Finite Fields and Their Applications 22 (2013) 70–78

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Irreducible polynomials with several prescribed coefficients

Paul Pollack *

University of Georgia, Department of Mathematics, Athens, GA 30602, USA

ARTICLE INFO

Article history:
Received 19 November 2012
Revised 11 February 2013
Accepted 1 March 2013
Available online 22 March 2013
Communicated by Stephen D. Cohen

MSC:
11T55
11T23

Keywords:
Hansen–Mullen conjecture
Prescribed coefficients
Exponential sums

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 $n \geqslant 3$, 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 large enough n depending on ϵ, 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 $(a_0, a_1, \ldots, a_{n-1})$ that correspond to these irreducibles. A great deal of work has gone into studying questions of this

* Fax: +1 (706) 542 5907.
E-mail address: pollack@math.uga.edu.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.03.001

nature; what we know, as well as what still remains mysterious, is surveyed in [1], [2, Chapter 3], and [3, §2].

One of the success stories in this area concerns the following conjecture of Hansen and Mullen [4, Conjecture B]: *Given any $n \geqslant 3$, any $0 \leqslant i < n$, 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 [5] when either $n \geqslant 36$ or $q > 19$; the (finitely many) remaining cases were disposed of soon after by Ham and Mullen [6].

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 [7] (see also [8]) have shown that Wan's method can sometimes be applied in this situation. For example, they prove that if $n \geqslant 22$ and $q \geqslant 107$, 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 $n \geqslant 112$, 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.

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 $n \geqslant 2$. Let $\mathcal{I}$ be a nonempty subset of $\{0, 1, 2, \ldots, n-1\}$, 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*

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

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 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 $n \geqslant 10$,

$$n \cdot q^{2 - \frac{1}{2}\lfloor \frac{n}{2} \rfloor} \leqslant n \cdot q^{(9-n)/4} = \frac{\log X}{\log q} \cdot X^{\frac{9-n}{4n}} \leqslant \frac{\log X}{\log 2} \cdot X^{-1/40}.$$

  So the relative error tends to zero as $X = q^n \to \infty$, within the regime $n \geqslant 10$.
- (Existence results) We now take advantage of the explicit nature of the inequality (2). Fix $n \geqslant 10$. 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

$$\sum_{\substack{P \in \mathscr{S} \\ P \text{ irreducible}}} 1 > 0,$$