Finite Fields and Their Applications 40 (2016) 10–25

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Irreducible polynomials with several prescribed coefficients

Junsoo Ha

ARTICLE INFO

Article history:
Received 18 July 2015
Received in revised form 18 February 2016
Accepted 24 February 2016
Available online 15 March 2016
Communicated by Stephen D. Cohen

MSC:
primary 11T55
secondary 11T23, 11T06

Keywords:
Hansen–Mullen conjecture
Prescribed coefficients
Exponential sums

ABSTRACT

We study the number of irreducible polynomials over $\mathbf{F}_q$ with some coefficients prescribed. Using the technique developed by Bourgain, we show that there is an irreducible polynomial of degree n with r coefficients prescribed in any location when $r \leq [(1/4-\epsilon)\,n]$ for any $\epsilon > 0$ and q is large; and when $r \leq \delta n$ for some $\delta > 0$ and for any q. The result improves earlier work of Pollack stating that a similar result holds for $r \leq [(1-\epsilon)\sqrt{n}]$.

1. Introduction and statement of result

The problem of finding irreducible polynomials with certain properties has been studied by numerous authors. One of the interesting problems among them is the existence of an irreducible polynomial with certain coefficients being prescribed.

The early form of this problem is as follows. Let $\mathbf{F}_q$ be the finite field of q elements and n be a given integer, and write a polynomial $P = \sum_{k \leq n} x_k T^k$. Then we ask if we can

E-mail address: junsoo.ha.31@gmail.com.

http://dx.doi.org/10.1016/j.ffa.2016.02.006
1071-5797/© 2016 Elsevier Inc. All rights reserved.

find an irreducible for any given pair of integers j, n and $a \in \mathbf{F}_q$ satisfying $x_j = a$, except when $a = 0$ and $j = 0$. This problem, widely known as the Hansen–Mullen conjecture, see [1], has been settled by Wan [2] when $n \geq 36$ or $q > 19$; the remaining cases were verified by Ham and Mullen [3].

One may ask if we can find an irreducible with several preassigned coefficients. In other words, we study the number of irreducible polynomials of degree n satisfying $x_i = a_i$ for all $i \in \mathcal{I}$, when the index set $\mathcal{I} \subset \{0, 1, \dots, n-1\}$ and a finite sequence $a_i \in \mathbf{F}_q$ for $i \in \mathcal{I}$ are given. Unless we assume that the location of prescribed coefficients has certain properties, the best known uniform bound is due to Pollack [4], who proved that when n is large, there is an irreducible polynomial with $\lfloor (1-\epsilon)\sqrt{n} \rfloor$ prescribed coefficients.

The analogue of the Hansen–Mullen conjecture in number theory is to find rational primes with prescribed (binary) digits. Recently, Bourgain [5] showed that for some $\delta > 0$ and for large n, there is a prime of n digits with δn digits prescribed without any restriction on their position. Thus it is believed that an analogous improvement holds for polynomials in finite fields.

In this paper, we show that we can prescribe a positive proportion of coefficients. The result presented here is the combination of several known ideas. The underlying setup in this type of problems is the circle method over $\mathbf{F}_q[T]$, which can be found in Hayes [6]. A recent application of this method, among others, can be found in Liu and Wooley [7] on Waring's problem. The work of Pollack [4] is also implicitly based on this method.

The main element of this paper is the combination of Pollack's estimate and the interpretation of the result of Bourgain [5] in finite fields, though it is greatly simplified thanks to the Weil bound, i.e., the analogue of the Riemann Hypothesis for irreducible polynomials.

Our main theorem is as follows.

Theorem 1.1. *Let $\mathcal{I}$ be a nonempty subset of $\{0, \dots, n-1\}$ and choose $a_i \in \mathbf{F}_q$ for each $i \in \mathcal{I}$. We write as $\mathscr{S}$ the set of monic degree n polynomials with T^i coefficient given by a_i for each $i \in \mathcal{I}$. Then if $\rho := |\mathcal{I}|/n \leq 1/4$,*

$$\left(\sum_{\substack{P \in \mathscr{S} \\ P \text{ is irreducible}}} 1 \right) = \frac{\mathfrak{S} q^{n-|\mathcal{I}|}}{n} \left(1 + O\left(\frac{\log_q\left(\frac{1}{\rho}\right) + 1}{q^{1/\rho - 4/(\rho+1)}} \right) \right) + O\left(q^{3n/4}\right), \tag{1}$$

where the implied constants are absolute, and

$$\mathfrak{S} = \begin{cases} 1 & 0 \notin \mathcal{I} \\ 1 + \frac{1}{q-1} & 0 \in \mathcal{I} \text{ and } a_0 \neq 0 \\ 0 & 0 \in \mathcal{I} \text{ and } a_0 = 0. \end{cases} \tag{2}$$