Finite Fields and Their Applications 33 (2015) 160–174

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A probabilistic approach to value sets of polynomials over finite fields ☆

Zhicheng Gao, Qiang Wang *

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada

A R T I C L E I N F O

Article history:
Received 7 August 2014
Accepted 3 December 2014
Available online 9 January 2015
Communicated by Gary L. Mullen

MSC:
05A16
60E05
11T06

Keywords:
Polynomials
Value sets
Normal distribution
Finite fields

A B S T R A C T

In this paper we study the distribution of the size of the value set for a random polynomial with a prescribed index $\ell \mid (q-1)$ over a finite field $\mathbb{F}_q$, through the study of a random r-th order cyclotomic mapping with index ℓ. We obtain the exact probability distribution of the value set size and show that the number of missing cosets (values) tends to a normal distribution as ℓ goes to infinity. A variation on the size of the union of some random sets is also considered.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Let γ be a fixed primitive element of $\mathbb{F}_q$ throughout the paper. The *value set* of a polynomial g over $\mathbb{F}_q$ is the set V_g of images when we view g as a mapping from $\mathbb{F}_q$ to itself. Clearly g is a *permutation*

☆ Research of authors was partially supported by NSERC of Canada.
* Corresponding author. Fax: +1 613 520 3536.
E-mail addresses: zgao@math.carleton.ca (Z. Gao), wang@math.carleton.ca (Q. Wang).

http://dx.doi.org/10.1016/j.ffa.2014.12.003
1071-5797/

polynomial (PP) of $\mathbb{F}_q$ if and only if the cardinality $|V_g|$ of the value set V_g is q. Asymptotic formulas such as $|V_g| = \lambda(g)q + O(q^{1/2})$, where $\lambda(g)$ is a constant depending only on certain Galois groups associated to g, can be found in Birch and Swinnerton-Dyer [3] and Cohen [9]. Later, Williams [27] proved that almost all polynomials g of degree d satisfy $\lambda(g) = 1 - \frac{1}{2!} + \frac{1}{3!} + \cdots + (-1)^{d-1}\frac{1}{d!}$.

There are also several results on explicit upper bound for $|V_g|$ if g is not a PP over $\mathbb{F}_q$; see for example [16,22,23]. Perhaps the most well-known result is due to Wan [23] who proved that if a polynomial g of degree d is not a PP then

$$|V_g| \le q - \frac{q-1}{d}. \tag{1}$$

On the other hand, it is easy to see that $|V_g| \ge \lceil q/d \rceil$ for any polynomial g over $\mathbb{F}_q$ with degree d. The polynomials achieving this lower bound are called *minimal value set polynomials*. The classification of minimal value set polynomials over $\mathbb{F}_{p^k}$ with $k \le 2$ can be found in [7,17], and in [4] for all the minimal value set polynomials in $\mathbb{F}_q[x]$ whose value set is a subfield of $\mathbb{F}_q$. See [11,24] for further results on lower bounds of $|V_g|$ and [15] for some classes of polynomials with small value sets. More recently, algorithms and complexity in computing $|V_g|$ have been studied in [8]. For a recent survey on value sets of polynomials over finite fields, we refer the readers to Section 8.3 in [18].

We note that all of these previous results mentioned above relate $|V_g|$ to the degree d of g. It is also well known that every polynomial g over $\mathbb{F}_q$ such that $g(0) = b$ has the form $ax^r f(x^s) + b$ with some positive integers r, s such that $s \mid (q-1)$. There are different ways to choose r, s in the form $ax^r f(x^s) + b$. However, in [1], the concept of the index of a polynomial was first introduced and any non-constant polynomial $g \in \mathbb{F}_q[x]$ of degree $\le q-1$ can be written *uniquely* as $g(x) = a(x^r f(x^{(q-1)/\ell})) + b$ with index ℓ defined below. Namely, write

$$g(x) = a\big(x^n + a_{n-i_1}x^{n-i_1} + \cdots + a_{n-i_k}x^{n-i_k}\big) + b,$$

where $a, a_{n-i_j} \ne 0$, $j = 1, \ldots, k$. The case that $k = 0$ is trivial. Thus, we shall assume that $k \ge 1$. Write $n - i_k = r$, the vanishing order of x at 0 (i.e., the lowest degree of x in $g(x) - b$ is r). Then $g(x) = a(x^r f(x^{(q-1)/\ell})) + b$, where $f(x) = x^{e_0} + a_{n-i_1}x^{e_1} + \cdots + a_{n-i_{k-1}}x^{e_{k-1}} + a_r$,

$$\ell = \frac{q-1}{\gcd(n-r, n-r-i_1, \ldots, n-r-i_{k-1}, q-1)} := \frac{q-1}{s},$$

and $\gcd(e_0, e_1, \ldots, e_{k-1}, \ell) = 1$. The integer $\ell = \frac{q-1}{s}$ is called the *index* of $g(x)$. From the above definition of index ℓ, one can see that the greatest common divisor condition makes ℓ minimal among those possible choices.

Clearly, the study of the value set of g over $\mathbb{F}_q$ is equivalent to studying the value set $x^r f(x^{(q-1)/\ell})$ over $\mathbb{F}_q$ with index ℓ. Recently Mullen, Wan and Wang [20] used an index