Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Estimating the number of roots of trinomials over finite fields

Zander Kelley [1], Sean W. Owen [1]

ARTICLE INFO

Article history:
Received 19 April 2016
Accepted 17 July 2016
Available online xxxx

Keywords:
Finite field
Sparse polynomial
Trinomial
Poisson distribution
Chebotarev density

ABSTRACT

We show that univariate trinomials $x^n + ax^s + b \in \mathbb{F}_q[x]$ can have at most $\delta\left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{\delta}} \right\rfloor$ distinct roots in $\mathbb{F}_q$, where $\delta = \gcd(n, s, q-1)$. We also derive explicit trinomials having $\sqrt{q}$ roots in $\mathbb{F}_q$ when q is square and $\delta = 1$, thus showing that our bound is tight for an infinite family of finite fields and trinomials. Furthermore, we present the results of a large-scale computation which suggest that an $O(\delta \log q)$ upper bound may be possible for the special case where q is prime. Finally, we give a conjecture (along with some accompanying computational and theoretical support) that, if true, would imply such a bound.

1. Introduction

For univariate polynomial equations defined over a field, it is desirable to obtain general upper bounds on the number of solutions given in simple terms of plainly available information, such as the coefficients, exponents, or number of terms. The ubiquitous example of this is the degree bound, but over non-algebraically closed fields, it is possible to considerably improve upon the degree bound for certain non-negligible families of polynomials. Over the real numbers, Descartes' Rule of Signs implies that a t-nomial f must have less than $2t$ real roots. For sparse polynomials – those with a small number of nonzero terms – this can provide a remarkable improvement on the trivial upper estimate given by the degree of f.

In Canetti et al. (2000), the authors establish a finite field analogue of Descartes' Rule: a sparsity-dependent upper bound on the number of roots of a t-nomial over $\mathbb{F}_q$. More recently, an improved

E-mail address: zander_k@tamu.edu (Z. Kelley).

[1] Partially supported by NSF grants DMS-1156589, DMS-1460766, and CCF-1409020.

http://dx.doi.org/10.1016/j.jsc.2016.08.008
0747-7171/

upper bound was derived in Kelley (2016). Here, we investigate possible further improvements to the bound for the special case of $t = 3$. This can be considered the smallest nontrivial choice of t, since the zero sets of univariate binomials are easily characterized – they are simply cosets of subgroups of $\mathbb{F}_q^*$, possibly together with $0 \in \mathbb{F}_q$.

Theorem 1.1. *(Kelley, 2016, Theorems 2.2 and 2.3) Let*

$$f(x) = c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_t x^{a_t} \in \mathbb{F}_q[x]$$

with all c_i nonzero and $a_1 > a_2 > \cdots > a_t = 0$. If f vanishes on an entire coset of a subgroup $H \subseteq \mathbb{F}_q^*$, then

$$\#H \in \{k \in \mathbb{N} : \text{for each } a_i, \text{ there is an } a_j \text{ with } j \neq i \text{ and } a_i \equiv a_j \pmod{k}\}.$$

Furthermore, let $R(f)$ denote the number of distinct roots of f in $\mathbb{F}_q$, and suppose $R(f) > 0$. If C denotes the maximal cardinality of a coset on which f vanishes, then

$$R(f) \leq 2(q-1)^{1-1/(t-1)} C^{1/(t-1)}.$$

For a trinomial $f(x) = x^n + ax^s + b \in \mathbb{F}_q[x]$, with a and b nonzero, associate the parameter

$$\delta = \gcd(n, s, q-1).$$

Suppose that $R(f) > 0$. It follows from Theorem 1.1 that if f vanishes on a coset of size C, then $n \equiv s \equiv 0 \pmod{C}$. Since C must divide $\#\mathbb{F}_q^*$, we have that C divides δ. On the other hand, if f vanishes at $\alpha \in \mathbb{F}_q$, then $\alpha \in \mathbb{F}_q^*$, and f vanishes on the entire coset $\{x \in \mathbb{F}_q^* : x^\delta = \alpha^\delta\}$ of order δ. So, in the trinomial case we have explicitly that $C = \delta$, and the bound given above simplifies to

$$R(f) \leq 2\sqrt{\delta(q-1)}.$$

As pointed out in Cheng et al. (2014), this bound for trinomials is also a consequence of an earlier result from Bi et al. (2013) which bounds the number of cosets $S_i \subset \mathbb{F}_q^*$ needed to express the zero set of a sparse polynomial as a union of the form $\bigcup_{i=1}^N S_i$. Our first result refines this upper bound.

Theorem 1.2. *The roots of a trinomial*

$$f(x) = x^n + ax^s + b \in \mathbb{F}_q[x]$$

are the union of no more than $\left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{\delta}} \right\rfloor$ cosets of the subgroup $H \subseteq \mathbb{F}_q^*$ of size δ.

Consequently, we now have $R(f) \leq \delta \left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{\delta}} \right\rfloor$, improving the previous result by approximately a factor of 2 when $\delta \ll q$. The method of proof is elementary but interesting: given a trinomial with $\delta = 1$ and r roots in a field of undetermined size, we construct $r^2 - r + 1$ distinct nonzero elements in the field, giving a lower bound on its size.

Additionally, we show that when $\delta = 1$, this new bound is optimal for even-degree extensions of $\mathbb{F}_p$. If q is an even power of a prime p and $\delta = 1$, the bound reduces to $R(f) \leq \sqrt{q}$, and we can indeed construct trinomials with $\delta = 1$ and $\sqrt{q}$ distinct roots in $\mathbb{F}_q$.

Theorem 1.3. *For any odd prime p, the trinomial $x^{p^k} + x - 2$ has exactly p^k roots in $\mathbb{F}_{p^{2k}}$.*

We prove Theorem 1.3 via linear-algebraic techniques: the extremal examples provided are translations of linear maps with null-spaces of exactly half the dimension of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_{\sqrt{q}}$. The optimality of the bound is somewhat murkier when $\mathbb{F}_q$ is not an even-degree extension. Trinomials with nearly as many roots have been found for some other cases; for example, when q is a cube, Cheng et al. (2014) give the example $f(x) = x^{1+q^{1/3}} + x + 1$ which has $q^{1/3} + 1$ roots.

Please cite this article in press as: Kelley, Z., Owen, S.W. Estimating the number of roots of trinomials over finite fields. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.08.008