certain preassigned coefficients, where we assume that the constant term (if preassigned) is nonzero. Hansen and Mullen conjectured that for $n \geq 3$, one can always find an irreducible polynomial with any one coefficient preassigned (regardless of the ground field $\mathbf{F}_q$). Their conjecture was established in all but finitely many cases by Wan, and later resolved in full in work of Ham and Mullen. In this note, we present a new, explicit estimate for the number of irreducibles with several preassigned coefficients. One consequence is that for any $\epsilon > 0$, and all $n \geq n_0(\epsilon)$, one can find a degree $n$ monic irreducible with any $\lfloor (1-\epsilon)\sqrt{n} \rfloor$ coefficients preassigned (uniformly in the choice of ground field $\mathbf{F}_q$). For the proof, we adapt work of Kátai and Harman on rational primes with preassigned digits.

## 1. Introduction

Since the time of Gauss, we have known that there are roughly $q^n/n$ monic irreducible polynomials $P$ of degree $n$ over the finite field $\mathbf{F}_q$. Writing

$$P = T^n + \sum_{i=0}^{n-1} a_i T^i, \tag{1}$$

it is natural to wonder what can be said about the coefficient sequences $(a_0, a_1, \dots, a_{n-1})$ that correspond to these irreducibles. A great deal of work has gone into studying questions of this nature; what we know, as well as what still remains mysterious, is surveyed in [GHP99], [Shp99, Chapter 3], and [Coh05, §2].

One of the success stories in this area concerns the following conjecture of Hansen and Mullen [HM92, Conjecture B]: *Given any $n \geq 3$, any $0 \leq i < n$, and any $a \in \mathbf{F}_q$, one can find an irreducible polynomial $P$ of the form* (1) *with $a_i = a$, where we assume $a \neq 0$ in the case $i = 0$.* This conjecture was proved by Wan [Wan97] when either $n \geq 36$ or $q > 19$; the (finitely many) remaining cases were disposed of soon after by Ham and Mullen [HM98].

It is natural to ask for generalizations of the Hansen–Mullen conjecture where more than one coefficient is allowed to be preassigned. Panario and Tzanakis [PT12] (see also [Tza10]) have shown that Wan's method can sometimes be applied in this situation. For example, they prove that if $n \geq 22$ and $q \geq 107$, then one can arbitrarily prescribe both $a_{n-1}$ and any other $a_i$ (subject to $a_0 \neq 0$ if $i = 0$); moreover, if $n \geq 112$, then the same result holds with no restriction on $q$. However, their method will not give a similar result for two arbitrary coefficients $a_i$ and $a_j$.

1991 *Mathematics Subject Classification.* Primary: 11T55, Secondary: 11T23.

*Key words and phrases.* Hansen–Mullen conjecture, prescribed coefficients, exponential sums.

For each prime power $q$ and each natural number $n$, we let $\pi_q(n)$ denote the number of monic irreducible polynomials of degree $n$ over $\mathbf{F}_q$. Our main objective in this note is to establish the following theorem:

**Theorem 1.** *Let $n \geq 2$. Let $\mathcal{I}$ be a nonempty subset of $\{0, 1, 2, \dots, n-1\}$, and put $I = \#\mathcal{I}$. Choose an element $a_i \in \mathbf{F}_q$ for each $i \in \mathcal{I}$, with $a_0 \neq 0$ if $0 \in \mathcal{I}$. Let $\mathscr{S}$ be the set of monic, degree $n$ polynomials where the coefficient of $T^i$ is $a_i$, for all $i \in \mathcal{I}$. Then*

$$\left|\left(\sum_{\substack{P \in \mathscr{S} \\ P \text{ irreducible}}} 1\right) - \mathfrak{S} \cdot \pi_q(n)\right| \leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + q^{n-1-\lfloor \frac{n}{I+1} \rfloor}, \tag{2}$$

*where $\mathfrak{S} = q^{-I}$ if $0 \notin \mathcal{I}$, and $\mathfrak{S} = (q-1)^{-1} q^{-(I-1)}$ if $0 \in \mathcal{I}$.*

*Example* (irreducibles with two preassigned coefficients). Let us consider what Theorem 1 has to say about the problem of preassigning two arbitrary coefficients; in other words, we look at the special case of Theorem 1 when $I = \#\mathcal{I} = 2$.

- (Asymptotics) Theorem 1 supplies us with a main term and an error term for the number of irreducible elements of $\mathscr{S}$. We temporarily ignore the the explicit inequalities and think in terms of the big picture. Since $\mathfrak{S}$ has order $q^{-2}$ and $\pi_q(n)$ has order $q^n/n$ (see, e.g., Lemma 4 below), the main term has order $q^{n-2}/n$; on the other hand, the error bound has order $q^{n-\frac{1}{2}\lfloor\frac{n}{2}\rfloor}$. So the relative error is bounded by an expression of order $n \cdot q^{2-\frac{1}{2}\lfloor\frac{n}{2}\rfloor}$. Now putting $X := q^n$, we see that once $n \geq 10$,
$$n \cdot q^{2-\frac{1}{2}\lfloor\frac{n}{2}\rfloor} \leq n \cdot q^{(9-n)/4} = \frac{\log X}{\log q} \cdot X^{\frac{9-n}{4n}} \leq \frac{\log X}{\log 2} \cdot X^{-1/40}.$$
So the relative error tends to zero as $X = q^n \to \infty$, within the regime $n \geq 10$.
- (Existence results) We now take advantage of the explicit nature of the inequality (2). Fix $n \geq 10$. For prime powers $q$ satisfying
$$q^{-2}\pi_q(n) > q^{n-\frac{1}{2}\lfloor\frac{n}{2}\rfloor} + q^{n-1-\lfloor\frac{n}{3}\rfloor},$$
the estimate (2) yields
$$\sum_{\substack{P \in \mathscr{S} \\ P \text{ irreducible}}} 1 > 0,$$
and thus there is a monic, degree $n$ irreducible with any two coefficients arbitrarily preassigned. For example, if $n = 10$, a calculation in Maple shows that $q \geq 101$ is sufficient. Moreover, once $n \geq 30$, the lower bound implicit in (2) for the number of irreducibles in $\mathscr{S}$ is always positive, regardless of $q$.

Similar considerations apply with any fixed number of preassigned coefficients.

In fact, it is not necessary to fix the number of prescribed coefficients to obtain an asymptotic result from Theorem 1.

**Corollary 2.** *Adopt the notation and assumptions of Theorem 1. Let $\epsilon > 0$. Then we have the uniform asymptotic estimate*

$$\sum_{\substack{P \in \mathscr{S} \\ P \text{ irreducible}}} 1 \sim \mathfrak{S} \cdot \pi_q(n) \qquad (\text{as } n \to \infty),$$

*as long as the number of prescribed coefficients $I$ satisfies $I \leq (1-\epsilon)\sqrt{n}$.*

It should be emphasized that the asymptotic result asserted in Corollary 2 holds whenever $n \to \infty$, *uniformly in* $q$. In particular, we can arbitrarily prescribe $\lfloor (1-\epsilon)\sqrt{n} \rfloor$ coefficients whenever $n > n_0(\epsilon)$ (over any ground field $\mathbf{F}_q$).

As the above examples illustrate, the method of this paper only gives results once $n$ is sufficiently large. When $n$ is fixed, an alternative method of Cohen, depending on the function field analogue of the Chebotarev density theorem, can often be applied. See [Coh72, Theorem 1] and [Coh99].

The proofs of Theorem 1 and Corollary 2 are given in §3, after a brief discussion in §2 of preparatory results. Our strategy for proving Theorem 1 is substantially different from that used by Wan and earlier authors. We adapt a method developed by Harman and Kátai to study rational primes with preassigned digits [Kát86, Har06, HK08] (cf. work of Wolke [Wol05]). The proof makes essential use of an exponential sum estimate obtained by Hayes [Hay66] in his investigations into the additive number theory of irreducible polynomials.

**Notation and definitions.** We need a number of definitions, most of which will be familiar to function field aficionados. Below, $\mathbf{F}_q(T)_\infty$ denotes the completion of $\mathbf{F}_q(T)$ at the prime associated to the $(1/T)$-adic valuation, and we identify $\mathbf{F}_q(T)_\infty$ with the field $\mathbf{F}_q((1/T))$ of finite-tailed Laurent series in $1/T$. We use $|\cdot|$ for the induced absolute value on $\mathbf{F}_q(T)_\infty$, so that $|0| = 0$ and $\left|\sum_{i=-\infty}^{n} a_i T^i\right| = q^n$ if $a_n \neq 0$. We define the *unit interval* $\mathscr{U}$ by

$$\mathscr{U} := \left\{ \sum_{i<0} a_i T^i : a_i \in \mathbf{F}_q \right\}.$$

If $A = \sum_i a_i T^i \in \mathbf{F}_q(T)_\infty$, we define its *fractional part*, denoted $\{A\}$, as the element $\sum_{i<0} a_i T^i \in \mathscr{U}$. We use $\psi(\cdot)$ for the additive character on $\mathbf{F}_q$ defined by

$$\psi(a) = \exp\left(\frac{2\pi \mathrm{i}}{p}\mathrm{Tr}(a)\right),$$

where the trace is taken from $\mathbf{F}_q$ down to its prime field $\mathbf{F}_p$. We write $\mathbf{e}\colon \mathbf{F}_q(T)_\infty \to S^1$ for the map defined by

$$\mathbf{e}\left(\sum_{i=-\infty}^{n} a_i T^i\right) = \psi(a_{-1}).$$

In all that follows, the letter $P$ is reserved for monic irreducible elements of $\mathbf{F}_q[T]$. If $A \in \mathbf{F}_q[T]$, we write $\phi(A) = \#(\mathbf{F}_q[T]/(A))^\times$ for the size of the unit group mod $A$. We set $\mu(A) = 0$ if $P^2 \mid A$ for some $P$; otherwise, we put $\mu(A) = (-1)^k$, where $k$ is the number of distinct monic primes dividing $A$.

In order to keep track of explicit constants, we adopt the nonstandard convention that $U = \Theta(V)$ means $|U| \leq V$.

## 2. Preliminaries

2.1. **An exponential sum estimate.** The following lemma of Hayes [Hay66, Theorem 4.3] is an analogue of a well-known result of Dirichlet in the theory of Diophantine approximation.

**Lemma 3.** *For each* $\theta \in \mathscr{U}$*, there is a unique pair of coprime polynomials* $G, H \in \mathbf{F}_q[T]$ *with* $H$ *monic,* $\deg G < \deg H \leq n/2$*, and*

$$\left|\theta - \frac{G}{H}\right| < \frac{1}{q^{\deg H + \frac{n}{2}}}.$$

It will also be convenient for us to have a reasonably sharp form of Gauss's prime number theorem for polynomials.

**Lemma 4.** *For each prime power $q$ and each natural number $n$, we have*

$$\frac{q^n}{n} - 2\frac{q^{n/2}}{n} \leq \pi_q(n) \leq \frac{q^n}{n}. \tag{3}$$

*Also,*

$$\pi_q(n) \geq \frac{1}{2}\frac{q^n}{n}. \tag{4}$$

*Proof (sketch).* The lower and upper bounds for $\pi_q(n)$ in (3) are well-known. See, e.g., [LN97, Exercises 3.26 and 3.27, p. 142] for slightly stronger results. The lower bound in (3) immediately implies (4) for $q^n \geq 16$. Since $\pi_q(1) = q$, the estimate (4) also holds whenever $n = 1$. This leaves only the pairs $(q, n) \in \{(2, 2), (2, 3), (3, 2)\}$ to check, which can be done directly. □

We now introduce the function field analogue of the usual exponential sum over primes. For each $\theta \in \mathscr{U}$, let

$$f(\theta) := \sum_{\deg P = n} \mathbf{e}(\theta P),$$

where the sum is over the monic irreducible polynomials $P$ of degree $n$. The following fundamental estimate is due to Hayes and relies in a crucial way on Weil's analogue of the Riemann Hypothesis.

**Lemma 5.** *Given $\theta \in \mathscr{U}$, choose $G$ and $H$ as in Lemma 3. If $|\theta - G/H| < 1/q^n$, then*

$$\left| f(\theta) - \frac{\mu(H)}{\phi(H)}\mathbf{e}\left(T^n(\theta - G/H)\right) \cdot \pi_q(n) \right| \leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor}. \tag{5}$$

*Otherwise,*

$$|f(\theta)| \leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor}. \tag{6}$$

*Proof (sketch).* This follows from a careful reading of the proofs of [Hay66, Theorem 5.3 and Lemma 7.1]. Indeed, in our notation, [Hay66, eq. (5.14)] asserts that the left-hand sides of (5) and (6) are bounded above by

$$q^{n/2} \cdot (q^{n - \lfloor n/2 \rfloor - \deg H}\phi(H))^{1/2}.$$

To complete the proof of the lemma, we observe that $\phi(H) \leq |H| = q^{\deg H}$. □

2.2. **Further preliminaries.** We note the following consequence of Lemma 5.

**Lemma 6.** *Let $n \geq 2$. Let $\mathscr{J}$ be a nonempty subset of $\{0, 1, 2, \dots, n-1\}$, and suppose that $\theta \in \mathscr{U}$ has the form $\theta = \sum_{j \in \mathscr{J}} c_j T^{-j-1}$, where each $c_j$ is a nonzero element of $\mathbf{F}_q$. Choose $G$ and $H$ as described in Lemma 3. Then*

$$|f(\theta)| \leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + q^{n - \deg H}. \tag{7}$$

*Proof.* We can assume that $H$ is squarefree and that $|\theta - G/H| < q^{-n}$; otherwise, Lemma 5 shows that (7) holds even with its second right-hand summand omitted. Appealing now to (5), we see that

$$\begin{aligned} |f(\theta)| &\leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + \frac{\pi_q(n)}{\phi(H)} \\ &\leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + \frac{q^n}{n \cdot \phi(H)}, \end{aligned} \tag{8}$$

using in the second line the upper bound of Lemma 4.

Put $h := \deg H$. Then $h \geq 1$; otherwise, $G = 0$ and $H = 1$, and the inequality $|\theta - G/H| < q^{-n}$ contradicts the assumptions on $\theta$. If $H$ is not irreducible, then every monic irreducible polynomial of degree $h$ over $\mathbf{F}_q$ reduces to a unit modulo $H$, and distinct monic irreducibles reduce to distinct elements mod $H$. So $\phi(H) \geq \pi_q(h) \geq \frac{1}{2}q^h/h$, by (4). This final lower bound on $\phi(H)$ also holds when $H$ is irreducible, since in that case $\phi(H) = q^h - 1 \geq \frac{1}{2}q^h$. So in either case,

$$\frac{q^n}{n \cdot \phi(H)} \leq \frac{2h}{n} q^{n-h} \leq q^{n-h},$$

using in the final step that $h \leq n/2$. Inserting this upper bound into (8) yields (7). □

The following estimate will play a starring role in our proof of Theorem 1:

**Lemma 7.** *Let $n \geq 2$. Let $\mathscr{J}$ be a subset of $\{0, 1, 2, \dots, n-1\}$, and suppose that $\theta \in \mathscr{U}$ has the form $\theta = \sum_{j \in \mathscr{J}} c_j T^{-j-1}$, where each $c_j$ is a nonzero element of $\mathbf{F}_q$. Suppose also that $\theta$ is* not *of the form $c/T$ for any $c \in \mathbf{F}_q$. Then with $J := \#\mathscr{J}$, we have*

$$|f(\theta)| \leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + q^{n-1-\lfloor \frac{n}{J+1} \rfloor}.$$

*Proof.* Choose $G$ and $H$ as in Lemma 3. As in the proof of Lemma 6, we may assume that $H$ is squarefree and that $|G/H - \theta| < q^{-n}$. By Lemma 6, it is enough to show that $h := \deg H$ satisfies $h \geq 1 + \lfloor \frac{n}{J+1} \rfloor$; in other words, it suffices to prove that

$$h > \frac{n}{J+1}. \qquad (9)$$

Write $H = T^e H'$, where $T \nmid H'$. Since $H$ is squarefree, we must have $e = 0$ or $e = 1$. We must also have $H'$ nonconstant: Otherwise, $G/H = c/T$ for some (possibly vanishing) constant $c \in \mathbf{F}_q$. But then $|G/H - \theta| < 1/q^n$ forces $\theta = c/T$, contrary to hypothesis.

We claim that in the Laurent expansion of $G/H$, there is no string of $h$ consecutive vanishing coefficients. Otherwise, $|\{T^r G/H\}| < q^{-h}$ for some exponent $r \geq 0$. But for every $r$, we have $|\{T^r G/H\}| \geq |H|^{-1} = q^{-h}$. (We use here that $H'$ is a nonconstant divisor of $H$ coprime to both $T$ and $G$, so that $H$ cannot divide $T^r G$.) We deduce that at least $\lfloor n/h \rfloor$ of the coefficients of $T^{-1}, T^{-2}, \dots, T^{-n}$ in the Laurent expansion of $G/H$ are nonzero. Since $|G/H - \theta| < q^{-n}$, the corresponding coefficients in the expansion of $\theta$ are also nonvanishing. But by definition, $\theta$ has exactly $J$ nonvanishing coefficients. So $J \geq \lfloor n/h \rfloor > n/h - 1$, yielding (9). □

Our final lemma allows us to convert the problem of counting irreducible polynomials with preassigned coefficients to one of estimating exponential sums.

**Lemma 8.** *If $A = \sum_i a_i T^i \in \mathbf{F}_q(T)_\infty$, $j \in \mathbf{Z}$, and $a \in \mathbf{F}_q$, we set $\chi(A; j, a) = 1$ if $a = a_j$ and $\chi(A; j, a) = 0$ otherwise. Then*

$$\chi(A; j, a) = \frac{1}{q} \sum_{c \in \mathbf{F}_q} \mathbf{e}(cT^{-j-1} \cdot A) \cdot \psi(-ac).$$

*Proof.* Expanding out the definitions, we find that

$$\sum_{c \in \mathbf{F}_q} \mathbf{e}(cT^{-j-1} \cdot A) \cdot \psi(-ac) = \sum_{c \in \mathbf{F}_q} \psi(c(a_j - a)).$$

As $c$ ranges over $\mathbf{F}_q$, the functions $a \mapsto \psi(ca)$ range over the additive characters of $\mathbf{F}_q$ (see [LN97, Theorem 5.7, p. 190]). The lemma now follows from the familiar orthogonality relations (e.g., see [LN97, p. 189]). □

## 3. Proofs of the main results

*Proof of Theorem 1.* By Lemma 8, we have

$$\begin{aligned}\sum_{P\in\mathscr{S}} 1 &= \sum_{\deg P=n}\prod_{i\in\mathcal{I}}\chi(P;i,a_i)\\ &= q^{-I}\sum_{\deg P=n}\prod_{i\in\mathcal{I}}\left(\sum_{c_i\in\mathbf{F}_q}\mathbf{e}(c_iT^{-i-1}\cdot P)\cdot\psi(-a_ic_i)\right)\\ &= q^{-I}\sum_{\{c_i\}_{i\in\mathcal{I}}}\left(\prod_{i\in\mathcal{I}}\psi(-a_ic_i)\right)\sum_{\deg P=n}\mathbf{e}\left(\left(\sum_{i\in\mathcal{I}}c_iT^{-i-1}\right)P\right); \qquad (10)\end{aligned}$$

in (10), the outermost sum is over all tuples $\{c_i\}_{i\in\mathcal{I}}$ with each $c_i\in\mathbf{F}_q$.

Suppose first that $0\notin\mathcal{I}$, so that we are not prescribing the constant term. The tuple $\{c_i\}=\mathbf{0}$ makes a contribution to (10) of exactly

$$q^{-I}\pi_q(n).$$

For all of the remaining tuples $\{c_i\}$, the innermost sum in (10) can be estimated by applying Lemma 7 with

$$\theta := \sum_{i\in\mathcal{I}}c_iT^{-i-1}. \qquad (11)$$

We find that each of these $q^I-1$ remaining tuples makes a contribution to (10) of

$$\Theta\left(q^{-I}\left(q^{n-\frac{1}{2}\lfloor\frac{n}{2}\rfloor}+q^{n-1-\lfloor\frac{n}{I+1}\rfloor}\right)\right). \qquad (12)$$

Putting this together with our estimate when $\{c_i\}=\mathbf{0}$ gives

$$\sum_{P\in\mathscr{S}}1 = q^{-I}\pi_q(n)+\Theta\left(q^{n-\frac{1}{2}\lfloor\frac{n}{2}\rfloor}+q^{n-1-\lfloor\frac{n}{I+1}\rfloor}\right),$$

which is the claim of Theorem 1 in this case.

In the case when $0\in\mathcal{I}$, we partition the tuples $\{c_i\}_{i\in\mathcal{I}}$ into two classes: In the first class, we put the $q$ tuples having $c_i=0$ for all $i\in\mathcal{I}\setminus\{0\}$. In the second class, we put the remaining $q^I-q$ tuples. The contribution to (10) of the tuples in the first class is described by the double sum

$$q^{-I}\sum_{c_0\in\mathbf{F}_q}\psi(-a_0c_0)\sum_{\deg P=n}\mathbf{e}\left(c_0T^{-1}\cdot P\right). \qquad (13)$$

When $c_0=0$, the inner sum in (13) is precisely $\pi_q(n)$. For $c_0\neq 0$, Lemma 5 (taking $G=c_0$ and $H=T$) shows that the inner sum may be estimated as

$$\sum_{\deg P=n}\mathbf{e}\left(c_0T^{-1}\cdot P\right) = -\frac{1}{q-1}\pi_q(n)+\Theta(q^{n-\frac{1}{2}\lfloor\frac{n}{2}\rfloor}).$$

Substituting these estimates into (13), we find that

$$\begin{aligned} q^{-I} \sum_{c_0 \in \mathbf{F}_q} \psi(-a_0 c_0) &\sum_{\deg P = n} \mathbf{e}\left(c_0 T^{-1} \cdot P\right) \\ &= q^{-I} \cdot \pi_q(n) \left( 1 - \frac{1}{q-1} \sum_{\substack{c_0 \in \mathbf{F}_q \\ c_0 \neq 0}} \psi(-a_0 c_0) \right) + \Theta(q^{-I} \cdot (q-1) \cdot q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor}) \\ &= q^{-I} \cdot \pi_q(n) \left( \frac{q}{q-1} - \frac{1}{q-1} \sum_{c_0 \in \mathbf{F}_q} \psi(-a_0 c_0) \right) + \Theta(q^{-I} \cdot q \cdot q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor}). \end{aligned}$$

We are assuming that $a_0 \neq 0$, and so the orthogonality relations imply that the remaining sum over $c_0$ vanishes. Hence, the contribution of the tuples in the first class simplifies to

$$q^{-(I-1)}(q-1)^{-1} \cdot \pi_q(n) + \Theta(q^{-I} \cdot q \cdot q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor}).$$

For each of the $q^I - q$ tuples in the second class, Lemma 7 can be applied with $\theta$ given by (11), and each tuple makes a contribution to (10) of size (12). Putting everything together, we obtain for $\sum_{P \in \mathscr{S}} 1$ the main term predicted by Theorem 1, with an error term that is

$$\Theta(q^{-I} \cdot q \cdot q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor}) + \Theta\left(q^{-I} \cdot (q^I - q) \cdot \left(q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + q^{n-1-\lfloor \frac{n}{I+1} \rfloor}\right)\right) = \\ \Theta\left(q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + q^{n-1-\lfloor \frac{n}{I+1} \rfloor}\right),$$

which also agrees with Theorem 1. □

*Proof of Corollary 2.* Theorem 1 gives us a main term for $\sum_{P \in \mathscr{S}} 1$ of order $q^{n-I}/n$, and an error bound of $q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + q^{n-1-\lfloor \frac{n}{I+1} \rfloor}$. So the relative error is bounded, in order of magnitude, by $n \cdot q^{I - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + n \cdot q^{I-1-\lfloor \frac{n}{I+1} \rfloor}$. Since we are assuming that $I \leq (1-\epsilon)\sqrt{n}$, we find that for large $n$,

$$n \cdot q^{I - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + n \cdot q^{I-1-\lfloor \frac{n}{I+1} \rfloor} \leq n \cdot q^{\sqrt{n} - \frac{n}{4}} + n \cdot q^{-\epsilon\sqrt{n}} \leq n \cdot 2^{\sqrt{n} - \frac{n}{4}} + n \cdot 2^{-\epsilon\sqrt{n}}.$$

The final expression tends to 0 as $n \to \infty$, and the corollary follows. □

## 4. Concluding remarks

4.1. **An alternative error bound.** We take this opportunity to record that Theorem 1 remains true with its conclusion (2) replaced by

$$\left| \left( \sum_{\substack{P \in \mathscr{S} \\ P \text{ irreducible}}} 1 \right) - \mathfrak{S} \cdot \pi_q(n) \right| \leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + q^{n-1-\min \mathcal{I}}. \tag{14}$$

When all of the elements of $\mathcal{I}$ are large, this bound is more useful than (2), in the sense that it gives nontrivial estimates for $\sum_{P \in \mathscr{S}} 1$ for larger values of $\#\mathcal{I}$. The proof of (14) is exactly the same as that given for Theorem 1, except that everywhere Lemma 7 was used, we substitute the following result:

**Lemma 9.** *Let $n \geq 2$. Let $\mathscr{J}$ be a nonempty subset of $\{0, 1, 2, \ldots, n-1\}$, and suppose that $\theta \in \mathscr{U}$ has the form $\theta = \sum_{j \in \mathscr{J}} c_j T^{-j-1}$, where each $c_j$ is a nonzero element of $\mathbf{F}_q$. Then*

$$|f(\theta)| \leq q^{n - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} + q^{n-1-\min \mathscr{J}}. \tag{15}$$

*Proof of Lemma 9.* Choose $G$ and $H$ as in Lemma 3. As in the proof of Lemma 6, we may assume that $H$ is squarefree and that $|\theta - G/H| < q^{-n}$. We have $|\theta| = q^{-1-\min \mathscr{J}} \geq q^{-n}$; thus, $|G/H| = |\theta|$ by the ultrametric triangle inequality. This forces $\deg H \geq 1 + \min \mathscr{J}$. The estimate (15) now follows from Lemma 6. □

4.2. **Prescribing consecutive coefficients.** It has long been known that for the problem of prescribing the first and last several coefficients, one can do much better than what is guaranteed by Theorem 1. The next proposition is a consequence of work of Hayes together with Weil's Riemann Hypothesis (compare with [Hay65, Theorem 1.3]). For more refined results, see the papers of Rhin [Rhi72, Chapter 2], Hsu [Hsu96], and Car [Car99].

**Proposition 10.** *Fix $\epsilon > 0$, and assume that $n > n_0(\epsilon)$. Let $s$ and $t$ be nonnegative integers with $s + t \leq (\frac{1}{2} - \epsilon)n$. For all all prime powers $q$, there is a degree $n$ monic irreducible over $\mathbf{F}_q$ with the coefficient of $T^i$ arbitrarily prescribed for all $i \in [0, s) \cup [n-t, n)$. We assume that the constant term, if prescribed, is nonzero.*

So in some sense, it is the middle coefficients that present the most difficulty. In this direction, Garefalakis [Gar08] has shown that for $n > n_0(\epsilon)$, there is a monic, degree $n$ irreducible with *any* $\lfloor (\frac{1}{3} - \epsilon)n \rfloor$ consecutive coefficients set to zero (excluding, of course, the $T^n$-coefficient and the constant term).

The method of this note permits us to arbitrarily prescribe any $\lfloor (\frac{1}{4} - \epsilon)n \rfloor$ consecutive coefficients, again for $n > n_0(\epsilon)$. (We exclude the $T^n$-coefficient from this statement and assume that the constant term, if prescribed, is nonzero.) Indeed, let $\mathcal{I} \subset [0, n)$ be a set of $\lfloor (\frac{1}{4} - \epsilon)n \rfloor$ consecutive integers. If $\min \mathcal{I} < \frac{1}{4}n$ and $n$ is sufficiently large, we can prescribe the coefficient of $T^i$ for all $i \in \mathcal{I}$ by Proposition 10. On the other hand, when $\min \mathcal{I} \geq \frac{1}{4}n$, the same conclusion follows from (14).

## References

[Car99] M. Car, *Distribution des polynômes irréductibles dans $\mathbf{F}_q[T]$*, Acta Arith. **88** (1999), 141–153.

[Coh72] S. D. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. (2) **6** (1972), 93–102.

[Coh99] ______, *Some function field estimates with applications*, Number theory and its applications (Ankara, 1996), Lecture Notes in Pure and Appl. Math., vol. 204, Dekker, New York, 1999, pp. 23–45.

[Coh05] ______, *Explicit theorems on generator polynomials*, Finite Fields Appl. **11** (2005), 337–357.

[Gar08] T. Garefalakis, *Irreducible polynomials with consecutive zero coefficients*, Finite Fields Appl. **14** (2008), 201–208.

[GHP99] S. Gao, J. Howell, and D. Panario, *Irreducible polynomials of given forms*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997), Contemp. Math., vol. 225, Amer. Math. Soc., Providence, RI, 1999, pp. 43–54.

[Har06] G. Harman, *Primes with preassigned digits*, Acta Arith. **125** (2006), 179–185.

[Hay65] D. R. Hayes, *The distribution of irreducibles in* GF$[q, x]$, Trans. Amer. Math. Soc. **117** (1965), 101–127.

[Hay66] ______, *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. **11** (1966), 461–488.

[HK08] G. Harman and I. Kátai, *Primes with preassigned digits. II*, Acta Arith. **133** (2008), 171–184.

[HM92] T. Hansen and G. L. Mullen, *Primitive polynomials over finite fields*, Math. Comp. **59** (1992), 639–643, S47–S50.

[HM98] K. H. Ham and G. L. Mullen, *Distribution of irreducible polynomials of small degrees over finite fields*, Math. Comp. **67** (1998), 337–341.

[Hsu96] C.-N. Hsu, *The distribution of irreducible polynomials in* $\mathbf{F}_q[t]$, J. Number Theory **61** (1996), 85–96.

[Kát86] I. Kátai, *Distribution of digits of primes in q-ary canonical form*, Acta Math. Hungar. **47** (1986), 341–359.

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[PT12] D. Panario and G. Tzanakis, *A generalization of the Hansen-Mullen conjecture on irreducible polynomials over finite fields*, Finite Fields Appl. **18** (2012), 303–315.

[Rhi72] G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Math. **95** (1972), 75 pages.

[Shp99] I. E. Shparlinski, *Finite fields: theory and computation*, Mathematics and its Applications, vol. 477, Kluwer Academic Publishers, Dordrecht, 1999.

[Tza10] G. Tzanakis, *On the existence of irreducible polynomials with prescribed coefficients over finite fields*, Master's thesis, Carleton University, 2010.

[Wan97] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comp. **66** (1997), 1195–1212.

[Wol05] D. Wolke, *Primes with preassigned digits*, Acta Arith. **119** (2005), 201–209.

University of Georgia, Department of Mathematics, Athens, Georgia 30602, USA
*E-mail address*: `pollack@uga.edu`