Finite Fields and Their Applications 46 (2017) 235–246

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Sparse univariate polynomials with many roots over finite fields[☆]

Qi Cheng[a], Shuhong Gao[b], J. Maurice Rojas[c,*], Daqing Wan[d]

[a] School of Computer Science, University of Oklahoma, Norman, OK 73019, United States
[b] Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, United States
[c] TAMU 3368, College Station, TX 77843-3368, United States
[d] Department of Mathematics, University of California, Irvine, CA 92697-3875, United States

ARTICLE INFO

Article history:
Received 6 July 2016
Received in revised form 16 March 2017
Accepted 18 March 2017
Available online xxxx
Communicated by Igor Shparlinski

MSC:
11Y05
11T06
11C99
11T99

Keywords:
Sparse polynomial
t-nomial
Finite field
Descartes
Coset
Torsion

ABSTRACT

Suppose q is a prime power and $f \in \mathbb{F}_q[x]$ is a univariate polynomial with exactly t monomial terms and degree $< q-1$. To establish a finite field analogue of Descartes' Rule, Bi, Cheng, and Rojas (2013) proved an upper bound of $2(q-1)^{\frac{t-2}{t-1}}$ on the number of cosets in $\mathbb{F}_q^*$ needed to cover the roots of f in $\mathbb{F}_q^*$. Here, we give explicit f with root structure approaching this bound: When q is a perfect $(t-1)$-st power we give an explicit t-nomial vanishing on $q^{\frac{t-2}{t-1}}$ distinct cosets of $\mathbb{F}_q^*$. Over prime fields $\mathbb{F}_p$, computational data we provide suggests that it is harder to construct explicit sparse polynomials with many roots. Nevertheless, assuming the Generalized Riemann Hypothesis, we find explicit trinomials having $\Omega\left(\frac{\log p}{\log\log p}\right)$ distinct roots in $\mathbb{F}_p$.

[☆] Partially supported by NSF grant CCF-1409020 and the American Institute of Mathematics. This work was also supported by LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

[*] Corresponding author.
E-mail addresses: qcheng@cs.ou.edu (Q. Cheng), sgao@math.clemson.edu (S. Gao), rojas@math.tamu.edu (J. Maurice Rojas), dwan@math.uci.edu (D. Wan).

http://dx.doi.org/10.1016/j.ffa.2017.03.006
1071-5797/© 2017 Elsevier Inc. All rights reserved.

Chebotarev density
Frobenius
Least prime

1. Introduction

How can one best bound the complexity of an algebraic set in terms of the complexity of its defining polynomials? Over the complex numbers (or any algebraically closed field), Bézout's Theorem [2] bounds the number of roots, for a system of multivariate polynomials, in terms of the degrees of the polynomials. Over finite fields, Weil's famous mid-20th century result [28] bounds the number of points on a curve in terms of the genus of the curve (which can also be bounded in terms of degree). These bounds are optimal for dense polynomials. For sparse polynomials, over fields that are not algebraically closed, these bounds can be much larger than necessary. For example, Descartes' Rule [24] tells us that a univariate real polynomial with exactly t monomial terms always has less than $2t$ real roots, even though the terms may have arbitrarily large degree. Descartes' 17th century results has since been generalized to number fields and p-adic extensions of $\mathbb{Q}$ [18], and local fields of positive characteristics [21].

Is there an analogue of Descartes' Rule over finite fields? Despite the wealth of beautiful and deep 20th-century results on point-counting for curves and higher-dimensional varieties over finite fields, varieties defined by sparse *univariate* polynomials were all but ignored until [7] (see Lemma 7 there, in particular). Aside from their own intrinsic interest, refined univariate root counts over finite fields are useful in applications such as cryptography (see, e.g., [7]), the efficient generation of pseudo-random sequences (see, e.g., [5]), and refined estimates for certain exponential sums over finite fields [6, Proof of Theorem 4]. For instance, estimates on the number of roots of univariate tetranomials over a finite field were a key step in establishing the uniformity of the *Diffie–Helman distribution* [7, Proof of Thm. 8, Sec. 4]—a quantitative statement relevant to justifying the security of cryptosystems based on the Discrete Logarithm Problem.

We are thus interested in the number of roots of sparse univariate polynomials over finite fields. The polynomial $x^q - x$ having two terms and exactly q roots in $\mathbb{F}_q$ might suggest that there is no finite field analogue of Descartes' rule. However, the roots of $x^q - x$ consist of 0 and the roots of $x^{q-1} - 1$, and the latter roots form the unit group $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. For an arbitrary binomial $ax^n + bx^m \in \mathbb{F}_q[x]$ with $n > m$ and a and b nonzero, the roots consist of 0 (if $m > 0$) and the roots of $x^{n-m} + b/a$. Note that the number of roots of $x^{n-m} + b/a$ in $\mathbb{F}_q$ is either 0 or $\gcd(n - m, q - 1)$. In the latter case, the roots form a coset of a subgroup of $\mathbb{F}_q^*$. For polynomials with three or more terms, the number of roots quickly becomes mysterious and difficult, and, as we shall demonstrate in this paper, may exhibit very different behaviors in the two extreme cases where (a) q is a large power of a prime, and (b) q is a large prime.

To fix notation, we call a polynomial $f(x) = c_1x^{e_1} + c_2x^{e_2} + \cdots + c_tx^{e_t} \in \mathbb{F}_q[x]$ with $e_1 < e_2 < \cdots < e_t < q - 1$ and $c_i \neq 0$ for all i a *(univariate) t-nomial.* The best current