Extremal Trinomials over Quadratic Finite Fields

Sean W. Owen

July 22, 2015

Abstract

In the process of pursuing a finite field analogue of Descartes' Rule, Bi, Cheng, and Rojas (2014) proved an upper bound of $2\sqrt{q-1}$ on the number of roots of a trinomial $c_1 + c_2x^{a_2} + c_3x^{a_3} \in \mathbb{F}_q[x]$, conditional on the exponents satisfying $\delta = \gcd(a_2, a_3, q-1) = 1$, and Cheng, Gao, Rojas, and Wan (2015) showed that this bound is near-optimal for many cases. Our project set out to refine these results by finding new bounds and extremal examples for cases not yet explored. We construct a class of extremal examples having $\sqrt{q}$ roots on fields with q an even power of a prime, by using linear maps with large null spaces over $\mathbb{F}_q$. Additionally, we present a new upper bound of $\frac{1+\sqrt{4q-7}}{2}$ for all q under the same constraints as before, using an alternate method involving reduced trinomials with disjoint root sets, which establishes the examples as maximal. Our methods offer several possible generalizations to other cases.

1 Background and Objectives

Sparse polynomials, which have a fixed number of terms, regardless of their degree, often have much lower maximum numbers of roots than general polynomials over the same field. For example, over the real numbers, Descartes's Rule states that a polynomial with t nonzero roots must have less than $2t$ real roots. This bound is sharp; for example, the polynomial $x(x^2-1)(x^2-2)\cdots(x^2-(t-1))$ has t terms and $2t-1$ roots [2].

Our current work is part of an effort to formulate an analogous rule for finite fields $\mathbb{F}_q$. We define a univariate t-nomial as $f(x) = c_1 + c_2x^{a_2} + \cdots + c_tx^{a_t}$ with $a_2 < \cdots < a_t < q-1$, and for such f we define $\delta = \gcd(a_2, \ldots, a_t, q-1)$. Bi, Cheng and Rojas (2014) recently showed that the nonzero roots of t-nomials over $\mathbb{F}_q$ display a peculiar multiplicative structure: they can be partitioned into cosets of two subgroups of $\mathbb{F}_q^*$, whose number and size are predictable based on q, t, and δ.

Theorem 1.1 (Thm. 1.1 in [1]). *The nonzero roots of a univariate t-nomial as defined above are the union of at most $2\left(\frac{q-1}{\delta}\right)^{\frac{t-2}{t-1}}$ cosets of two subgroups $S_1 \subseteq S_2$, with $|S_1| = \delta$ and $|S_2| \geq \delta\left(\frac{q-1}{\delta}\right)^{\frac{1}{t-1}}$.*

Additionally, their proof shows that, in the case of trinomials ($t = 3$), all cosets are of the first size, δ, which implies an upper bound on the root count of $2\sqrt{\delta(q-1)}$.

Cheng, Gao, Rojas, and Wan (2015) also provided asymptotic lower bounds for the maximum number of roots of trinomials satisfying $\delta = 1$ on fields of various degrees. On fields whose orders are cubes ($q = p^{3n}$), they succeeded in producing examples with $q^{1/3} + 1$ roots, which is reasonably close in growth order to the upper bound of $\mathrm{O}(q^{1/2})$. However, on other fields, their bounds are sub-logarithmic, and in their strongest form rely on the Generalized Riemann Hypothesis.

We set out to refine these existing results by exploring a little-studied case, that of quadratic fields ($q = p^2$).

Our main tasks in pursuit of this goal were the following:

1. Conduct limited computational experiments to gather data on the root counts of trinomials on $\mathbb{F}_{p^2}$, as none have been conducted yet. Observe patterns in the data and propose conjectures about the numbers of roots.

2. Attempt to produce new extremal trinomials, to establish a higher lower bound on the maximum root count.

3. Prove stronger asymptotic or exact bounds on root counts if possible.

2 Summary of Results

Our first main result was the existence of a family of extremal trinomials on quadratic fields. We later determined that it could in fact be extended to any field of even degree, and this is the version that is presented here. This example is not unique; we can apply a variety of transformations of the exponents and coefficients to generate a broad class of extremal trinomials.

Theorem 2.1. *On a finite field $\mathbb{F}_q$ with $q = p^{2k}$ for k a natural number and p an odd prime, the trinomial*

$$x^{p^k} + x - 2$$

has exactly $p^k = \sqrt{q}$ nonzero roots.

Our second round of computational experiments suggested that this number of roots is in fact maximal for $\delta = 1$. We succeeded in proving this.

Theorem 2.2. *On any field $\mathbb{F}_q$, if a trinomial*

$$f(x) = 1 + c_2 x^{a_2} + c_3 x^{a_3}$$

satisfies $\delta = \gcd(a_2, a_3, q-1) = 1$, then it has no more than $\frac{\sqrt{4q-7}+1}{2}$ nonzero roots. In the case that q is an even power of a prime number p, the greatest integer less than or equal to this upper bound is exactly $\sqrt{q}$.

These two results taken together establish an exact upper bound on the number of roots of trinomials with $\delta = 1$ on even-degree fields, including the quadratic fields we set out to study. Additionally, on odd-degree fields, Theorem 2.2 provides an improvement on the existing upper bound of $2\sqrt{q-1}$.

3 Computational Data

Our computational work was relatively small in scale, covering few fields, since the size of successive quadratic fields grows very quickly. Nevertheless, we managed to amass enough data to motivate useful and provable conjectures.

3.1 Design

Our first task was to find ways to reduce the number of trinomials that we needed to solve without losing information, since the full set of trinomials

$$c_1x^{a_1} + c_2x^{a_2} + c_3x^{a_3} \in \mathbb{F}_{p^2}$$

grows in size as $\Theta(p^{12})$. We succeeded in making three restrictions.

- A trinomial may be multipled or divided by a power of x without changing its number of nonzero roots. Therefore, we may assume $a_1 = 0$.
- A trinomial may be multiplied or divided by a constant without changing its number of roots. Therefore, we may assume $c_1 = 1$.
- If f has a root $z \neq 0$, then transforming it by substituting $x \mapsto zx$ yields a trinomial with the same number of roots, and 1 as a root. Therefore, we may assume $c_1 + c_2 + c_3 = 0$.

In addition, we decided to limit $a_2 = 1$. We have no theoretical basis for this move, but based on limited inquiry into the case $a_2 = 2$, we believe it to have minimal impact on our data, and in any case this is the procedure followed by our colleagues. As a result, we need only search

$$cx^{a_3} - (c+1)x + 1,$$

and there are only $\Theta(p^4)$ of these.

Our final observation was that, all else being equal, substituting $a_3 \mapsto q - a_3$ does not change the number of roots, so checking $a_3 > q/2$ is unnecessary. This does not provide any improvements in growth order, but does cut the number of cases in half, which at the small scale of our experiments is fairly significant.

- On the first four odd-ordered fields ($\mathbb{F}_9, \mathbb{F}_{25}, \mathbb{F}_{49}, \mathbb{F}_{121}$), we gathered comprehensive data, writing down the root counts for every reduced trinomial, with all possible exponent pairs. This data motivated Theorem 2.1.

- On the odd-ordered fields below 100, we recorded possible root counts with sample trinomials, for all reduced trinomials with linear terms (as well as more limited data for reduced trinomials with quadratic terms). This data suggested Theorem 2.2, which we succeeded in proving shortly afterward.
- On the odd-ordered fields below 500, we recorded possible root counts for reduced trinomials with linear terms, as well as the lowest degree at which each root count appeared.

4 Proofs of Main Results

4.1 Extremal Trinomials

Our current proof of Theorem 2.1 relies on linear-algebraic techniques: the extremal examples provided are translations of linear maps with large null-spaces on $\mathbb{F}_q$.

Proof of Theorem 2.1. Observe that the function

$$T(x) = x^{p^k} + x$$

is an $\mathbb{F}_{p^k}$-linear map from $\mathbb{F}_q$ to $\mathbb{F}_q$: Since p is the characteristic of $\mathbb{F}_q$, we have that $(x+y)^p = x^p + y^p$ (which extends to all powers of p) and since all $a \in \mathbb{F}_{p^k}$ satisfy $a^{p^k} = a$, we have $(ax)^{p^k} = a(x^{p^k})$. $T(x)$ has as zeros all the solutions of $x^{p^k-1} = -1$, and since $(-1)^{\frac{q-1}{\gcd(q-1,p^k-1)}} = 1$, such solutions exist and are nonzero, so its null space has positive dimension. However, $T(x)$ is also not uniformly zero, as, for example, $T(1) = 2$, so its null space's dimension is not 2. We conclude, therefore, that the $T(x)$ has a null space of dimension 1, and therefore that it has p^k zeros.

We see that $f(x) = 0$ exactly when $T(x) = 2$. Since we know that $T(1) = 2$, we can then observe from the linearity of T that $T(x) = 2$ exactly when $x = z+1$ for $T(z) = 0$. Therefore, $f(x)$ has $p^k = \sqrt{q}$ roots, all of which are nonzero. □

Remark. The construction is slightly different for q a power of 2. In that case $2 \equiv 0$, and therefore $f(x)$ is a binomial and has a root of zero. However, it is a simple matter to translate $T(x)$, which is still a rank one linear map, by a different, nonzero element from its range.

4.2 The Upper Bound

Our central tool in this proof is our ability to reduce the trinomials in $\mathbb{F}_q[x]$ with a given support into a more restricted family that preserves its variety of root counts.

Definition 4.1. For a_2, a_3 fixed, define the family of trinomials in $\mathbb{F}_q[x]$

$$C(a_2, a_3) = \{f_c(x) = 1 - (c+1)x^{a_2} + cx^{a_3} | c \neq 0, -1.\}$$

Observe that $C(a_2, a_3)$ is exactly the set of trinomials with support $\{0, a_2, a_3\}$ and constant term 1 having 1 as a root: $f(1) = 0$ if and only if its coefficients sum to zero. As we showed in explaining our computational experiments, every trinomial may be transformed into one of this form having the same number of roots.

This family also has another, very useful property.

Lemma 4.2. *For* $\gcd(a_2, a_3, q-1) = 1$*, every* $x_0 \neq 1$ *in* $\mathbb{F}_q^*$ *is a root of at most one distinct* $f_c \in C(a_2, a_3)$*.*

Proof. $f_c(x_0) = 0$ is equivalent to the following linear equation in c:

$$c(x_0^{a_3} - x_0^{a_2}) = x_0^{a_2} - 1.$$

For all x_0 such that $x_0^{a_3} \neq x_0^{a_2}$, this trinomial may be solved for c; if $c \neq 0, -1$, then this is the unique c for which $f_c(x_0) = 0$, and otherwise no such f_c exists.

On the other hand, when $x_0^{a_3} = x_0^{a_2}$, the left-hand side is zero, and the equation is either true for all c or for no c. It is true for all c if and only if $x_0^{a_2} = 1$ as well. Since $\gcd(a_2, a_3, q-1) = 1$, the only x_0 satisfying $x^{a_3} = x^{a_2} = 1$ is 1, so, because $x_0 \neq 1$, we conclude that the equation holds for no c and these x_0 are roots of no f_c. □

The fact that the root sets of all of $C(a_2, a_3)$ cannot overlap suggests a bound of some sort on the root count of any individual polynomial, and that bound is in fact Theorem 2.2.

Proof of Theorem 2.2. It suffices to prove that all $f_c \in C(a_2, a_3)$ have at most $\sqrt{q}$ roots.

Assume that some $f_1 \in C(a_2, a_3)$ has r roots: $1, z_2, \ldots, z_r$, and let $f_i = f_1(z_i x)$ for $2 \leq i \leq r$. Each f_i has r roots and belongs to $C(a_2, a_3)$. Additionally, we can show that all are distinct: $f(zx) = f(x)$ iff $z^{a_3} = z_2^a = 1$, and since $\delta = 1$, that occurs only when $z = 1$. Finally, by Lemma 4.2, the only root shared between any two f_i is 1. Therefore, among them, the f_i have $r(r-1)+1$ distinct roots. The set of these roots is a subset of $\mathbb{F}_q^*$, so it must be true that:

$$r^2 - r + 1 \leq q - 1$$

which may be solved to give

$$r \leq \frac{\sqrt{4q-7}+1}{2}.$$

Additionally, assume $\sqrt{q} \in \mathbb{N}$. We may see fairly easily that, if $r = \sqrt{q}$, the original inequality is satisfied for $q \geq 4$, which covers all relevant cases, but $r = \sqrt{q} + 1$ implies that r is negative, which is a contradiction. Furthermore, since $r^2 - r + 1$ is an increasing function on positive r, we can surmise that the inequality is not satisfied for any higher r. □

5 Further Conjectures

Based on the data we gathered, we also made a few other observations that we were not able to prove. We present them here.

Conjecture 1. *Without restrictions on δ, the maximum number of roots of a trinomial on $\mathbb{F}_q$ with $q = p^2$ for an odd prime p is $\frac{2}{3}(q-1)$.*

We have an example of a trinomial with this many roots, namely, $f(x) = (x^{\frac{1}{3}(q-1)} - a)(x^{\frac{1}{3}(q-1)} - b)$ for $a^3 = b^3 = 1$, $a \neq b$. This relies on the fact that $p^2 - 1$ is always a multiple of 3.

Conjecture 2. *The upper bound supplied by Theorem 2.2 is not sharp for odd-degree fields.*

In these cases, $\sqrt{q}$ is not an integer, and thus no analogue to the trinomials of Theorem 2.1 can be constructed.

Conjecture 3. *If a trinomial on $\mathbb{F}_q$ with $\delta = 1$ attains a given root count, the same root count is attained by some trinomial with $a_2 = 1$.*

As mentioned before, our experiments assumed this to be the case, but we have had no success in proving it.

6 Acknowledgements

We thank Texas A&M University for hosting the REU in which we carried out this research, and the National Science Foundation for funding it. Thank you as well to our advisor, J. Maurice Rojas, for all of his guidance.

We also are grateful for the help of our colleague Alexander Kelley. He supplied us with several of the devices used to optimize our computational experiments, and, crucially, Lemma 4.2 is his insight, which we were able to refine and spin into a proof of our upper bound.

References

[1] Bi, Jingguo; Cheng, Qi; and Rojas, J. Maurice, *"Sub-Linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields"*, 2012, arXiv:1204.1113v2 [math.NT].

[2] Cheng, Qi; Gao, Shuhong; Rojas, J. Maurice; and Wan, Daqing, *"Sparse Univariate Polynomials with Many Roots Over Finite Fields"*, 2014, arXiv:1411.6346v2 [math.NT].