Accepted Manuscript

Counting polynomials with distinct zeros in finite fields

Haiyan Zhou, Li-Ping Wang, Weiqiong Wang

PII: S0022-314X(16)30290-6
DOI: http://dx.doi.org/10.1016/j.jnt.2016.10.008
Reference: YJNTH 5611

To appear in: *Journal of Number Theory*

Received date: 23 June 2016
Revised date: 14 October 2016
Accepted date: 14 October 2016

Please cite this article in press as: H. Zhou et al., Counting polynomials with distinct zeros in finite fields, *J. Number Theory* (2017), http://dx.doi.org/10.1016/j.jnt.2016.10.008

Counting Polynomials with Distinct Zeros in Finite Fields *

Haiyan Zhou[a] Li-Ping Wang[b] Weiqiong Wang[c,d†]

a. School of Mathematics, Nanjing Normal University, Nanjing 210023, China

Email: haiyanxiaodong@gmail.com

b. Institute of Information Engineering, Chinese Academy of Sciences Beijing 100093, China

Email: wangliping@iie.ac.cn

c. School of Mathematics, Northwest University, Xi'an 710127, China

d. School of Science, Chang'an University, Xi'an 710064, China

Email:wqwang@chd.edu.cn

Abstract Let $\mathbb{F}_q$ be a finite field with $q = p^e$ elements, where p is a prime and $e \geq 1$ is an integer. Let ℓ, n be two positive integers such that $\ell < n$. Fix a monic polynomial $u(x) = x^n + u_{n-1}x^{n-1} + \cdots + u_{\ell+1}x^{\ell+1} \in \mathbb{F}_q[x]$ of degree n and consider all degree n monic polynomials of the form

$$f(x) = u(x) + v_\ell(x),\ v_\ell(x) = a_\ell x^\ell + a_{\ell-1}x^{\ell-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x].$$

For any non-negative integer $k \leq \min\{n, q\}$, let $N_k(u(x), \ell)$ denote the total number of $v_\ell(x)$ such that $u(x) + v_\ell(x)$ has exactly k distinct roots in $\mathbb{F}_q$, i.e.

$$N_k(u(x), \ell) = |\{f(x) = u(x) + v_l(x) \mid f(x) \text{ has exactly } k \text{ distinct zeros in } \mathbb{F}_q\}|.$$

In this paper, we obtain explicit combinatorial formulae for $N_k(u(x), \ell)$ when $n - \ell$ is small, namely when $n - \ell = 1, 2, 3$. As an application, we define two kinds of Wenger graphs called jumped Wenger graphs and obtain their explicit spectrum.

Key words Polynomials, Inclusion-Exclusion Principle, Moments Subset-Sum, Distinct Coordinate Sieve, Spectrum of Graphs

1 Introduction

Let $\mathbb{F}_q$ be a finite field with $q = p^e$ elements, where p is a prime and $e \geq 1$ is an integer. Let $\ell, n(\ell < n)$ be two positive integers. Fix a monic polynomial $u(x) =$

*Research is supported in part by 973 Program (2013CB834203), National Natural Science Foundation of China under Grant No.61202437 and 11471162, in part by Natural Science Basic Research Plan in Shaanxi Province of China under Grant No.2015JM1022 and Natural Science Foundation of the Jiangsu Higher Education Institutes of China under Grant No.13KJB110016.