The Number of Roots of Trinomials over Prime Fields

Zander Kelley

July 20, 2015

Background and Previous Work

- Bi, Cheng, and Rojas (2014): A "Descartes Rule" for sparse polynomials over finite fields.
- They show the bound is optimal in many cases by explicitly finding polynomials with many roots.
- However their construction works only for t-nomials over $\mathbb{F}_{p^t}$

terms	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$	$\mathbb{F}_{p^3}$	$\mathbb{F}_{p^4}$	$\mathbb{F}_{p^5}$
3			✓		
4				✓	
5					✓

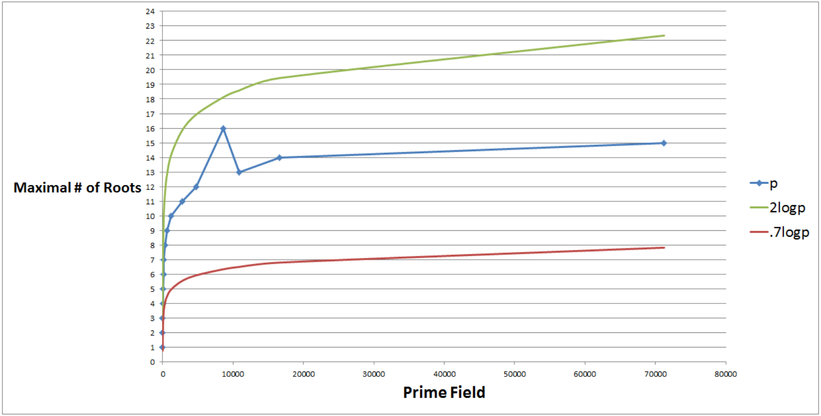
Current Bounds for the “Simplest” Case

$$f(x) = x^n + ax^s + b \mod p$$

- We restrict our attention to trinomials with $\delta = gcd(n, s, p-1) = 1$.
- When $\delta \neq 1$, we can use $|Z(x^n + ax^s + b)| = \delta * |Z(x^{n/\delta} + ax^{s/\delta} + b) \cap \langle g^\delta \rangle|$, where $\langle g \rangle = \mathbb{F}_p$.
- For trinomials $f \in \mathbb{F}_p[x]$ with $\delta = 1$, $|Z(f)| = O(\sqrt{p})$.

$O(\sqrt{p})$ appears to be far from optimal

- Cheng, Gao, Rojas, and Wan (2015): There is an infinite set of $\delta = 1$ trinomials with at least $\Omega(\frac{\log \log p}{\log \log \log p})$ roots.
- A brute force search through $\delta = 1$ trinomials suggests that $|Z(f)|$ may grow as slowly as $O(\log p)$.



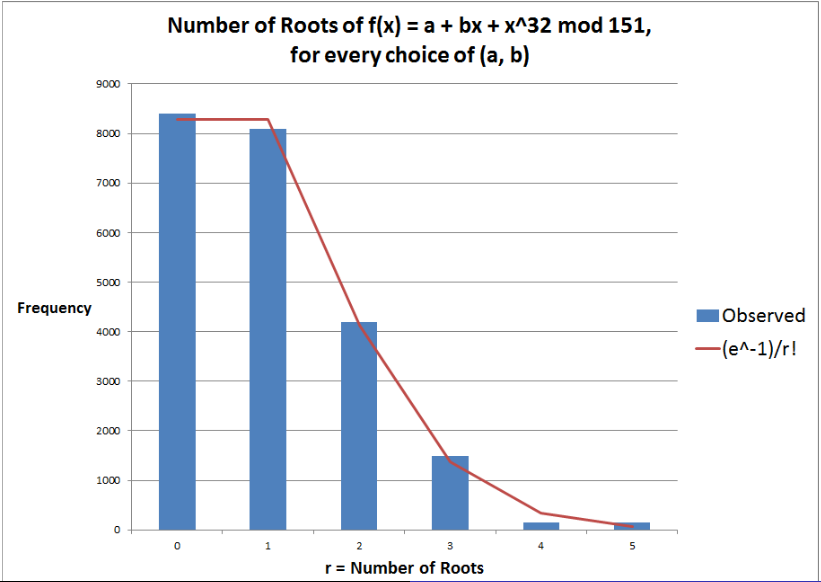
A New Direction: “Typical” Values of $|Z(f)|$

Question

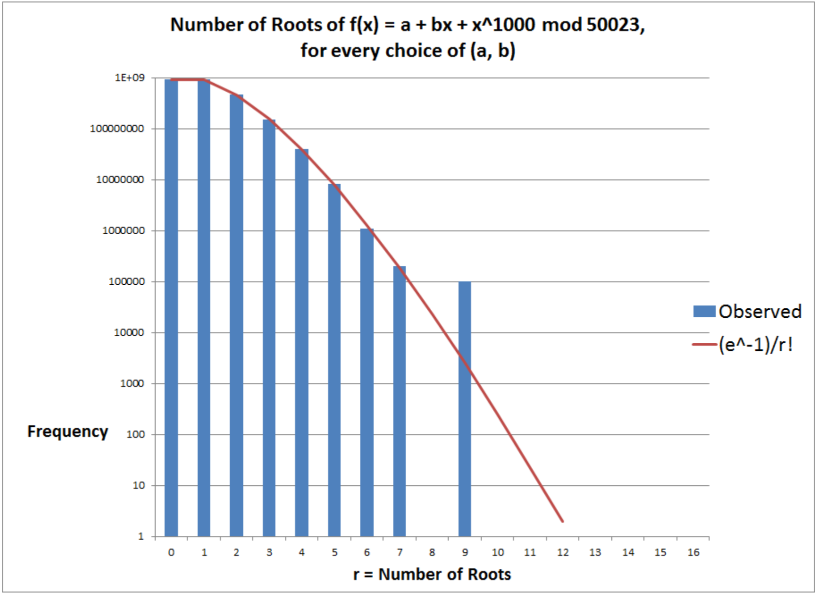
Given a uniform random pair $(a, b) \in (\mathbb{F}_p^*)^2$, what is the distribution of $|Z(x^n + ax^s + b)|$? (with n, s, and p fixed)

- Many similar questions have been posed and solved for polynomial systems over various fields.
- However, for finite fields, the focus has traditionally been on more general situations.
- As far as we know, this question is not well-studied for this simple case of trinomials over prime finite fields.

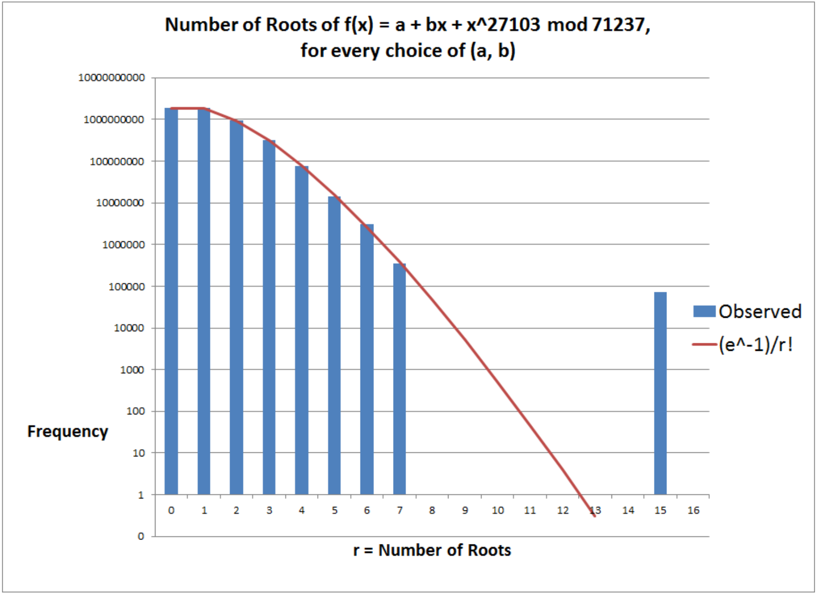
Experimental Data



Experimental Data



Experimental Data



A Partial Distribution Result

Theorem

Fix $n, s, r \in \mathbb{Z}$ with $gcd(n,s) = 1$. Let $P_M = \{p\, prime : p \leq M\}$. Let $p \in P_M$ and $(a,b) \in (\mathbb{F}_p^*)^2$ be uniformly random. Under the Generalized Riemann Hypothesis, the probability that $f(x) = x^n + ax^s + b$ has r roots converges to $\frac{e^{-1}}{r!}$ as $M \to \infty$.

Prime Density

Definition

A set of primes S has *density* δ if $\frac{\#\{q \in S : q \leq x\}}{\#\{p \ prime : p \leq x\}} \to \delta$ as $x \to \infty$.

(A Special Case Of) Frobenius' Density Theorem

For $g(x) \in \mathbb{Z}[x]$, let $Gal(g)$ be the Galois group of the splitting field of g over $\mathbb{Q}$, and let
$C_r = \{\sigma \in Gal(g) \ : \ \sigma \ has \ r \ fixed \ points\}$. Then
$density(\{p \ prime \ : \ (g \mod p) \ has \ r \ roots \ in \ \mathbb{F}_p\}) = \frac{|C_r|}{|Gal(g)|}$.

(A Special Case Of) Dirichlet's Density Theorem

Let p be prime and let $a \in \mathbb{N}$ be less than p. Then
$density(\{q \ prime \ : \ q \equiv a \mod p\}) = \frac{1}{\varphi(p)} = \frac{1}{p-1}$.

Fixed Points Of A Random Permutation

Theorem [CMS99]

For $g(x) = x^n + ax^s + b \in \mathbb{Z}[x]$, If $gcd(bn, as(n-s)) = 1$, Then $Gal(g) \cong S_n$ or A_n.

- Consider $g(x) = x^n + q_a x^s + q_b$ where q_a and q_b are primes.
- Suppose $Gal(g) \cong S_n$ (the A_n case is similar). By Frobenius, the density of primes p such that $(g \mod p)$ has r roots in $\mathbb{F}_p$ is

$$\frac{|C_r|}{|S_n|} \approx \frac{n!/er!}{|S_n|} = \frac{n!/er!}{n!} = \frac{e^{-1}}{r!}.$$

- Key trick: By Dirichlet, primes are distributed evenly among residue classes mod p, so choosing random (q_a, q_b) and then reducing mod p is equivalent to choosing random $(a, b) \in (\mathbb{F}_p^*)^2$.

A Convenient Way To Uniformly Sample $(a, b) \in (\mathbb{F}_p^*)^2$

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

$$g(x) = x^n + q_a x^s + q_b \in \mathbb{Z}[x]$$

- Choose q_a and q_b randomly from a large set of primes $Q = \{q \; prime : n < q \leq M^3\}$
- By Dirichlet, for a given $a \in \mathbb{F}_p$, the probability that $(q \mod p) = a$ approaches $\frac{1}{\varphi(p)} = \frac{1}{p-1}$ as $M \to \infty$.

A Partial Distribution Result

Theorem

Fix $n, s, r \in \mathbb{Z}$ with $gcd(n, s) = 1$. Let $P_M = \{p\, prime : p \leq M\}$. Let $p \in P_M$ and $(a, b) \in (\mathbb{F}_p^*)^2$ be uniformly random. Under the Generalized Riemann Hypothesis, the probability that $f(x) = x^n + ax^s + b$ has r roots converges to $\frac{e^{-1}}{r!}$ as $M \to \infty$.

- GRH is necessary to handle conflicting convergence requirements of the Frobenius and Dirichlet density theorems.
- Since the prime p is allowed to vary, this result is a weaker version of our Poisson distribution conjecture, which appears plausible for fixed p in our computational examples.
- If we could prove the conjectured version for fixed p, the conjectured $O(\log p)$ bound would follow by considering the expected maximum value out of p^2 samples of a Poisson process.

The Number of Roots of Trinomials over Prime Fields

Zander Kelley

July 20, 2015