ROOTS OF TRINOMIALS OVER PRIME FIELDS

ZANDER KELLEY

1. Introduction

The origin of this work was the search for a "Descartes' rule" for finite fields - a nontrivial upper bound for the number of roots of sparse polynomials. In [2], Bi, Cheng, and Rojas establish such an upper bound. Then, in [3], Cheng, Gao, Rojas, and Wan show that the bound is essentially optimal in an infinite number of cases by constructing t-nomials with many roots in $\mathbb{F}_{p^t}$. However, the bound's optimality remains open in other cases. Here, we look at the roots of trinomials over $\mathbb{F}_p$.

Let $Z(f)$ denote the zero-set of $f(x) = a_1 + a_2x^{e_2} + \cdots + a_tx^{e_t} \in \mathbb{F}_q[x]$. At first glance, a nontrivial upper bound for $|Z(f)|$ seems unlikely: consider $f(x) = x^{\frac{q-1}{2}} - 1$, which always has half of the nonzero elements of $\mathbb{F}_q$ as roots. However, a key observation of [2] is that sparse polynomials with many roots have a simple, common characterization: they have large values of $\delta(f) := gcd(e_0, \ldots, e_t, q-1)$.

Lemma 1.1 ([2])**.** *Let g be a generator of $\mathbb{F}_q$, and let f, $Z(f)$, and $\delta = \delta(f)$ be defined as above. We have:*

$$|Z(f)| = \delta \times |Z(a_1 + a_2x^{e_2/\delta} + \cdots + a_tx^{e_t/\delta}) \cap \langle g^\delta \rangle|,$$

where $\langle g^\delta \rangle$ denotes the subgroup generated by g^δ.

For example, consider the trinomial $f(x) = x^{800} - 2x^{400} + 1 = (x^{400} - 1)^2$ over $\mathbb{F}_{1201}$. Since the mapping $\phi(x) = x^{400}$ sends 400 elements to 1, $f(x) \equiv 0 \mod 1201$ has 400 solutions. Similarly, $Z(x^2 - 2x + 1) \cap \langle g^{400} \rangle = Z((x-1)^2) \cap \langle g^{400} \rangle = \{1\}$, and the pre-image $\phi^{-1}(1)$ has 400 elements.

This lemma is useful because it allows us to restrict our attention to $f \in \mathbb{F}_q$ with $\delta(f) = 1$. [1] This is because the number of roots of a $\delta > 1$ polynomial can be expressed in simple terms of the number of its corresponding $\delta = 1$ polynomial. Below we present the upper bound from [2] for the trinomial case.

Theorem 1.2 ([2])**.** *Let $f(x) = x^n + ax^s + b \in \mathbb{F}_q$ and suppose $\delta(f) := gcd(n, s, q-1) = 1$. Then:*

$$|Z(f)| \leq 2\sqrt{q-1}.$$

However, this bound appears to be far from optimal in the case of prime fields. Let R_p denote the maximum value of $|Z(f)|$ over all trinomials in $\mathbb{F}_p[x]$ with $\delta(f) = 1$. In [2], R_p is computed for all primes ≤ 16633, and they find no cases in which R_p exceeds $1.77 \log p$. As a result of a large-scale computation, we observe that the inequality $R_p \leq 1.77 \log p$ continues to hold for all primes ≤ 139571.

[1] Actually, for convenience we may further restrict our attention to polynomials with $d := gcd(e_1, \ldots, e_t) = 1$. This is because $\delta = gcd(d, q-1)$, so when $\delta = 1$, the map $x \to x^d$ is a bijection. Therefore $|Z(a_1 + a_2x^{e_2} + \cdots + a_tx^{e_t})| = |Z(a_1 + a_2x^{e_2/d} + \cdots + a_tx^{e_t/d})|$.

It is known that if f is a general polynomial over $\mathbb{F}_p$ with coefficients chosen from a uniform random distribution on $\mathbb{F}_p$, The size of f's zero-set is Poisson-distributed with mean 1 (for p sufficiently large) [8]. We might wonder if the same is true for sparse polynomials with $\delta = 1$. In other words, maybe it is the case the number of roots and the number of terms are in fact uncorrelated properties of $\delta = 1$ polynomials. If this were the case, we would able to readily explain the logarithmic growth of R_p by considering its expected value.

Since $\delta > 1$ polynomials are relatively rare, there are roughly p^{2t} polynomials of the form $f(x) = a_1 + a_2x^{e_2} + \cdots + a_tx^{e_t}$ with $\delta(f) = 1$ in $\mathbb{F}_p[x]$. Suppose for such f that $|Z(f)|$ has a discrete Poisson distribution. Then, the number of $\delta = 1$ t-nomials that have r roots is

$$\frac{e^{-1}}{r!}p^{2t}.$$

Therefore we expect that the maximum value of $|Z(f)|$ is r such that this value is equal to one:

$$\begin{aligned} 1 &= \frac{e^{-1}}{r!}p^{2t}, \\ r! &= e^{-1}p^{2t}, \\ \log r! &= -1 + 2t\log p. \end{aligned}$$

Since $r < \log r!$ when $r \geq 6$, we get:

$$r = O(\log r!) = O(t\log p).$$

In Section 2, we present computational evidence suggesting that:

- For $\delta = 1$ trinomials, the number of roots is Poisson-distributed when p is large.
- $\log r! \sim 2\log p$.

In section 3, we prove the following weaker version of the Poisson conjecture for trinomials, where we allow $\mathbb{F}_p$ to vary and assume the Generalized Riemann Hypothesis.

Theorem 1.3. *Assume GRH. Fix r, s, and n in $\mathbb{N}$ with $r \leq n$, $s < n-1$, and $gcd(n,s) = 1$. Let $P(M) := \{p \text{ prime} : p \leq M\}$. Consider all possible triples (p,a,b) with $p \in P(M)$ and $(a,b) \in (\mathbb{F}_p^* \times \mathbb{F}_p^*)$. For M sufficiently large, the proportion of these triples in which $f(x) = x^n + ax^s + b \in \mathbb{F}_p[x]$ has r roots is*

$$\frac{\hat{e}^{-1}}{r!},$$

where $\hat{e}$ is an approximation of e satisfying

$$\begin{cases} 1 \leq \hat{e}^{-1} \leq 2 & \text{if } r = n \\ \left|\hat{e}^{-1} - e^{-1}\right| < \dfrac{(n-r)}{(n-r)!} & \text{if } r < n. \end{cases}$$

Clearly $\hat{e}$ is a very accurate approximation of e whenever r is not too close to n. Therefore it is interesting to note that the proportion of trinomials of the form $x^n + ax^s + b$ having a specified number of roots is essentially independent of the degree, n.

2. Experimental Results

We have computed R_p, the maximum number of roots of any $\delta = 1$ trinomial in $\mathbb{F}_p$, for primes up to $p = 139,571$. In this section, we show that the results of this computation can be very accurately "predicted" under the assumption of the Poisson conjecture for trinomials. First however, we present this table, which compares the fraction of $\delta = 1$ trinomials with r roots in $\mathbb{F}_p$ with $e^{-1}/r!$ by listing the ratio of these two numbers. In an attempt to give a non-exceptional set of examples with varying sizes, we present the least prime above each power of 10.

r	$\mathbb{F}_{11}$	$\mathbb{F}_{101}$	$\mathbb{F}_{1009}$	$\mathbb{F}_{10007}$	$\mathbb{F}_{100003}$
0	0.80542	0.96272	0.98994	0.99953	0.99992
1	1.30880	1.04967	1.00896	1.00092	1.00008
2	0.80542	0.98961	1.01254	0.99937	1.00006
3	1.20813	1.00563	0.99323	0.99900	0.99994
4	0	0.98847	0.93526	0.99970	0.99962
5	0	0.27457	0.89177	1.00091	0.99912
6	0	0	0.73561	1.02570	0.99834
7	0	0	0.67754	1.00700	1.00276
8	0	0	0.21681	0.97258	0.99280
9	0	0	0	0.86743	1.00713
10	0	0	0	1.18286	0.91540
11	0	0	0	4.33717	0.88975
12	0	0	0	0	1.04166
13	0	0	0	0	0

In full generality, $\delta = 1$ trinomials have the form $ax^n + bx^s + c$. However, trinomials that differ by a constant factor clearly have the same number of roots, so we will instead consider the normalized form $f(x) = \alpha x^n + \beta x^s + 1$. In this section, we will fix $\mathbb{F}_p$ and suppose that the number roots of $f \in \mathbb{F}_p[x]$ follows a Poisson distribution (with mean 1) as the parameters α, β, n, and s range over their possible values. We have $(p-1)^2$ choices for the two coefficients (because $\alpha = 0$ or $\beta = 0$ means f is not a trinomial) and almost $(p-1)^2/2$ choices of exponents (since we do not count pairs with $\delta(f) = gcd(n, s, p-1) > 1$). The factor of $1/2$ is present because we do not want to double-count isomorphic exponent patterns; we will make the restriction $n > s$.

The exact number of pairs (n, s) that are relatively prime with $p-1$ is given by the *Jordan totient function*, $J_2(p-1)$ [5]. So overall, we are considering a Poisson distribution of $(p-1)^2 J_2(p-1)/2$ discrete elements. Normally, we would expect R_p to be the maximum choice of r so that

$$\frac{e^{-1}}{r!} \frac{(p-1)^2 J_2(p-1)}{2} \geq 1,$$

however the actual situation is slightly more delicate. It is not actually possible for only one of trinomials in $\mathbb{F}_p[x]$ to have a given number of roots. Given any $f(x) = \alpha x^n + \beta x^s + 1$, there are a number of possible transformations we can make that yield a different trinomial with the same number of roots, namely $x \to \lambda x$ and $x \to x^e$ (where $gcd(e, p-1) = 1$). Since these mappings are bijective, any

$g_\lambda(x) = \alpha\lambda^n x^n + \beta\lambda^s x^s + 1$ or $g_e(x) = \alpha x^{en} + \beta x^{es} + 1$ has the same number of roots as f.

Since $gcd(n, s, p-1) = 1$, every pair (λ^n, λ^s) will in fact be distinct, so there are $(p-1)$ transformations of this type that preserve root number. Additionally, there are $\varphi(p-1)$ transformations $x \to x^e$ that preserve the root number. In existence of these transformations means that we are still over-counting in a sense, because if there is any trinomial with r roots then there is at least $(p-1)\varphi(p-1)$ of them. Therefore our refined prediction for R_p is r such that

$$\frac{e^{-1}}{r!}\frac{(p-1)^2 J_2(p-1)}{2} = (p-1)\varphi(p-1),$$

or, equivalently,

$$(r!)(e) = \frac{(p-1)J_2(p-1)}{(2)\varphi(p-1)}.$$

By writing the totient functions in their product forms, we can simplify further:

$$\frac{J_2(p-1)}{\varphi(p-1)} = \frac{(p-1)^2(\prod_{q|(p-1)} 1 - 1/q^2)}{(p-1)(\prod_{q|(p-1)} 1 - 1/q)} = (p-1)\prod_{q|(p-1)} \frac{1-(1/q)^2}{1-(1/q)} = (p-1)\prod_{q|(p-1)} (1+1/q).$$

Continuing the prediction, we have:

$$(r!)(e) = (p-1)^2\frac{1}{2}\prod_{q|(p-1)} (1+1/q),$$

$$\log r! + 1 = 2\log(p-1) - \log(2) + \sum_{q|(p-1)} \log(1+1/q).$$

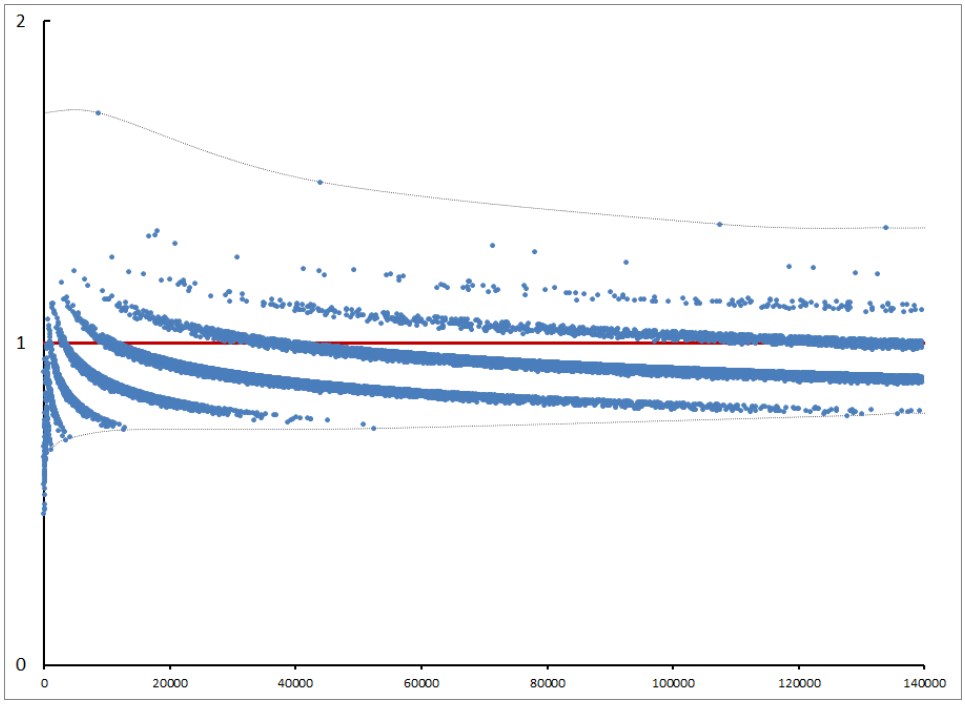
Even assuming the Poisson conjecture, we only expect these quantities to be approximately equivalent when $\mathbb{F}_p$ is sufficiently large. In other words, the actual prediction is:

$$\log(R_p!) + 1 \sim 2\log(p-1) - \log(2) + \sum_{q|(p-1)} \log(1+1/q),$$

Or, equivalently,

$$\lim_{p\to\infty}\left(\frac{\log(R_p!)+1}{2\log(p-1) - \log(2) + \sum_{q|(p-1)}\log(1+1/q)}\right) = 1.$$

The following graph displays the actual values of this function of p for all $p \leq 139,571$, which we believe constitutes strong evidence for the Poisson conjecture.



3. Proof of Theorem 1.3

For the proof of theorem 1.3, we will need the following special case of Chebotarev's density theorem.

Theorem 3.1. [13] *Suppose that $f(x) \in \mathbb{Z}[x]$ has a non-zero discriminant, and let $Gal(f)$ denote the Galois group of the splitting field of f over $\mathbb{Q}$. Let C_r contain all the permutations $\sigma \in Gal(f)$ that have exactly r fixed points. As usual, let $\pi(M)$ denote the number of primes $p \leq M$, and define $\pi_r(M)$ to be the number of these primes where $(f \mod p)$ has r roots in $\mathbb{F}_p$. Then:*

$$\lim_{M\to\infty} \frac{\pi_r(M)}{\pi(M)} = \frac{|C_r|}{|Gal(f)|}.$$

By far, the most common Galois groups to encounter are the entire symmetric group (S_n) and the alternating group (A_n). In both of these cases, the size of C_r is approximately Poisson-distributed over the values of r.

Proposition 3.2. *Suppose $A_n \subseteq Gal(f)$. Then:*

$$\begin{cases} \frac{1}{r!} \leq \frac{|C_r|}{|Gal(f)|} \leq \frac{2}{r!} & \text{if } r = n \\ \left| \frac{|C_r|}{|Gal(f)|} - \frac{e^{-1}}{r!} \right| < \frac{1}{r!} \frac{(n-r)}{(n-r)!} & \text{if } r < n \end{cases}$$

Clearly this is true for $r = n$, since C_r contains just the identity, the only permutation that fixes every point. The $r < n$ case can seen by considering the cycle shape of any $\sigma \in C_r$.

Since σ has exactly r fixed points, it looks like $\sigma = c_1c_2\cdots c_r\sigma_d$, where each c_i is a length-one cycle and σ_d permutes the remaining elements and has no fixed points. Permutations that have no fixed points are called *derangements*, and the proportion of permutations that are derangements is extremely well-approximated by e^{-1} [7]. Specifically, the number of derangements of k elements, d_k, satisfies

$$|d_k - e^{-1}k!| < \frac{1}{k}.$$

Furthermore, the number of derangements in the alternating group, d_k^*, satisfies $|2d_k^* - d_k| = k - 1$ [1], so we also have

$$|2d_k^* - e^{-1}k!| < k.$$

Therefore, to count the the number of σ that have cycle shape $\sigma = c_1c_2\cdots c_r\sigma_d$, we simply count the ways to chose $c_1, c_2, \ldots, c_r$ and multiply by the number of derangements of the remaining $n - r$ elements. Below, $\epsilon(x)$ denotes a real number bounded above by x.

$$\frac{|C_r|}{|S_n|} = \frac{\binom{n}{r}d_{n-r}}{n!} = \frac{\frac{n!}{r!(n-r)!}d_{n-r}}{n!} = \frac{e^{-1}(n-r)! \pm \epsilon(\frac{1}{n-r})}{r!(n-r)!} = \frac{e^{-1}}{r!} \pm \epsilon\left(\frac{1}{(n-r)!}\right).$$

$$\frac{|C_r|}{|A_n|} = \frac{\binom{n}{r}d_{n-r}^*}{n!/2} = \frac{\frac{n!}{r!(n-r)!}2d_{n-r}^*}{n!} = \frac{e^{-1}(n-r)! \pm \epsilon(n-r)}{r!(n-r)!} = \frac{e^{-1}}{r!} \pm \epsilon\left(\frac{(n-r)}{(n-r)!}\right).$$

So, for any polynomial that has a Galois group at least as big as A_n, we have that $\lim_{M\to\infty}(\frac{\pi_r(M)}{\pi(M)}) \approx \frac{e^{-1}}{r!}$, where the accuracy of the approximation satisfies the requirements of theorem 1.3.

To prove theorem 1.3, we will find a set of integer pairs $(A \times B) \subset (\mathbb{Z} \times \mathbb{Z})$ that simultaneously possesses two useful properties:

(1) For any $(a, b) \in A \times B$, $Gal(x^n + ax^s + b) \cong S_n$ or A_n.
(2) For any prime p, the members of A and B are evenly distributed among the (non-zero) residue classes mod p.

Clearly, it would be convenient to restrict our attention to coefficients from this set due to the first property. However, the second property is necessary to ensure that proportional statements about pairs in $(A \times B)$ are also valid for pairs in $(\mathbb{F}_p^* \times \mathbb{F}_p^*)$, which is what we actually want to know about. Thereom 1.3 obviously follows quickly from the existence of such a set, since, by proposition 3.2, all pairs have essentially the same behavior. As we will see, A and B can simply be taken to be large sets of primes numbers.

Proposition 3.3. *Let $s, n, q_a, q_b \in \mathbb{N}$, where*

- *q_a and q_b are primes.*
- *$gcd(n, s) = 1$.*
- *$s + 1 < n < q_a < q_b$.*

Then, for $f(x) = x^n + q_ax^s + q_b$, $Gal(f)$ is either S_n or A_n.

The constant of f term is prime and larger than the sum of its other coefficients, so f is irreducible [11]. Since f is irreducible, this proposition follows as a special case of theorem 1.2 of [4]. Also note that because the large size of $Gal(f)$, it is not possible for f to have any repeated roots in $\mathbb{C}$ (that is, the discriminant of f is non-vanishing). This is because the Galois group is a collection of permutations

of distinct roots of f, so $Gal(f)$ could have at most $(n-1)!$ elements if f had a repeated root. As a consequence of this proposition, a set $Q_a \times Q_b$ containing pairs of primes $q_a < q_b$ satisfies the first property that we want. To measure the extent to which the set satisfies the second property, we define the following formalism.

Definition 3.4. Let S be a finite set of integers, and consider a particular prime field $\mathbb{F}_p$. Let S_c denote $\{s \in S \ : \ s \equiv c \mod p\}$. We define the *Bias of S mod p* as follows:

$$B(S : \mathbb{F}_p) = \max_{c \in \mathbb{F}_p^*} \Big| \frac{|S_c|}{|S|} - \frac{1}{|\mathbb{F}_p^*|} \Big|.$$

For example, if a set S has exactly the same number of elements in each non-zero residue class mod p, we have $B(S : \mathbb{F}_p) = 0$. Let $Q(N)$ denote the set of primes $q \leq N$. Due to Dirichlet's theorem for the density of primes in arithmetic sequences [13], we have the amazing fact that, for any choice of $\mathbb{F}_p$, $B(Q(N) : \mathbb{F}_p) \to 0$ as $N \to \infty$. Therefore it seems likely that $Q_a \times Q_b$ also satisfies the second property as well, provided that it is large enough.

However, at this point the entire argument has a major structural problem. We would like to apply theorem 3.1 to every trinomial $x^n + q_a x^s + q_b$, which requires us to let $P(M)$ be sufficiently large. But, for every $p \in P(M)$, we must let that Q_a and Q_b be large enough so that their bias mod p is sufficiently small, forcing us to consider even more trinomials. It is not possible to compose these classical density theorems in a way that we can consider the limit of both structures at once; we will need to apply effective versions of them with explicit error terms.

We stress that this is not simply a technical detail - the two theorems actually have conflicting convergence conditions. As we will see, $|C_r|/|Gal(f)$ tends to be a good approximation of $\pi_r(M)/\pi(M)$ only when the coefficients of f are small enough, but we must let Q_a and Q_b be big enough to control their bias. This is why we must assume the Generalized Riemann Hypothesis, so that we can control the error term in the effective versions of these theorems simultaneously.

Theorem 3.5. [10]
Let $Q(N) = \{q \text{ prime } : \ N < q \leq 2N\}$. If $N = N(M) \geq M^{40}$, Then:

$$\sum_{p \in P(M)} B(Q(N) : \mathbb{F}_p) = O\left(\frac{1}{\log N}\right).$$

This is an interval version of the Bombieri-Vinogradov theorem, presented in terms of our bias notation. We use an interval version so we can ensure that $n < q_a < q_b$, which we need to utilize proposition 3.3. We can finally give an explicit description of $(Q_a \times Q_b)$: Let $Q_a = Q(M^{40})$ and $Q_b = Q(2M^{40})$. By taking M sufficiently large, we can make the bias of Q_a and Q_b arbitrarily small, and therefore $(Q_a \times Q_b)$ does in fact have the property that its elements are evenly distributed among non-zero residue classes mod any prime p.

Theorem 3.6. [6] [12]
Assume GRH. Suppose $f(x) \in \mathbb{Z}[x]$ has a non-zero discriminant. Let d_L denote the absolute field discriminant of L, the splitting field of f. Then, for some absolute constant c_0,

$$\Big| \frac{\pi_r(M)}{\pi(M)} - \frac{|C_r|}{|Gal(f)|} \Big| \leq c_0 \frac{|C_r|}{|Gal(f)|} \frac{\sqrt{M}}{Li(M)} (\log d_L + deg(f) \log M).$$

It is crucial to get a bound on this error term that does not depend on the specific coefficients of f, so that we can apply the theorem to all trinomials $f(x) = x^n + q_a x^s + q_b$ at once. First, by proposition 3.2, we have that $\frac{|C_r|}{|Gal(f)|} \leq \frac{2}{n!}$ in any case. All that is left is to find a bound for $\log d_L$ in terms of M. Consider this slightly relaxed version of the upper bound for d_L used in [3]: $d_L \leq disc(f)^{(n^n)}$. By combining this with Mahler's bound for polynomial discriminants [9], we have

$$\log d_L \leq \log(disc(f)^{(n^n)}) < n^{n+1} \log(n(1 + q_a + q_b)).$$

Since $q_a \leq 2M^{40}$ and $q_b \leq 4M^{40}$,

$$\log d_L < n^{n+1} \log(n7M^{40}) < 40n^{n+1}(\log 7n + \log M).$$

Therefore, we have an overall bound for the error term that holds generally for all $(q_a, q_b) \in (Q_a \times Q_b)$:

$$\Big|\frac{\pi_r(M)}{\pi(M)} - \frac{|C_r|}{|Gal(f)|}\Big| \leq c_0 \frac{2}{n!} \frac{\sqrt{M}}{Li(M)} (40n^{n+1}(\log 7n + \log M) + n \log M) = O\left(\frac{\sqrt{M} \log M}{Li(M)}\right).$$

It is well known that $Li(M) \sim M/\log M$, so we conclude with

$$\Big|\frac{\pi_r(M)}{\pi(M)} - \frac{|C_r|}{|Gal(f)|}\Big| = O\left(\frac{\sqrt{M}(\log M)^2}{M}\right) = O\left(\frac{(\log M)^2}{\sqrt{M}}\right).$$

In summary, by taking M to be large enough, it is possible to (simultaneously)

(1) make $\left|\frac{\pi_r(M)}{\pi(M)} - \frac{|C_r|}{|Gal(f)|}\right|$ arbitrarily small for every (q_a, q_b), and
(2) make $B(Q_a, \mathbb{F}_p)$ and $B(Q_b, \mathbb{F}_p)$ arbitrarily small for every $\mathbb{F}_p$.

By considering the estimate of $|C_r|/|Gal(f)|$ given by proposition 3.2, we get the desired result. In particular, we see that the proportion of triples $(p, q_a, q_b) \in (P(M) \times Q_a \times Q_b)$, in which $(x^n + q_a x^s + q_b \mod p)$ has r roots in $\mathbb{F}_p$, is approximately $\frac{e^{-1}}{r!}$, with the desired amount of accuracy. Because the bias of Q_a and Q_b can be made arbitrarily small, the same is true of the proportion of triples of the form $(p, a, b) \in (P(M) \times \mathbb{F}_p^* \times \mathbb{F}_p^*)$.

References

[1] Ali, Bashir, and A. Umar. "Some Combinatorial Properties of the Alternating Group." Southeast Asian Bulletin of Mathematics 32.5 (2008).

[2] Bi, Jingguo, Qi Cheng, and J. Maurice Rojas. "Sub-Linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields." proceedings of ISSAC (International Symposium on Symbolic and Algebraic Computation, June 26-29, Boston, MA), pp. 61-68, ACM Press, 2013.

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

[4] Cohen, S. D., A. Movahhedi, and A. Salinier. "Galois groups of trinomials." Journal of Algebra 222.2 (1999): 561-573.

[5] Dickson, Leonard E. *History Of The Theory Of Numbers*. pp. 147, New York, Chelsea Pub. Co, 1966.

[6] Lagarias, Jeff and Odlyzko, Andrew, "Effective Versions of the Chebotarev Density Theorem." Algebraic Number Fields: L-functions and Galois Properties (Proc. Sympos. Univ. Durham, Durham, 1975), 409-464, Academic Press, London, 1977.

[7] Mehdi Hassani, "Derangements and Applications." Journal of Integer Sequences, 6(1), Article 03.1.2, 2003.

[8] Leont'ev, Vladimir Konstantinovich."Roots of random polynomials over a finite field." Mathematical Notes 80.1 (2006): 300-304.

[9] Mahler, Kurt. "An inequality for the discriminant of a polynomial." The Michigan Mathematical Journal 11.3 (1964): 257-262.
[10] Perelli, A., J. Pintz, and S. Salerno. "Bombieri's theorem in short intervals. II." Inventiones mathematicae 79.1 (1985): 1-9.
[11] Prasolov, Viktor V, and D A. Leites. *Polynomials*. pp. 58, Berlin: Springer, 2010.
[12] Serre, Jean-Pierre. "Quelques applications du thoreme de densit de Chebotarev." Publications Mathmatiques de l'IHS 54 (1981): 123-201.
[13] Stevenhagen, Peter, and Hendrik Willem Lenstra. "Chebotarv and his density theorem." The Mathematical Intelligencer 18.2 (1996): 26-37.