Finite Fields and Their Applications 53 (2018) 36–63

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Tuples of polynomials over finite fields with pairwise coprimality conditions

Juan Arias De Reyna [a], Randell Heyman [b,*]

[a] Department of Mathematical Analysis, Seville University, Seville, Spain
[b] School of Mathematics and Statistics, University of New South Wales, Sydney, Australia

ARTICLE INFO

Article history:
Received 11 July 2017
Received in revised form 11 May 2018
Accepted 29 May 2018
Available online xxxx
Communicated by Xiang-dong Hou

MSC:
11C08

Keywords:
Relatively prime
Coprime
Polynomials
Finite fields
Dedekind domains

ABSTRACT

Let q be a prime power. We estimate the number of tuples of degree bounded monic polynomials $(Q_1, \ldots, Q_v) \in (\mathbb{F}_q[z])^v$ that satisfy given pairwise coprimality conditions.

1. Introduction

The question of calculating the number of relatively prime polynomials of fixed degree in finite fields arose in [7, Section 4.6.1, Ex. 5]. Further results can be found in [4,11,2,3,6].

[*] Corresponding author.
E-mail addresses: arias@us.es (J. Arias De Reyna), randell@unsw.edu.au (R. Heyman).

https://doi.org/10.1016/j.ffa.2018.05.006
1071-5797/© 2018 Elsevier Inc. All rights reserved.

This naturally leads to the concept of tuples of polynomials in finite fields that exhibit pairwise coprimality conditions. This concept is also relevant to polynomial remainder codes used in, amongst other things, error correction (see [12] for an early paper). The density of pairwise coprime polynomials in tuples of finite fields can be inferred from a recent paper [9]. We improve on this result in two ways. Firstly, we contemplate generalised pairwise coprimality conditions. That is, conditions that require some, not necessarily all, of the pairs of polynomials to be coprime. Secondly, we give an asymptotic counting formula rather than simply a density. Another recent paper [5] gives an exact formula for the number of tuples with given coprimality conditions (as we do in Section 3). But we take the analysis further which yields an asymptotic formula.

Our result is heavily based on [1]; a paper that estimates tuples of pairwise coprime integers of bounded height. We use a graph to represent the required primality conditions as follows. Let $G = (V, E)$ be a graph with v vertices and e edges. The set of vertices, V, will be given by $V = \{1, \dots, v\}$ whilst the set of edges of G, denoted by E, is a subset of the set of pairs of elements of V. That is, $E \subseteq \{\{1, 2\}, \{1, 3\}, \dots, \{r, s\}, \dots, \{v-1, v\}\}$. We admit isolated vertices (that is, vertices that are not adjacent to any other vertex). An edge is always of the form $\{r, s\}$ with $r \neq s$ and $\{r, s\} = \{s, r\}$. Let

$$X = \{(Q_1, \dots, Q_v) \in (\mathbb{F}_q[z])^v : Q_r \text{ monic}, 1 \leq r \leq v\}.$$

For each real $x > 0$ and any prime power q, we define the set of all tuples that satisfy the primality conditions by

$$Y_G(x) := \{(Q_1, \dots, Q_v) \in X : \deg Q_r \leq x,\ \ \gcd(Q_r, Q_s) = 1 \text{ if } \{r, s\} \in E\}.$$

We also let $g(x) = |Y_G(x)|$, and denote with d the maximum degree of the vertices of G. All references to polynomials in $\mathbb{F}_q[z]$ will refer to monic polynomials.

Finally, let $Q_G(z)$ and $Q^+_G(z)$ be polynomials in $\mathbb{Q}[z]$ with constant term equal to 1, associated to the graph G and defined by

$$Q_G(z) = \sum_{F \subset E} (-1)^{|F|} z^{|v(F)|}, \qquad Q^+_G(z) = \sum_{F \subset E} z^{|v(F)|}, \tag{1.1}$$

where $|v(F)|$ is the number of non-isolated vertices of graph (V, F).

Our main result is as follows.

Theorem 1.1. *For a natural number $n > 1$, let $g(n)$ be the cardinality of tuples of monic polynomials $(Q_1, \dots, Q_v)$ in $\mathbb{F}_q[z]$ of degree $\deg(Q_r) \leq n$ satisfying the coprimality conditions given by the graph G whose vertices have degree $\leq d$. Then for any $0 < \varepsilon < \frac{1}{2}$ we have*

$$g(n) = \frac{\rho_{G,q}}{(q-1)^v} q^{(n+1)v} \Big(1 + O_{G,q}(n^d q^{-n}) + O_{G,q}(q^{-(1-\varepsilon)n})\Big), \tag{1.2}$$