Extremal Trinomials over Quadratic Finite Fields

Sean W. Owen

University of Maryland, Baltimore County

July 19, 2015

The Ten-Second Version

We present bounds on the numbers of roots of trinomials over finite fields whose orders are the squares of prime numbers.

Background: Descartes' Rule

The number of solutions of sparse polynomials over the reals is bounded above sharply by Descartes' Rule.

Theorem (Descartes' Rule)

A polynomial $f(x) \in \mathbb{R}[x]$ with t nonzero terms has at most $2t-1$ real zeros. Furthermore, $x(x^2-1)(x^2-2)\cdots(x^2-(t-1))$ attains this maximum.

.

The same rule does not hold over finite fields (ex: $x^q - x$ over $\mathbb{F}_q$), so it is necessary to find an alternate rule.

Background: The Coset Rule

- Bi, Cheng, and Rojas (2014) recently proved a rule for polynomials with t terms over $\mathbb{F}_q$.
- The roots appear in multiplicative cosets, whose number and size are bounded in terms of t and the quantity δ, which is the gcd of the exponents with $q-1$.

$$\delta = \gcd(a_2, \ldots, a_t, q-1)$$

Existing Results for Trinomials

These are Cheng, Gao, Rojas, and Wang's previous bounds for trinomials in $\mathbb{F}_q$ with $q = p^k$.

UPPER	All k	$O(q^{\frac{1}{2}})$ (follows from coset result)
LOWER	$3\|k$	$\Omega(q^{\frac{1}{3}})$ (by example)
	Other	$\Omega(\frac{\log\log q}{\log\log\log q})$ unconditionally $\Omega(\frac{\log q}{\log\log q})$ assuming GRH

Our Mission

We set out to find results for a little-explored case, $k = 2$. Our plan of attack for achieving this was the following:

1. Obtain raw data on the numbers of roots of trinomials on small quadratic fields, primarily through computational experiments.
2. Find trinomials with unusually large numbers of roots, to establish a lower bound on the maximum.
3. Formulate conjectures about upper and lower bounds on the root count, and, if possible, prove them.

Summary of Results

1. We completed basic computational surveys of the quadratic fields of order less than 250,000.
2. We discovered a class of trinomials with $\delta = 1$ having p roots on all $\mathbb{F}_{p^2}$, using linear algebra techniques.
3. We then proved an upper bound of p for $\delta = 1$ by showing that all such trinomials can be reduced to a smaller class that share no roots among themselves.

The end result is a precise upper bound of p on root counts for $\delta = 1$.

The Extremal Examples

Theorem

$f(x) = x^p + x - 2$ *has* p *nonzero roots in* $\mathbb{F}_{p^2}$.

- We originally noticed these trinomials while writing the first program, by observing that they had the property $f(x+z) = f(x)$ for certain z.
- It later became apparent that this property was a result of f being a translation of the linear map $T(x) = x^p + x$.

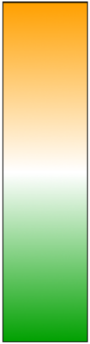
The Extremal Examples, cont.

- Briefly: $\mathbb{F}_{p^2}$ is a two-dimensional vector space over $\mathbb{F}_p$.
- If we can find a linear map with a nonzero root that isn't the zero transformation, we know that it has nullity 1, and p roots.
- $T(x) = x^p + x$ is such a map. Since it's linear, we know that it also attains the value 2 p times, and therefore that $f(x) = T(x) - 2$ attains zero p times, for nonzero x.

Designing the Computational Experiments

Our experiments all ran on the same core method - check the roots of each member of a subset of all the trinomials on $\mathbb{F}_{p^2}$ (more on that shortly).
We varied whether they covered many fields, or recorded detailed data.

More Detail



More Reach

$0 < p < 20$	Record root count for every trinomial in test class
$20 < p < 100$	Record distinct root counts found for each choice of exponents
$100 < p < 500$	Record distinct root counts found and lowest degree at which found

The Experiments, pt. 2: The Empire Strikes Back

Our challenge was to cut down the set of trinomials we needed to check: with no restrictions, its size grows as the sixth power of the order of the field.

- Start with all trinomials over $\mathbb{F}_{p^2}$.

$$c_1 x^{a_1} + c_2 x^{a_2} + c_3 x^{a_3} : \Theta(q^6)$$

- We're allowed to divide by a monomial, so we can assume $c_1 = 1$ and $a_1 = 0$.

$$1 + c_2 x^{a_2} + c_3 x^{a_3} : \Theta(q^4)$$

The Experiments, pt. 3: The Return of the Jedi

- If f has any roots, a transformation $f(x) \mapsto f(zx)$ for $f(z) = 0$ will make 1 a root. So we can assume that the sum of the coefficients is zero.

$$1 + cx^{a_2} - (c+1)x^{a_3} : \Theta(q^3)$$

- We also chose to restrict $a_2 = 1$.

$$1 + cx - (c+1)x^{d} : \Theta(q^2)$$

This is as well as we can do, more or less.

The Experiments, pt. 4: The Force Awakens

$$f(x) = 1 + cx - (c+1)x^d$$

- Naive method: Set d, c. Cycle over all x and count zeros. $\Theta(q^3)$
- However! Once d is set, x is a root for at most one c.
- So instead... Set d. For each x, solve for c. Count how many times each c appears. $\Theta(q^2)$.

The Upper Bound

All of that turns out to have more uses than just optimizing our experiments; each of those results is integral to the proof of our upper bound.

Theorem

Over a finite field $\mathbb{F}_q$ with $q = p^2$, if a trinomial

$$f(x) = c_1 + c_2 x^{a_2} + c_3^{a_3}$$

satisfies $\delta = \gcd(a_2, a_3, q-1) = 1$, then it has no more than p roots.

The Upper Bound, pt. 2: The Temple of Doom

- Say that $f(x)$ has r roots.
- It can be turned into $1 + cx^{a_2} - (c+1)x^{a_3}$ for some c, by dividing by c_1 and taking $f(zx)$.
- However, if $r > 1$, we can make more than one choice of z for that process. We can make r choices, in fact.
- So, from $f(x)$, we can find r, trinomials of that reduced form with r roots, and $\delta = 1$ guarantees they're all distinct.

The Upper Bound, pt. 3; The Last Crusade

- Now, remember, none of those trinomials have any roots in common but 1.
- So, together, they have $r(r-1)+1$ roots.
- But there are only p^2-1 nonzero elements in the field. So

$$r^2 - r + 1 \leq p^2 - 1.$$

- And we find that the largest integer satisfying this is p.

Extensions

- Both of our major results work in the same way on any even-degree field. $x^{p^n} + x - 2$ has p^n roots on $\mathbb{F}_{p^{2n}}$, and we can show that this is a maximum.

- We can apply this method to $\delta \neq 1$, by substituting $y = x^\delta$.

$$1 + x^2 + x^6 \longmapsto 1 + y + y^3$$

- Our proof of the upper bound may work in a modified form on polynomials with more terms. We're not sure.