ON THE PRIME SELMER RANKS OF CYCLIC PRIME TWIST FAMILIES OF ELLIPTIC CURVES OVER GLOBAL FUNCTION FIELDS

SUN WOO PARK

Abstract. Fix a prime number \( p \). Let \( \mathbb{F}_q \) be a finite field of characteristic coprime to 2, 3, and contains the primitive \( p \)-th root of unity \( \mu_p \). Based on the works by Swinnerton-Dyer and Klagsbrun, Mazur, and Rubin, we prove that the probability distribution of the sizes of prime Selmer groups over a family of cyclic prime twists of non-isotrivial elliptic curves over \( \mathbb{F}_q(t) \) satisfying a number of mild constraints conforms to the distribution conjectured by Poonen and Rains with explicit error bounds. The key tools used in proving these results are the Riemann hypothesis over global function fields, the Erdös-Kac theorem, and the geometric ergodicity of Markov chains.

Contents

1. Introduction 1
2. Remarks and Outlines 4
   2.1. Key Ingredients 4
   2.2. Outline of the proof 4
   2.3. Relevant works 5
3. Effective theorems from the Riemann hypothesis 7
   3.1. Effective Chebotarev density theorem 7
   3.2. Erdös-Kac Theorem 8
4. Splitting partitions of polynomials 9
   4.1. Some sets of places 9
   4.2. Splitting partition of polynomials over finite fields 10
   4.3. Equidistribution of local characters 14
5. Local Selmer groups 16
   5.1. Local twists 17
   5.2. Auxiliary places 21
6. Global Selmer groups 28
   6.1. Governing Markov operator 28
   6.2. Relating global and local Selmer groups 31
Acknowledgements 35
References 36

1. Introduction

Let \( p \) be a fixed prime number. Let \( \mu_p \) be the set of primitive \( p \)-th roots of unity. We fix an element \( \zeta_p \) which generates \( \mu_p \). Let \( K \) be the global function field \( \mathbb{F}_q(t) \) of characteristic coprime to 2 and 3 which contains \( \mu_p \), i.e. \( q \equiv 1 \mod p \). Let \( F_n(\mathbb{F}_q) \) be the set of monic polynomials of degree \( n \) over \( \mathbb{F}_q \).

Key words and phrases. Elliptic curves, Weil restrictions, Selmer groups, Global function fields, Markov processes.
Given a polynomial $f \in F_n(\mathbb{F}_q)$, there is a cyclic order-$p$ Galois extension $L_f := K(\sqrt[p]{f})$ over $K$. Choose a generator $\sigma_f$ of the cyclic Galois group $\text{Gal}(K(\sqrt[p]{f})/K) \cong \mathbb{Z}/p\mathbb{Z}$. We may associate the field $L_f$ with a cyclic order-$p$ character $\chi_f \in \text{Hom}(\text{Gal}(K/K), \mu_p)$ defined via the quotient map

$$\chi_f : \text{Gal}(\overline{K}/K) \twoheadrightarrow \text{Gal}(L_f/K) \to \mu_p$$

that maps $\sigma_f$ to $\zeta_p \in \mu_p$. Note that $L_f$ is the fixed field of $\text{Ker}(\chi_f)$ in $\overline{K}$.

Fix a non-isotrivial elliptic curve $E$ over $K$. The goal of this manuscript focuses on understanding the following question.

**Question 1.1.** Compute $\text{rank}_\mathbb{Z} E(L_f) - \text{rank}_\mathbb{Z} E(K)$ for any $f \in F_n(\mathbb{F}_q)$.

We study the question above by constructing what we call the cyclic order-$p$ Selmer group of elliptic curves for some prime number $p$. We elaborate on the statement of the conjecture. We first compute the probability distribution of Selmer groups over the set of finitely many elliptic curves $y^2 = x^3 + Ax + B$ whose coefficients $A, B \in K$ have bounded height $\mathcal{B}$. The conjecture states that the limit of the probability distribution obtained from letting $\mathcal{B}$ to grow arbitrarily large can be explicitly determined.
In this manuscript, we focus on computing the dimension of the following family of $\pi$-Selmer groups of $E^{x_f}$, defined as

$$\text{Sel}_\pi(E^{x_f}) := \text{Ker} \left( H^1_{\text{ét}}(K, E[p]) \to \prod_{v\text{ place of } K} H^1_{\text{ét}}(K_v, E^{x_f}[^p]) \right),$$

where we use the $\text{Gal}(\overline{K}/K)$-equivariant isomorphism $E^{x_f}[\pi] \cong E[p]$ to identify $H^1_{\text{ét}}(K, E^{x_f}[\pi]) \cong H^1_{\text{ét}}(K, E[p])$. The main theorem of this paper confirms the Poonen-Rains heuristics for these families of $\pi$-Selmer groups of $E^{x_f}$. We use the following abbreviation to denote the probability distribution of dimensions of $\text{Sel}_\pi(E^{x_f})$ ranging over $f \in F_n(\mathbb{F}_q)$.

$$\mathbb{P} \left[ \dim_{\mathbb{F}_p} \text{Sel}_\pi(E^{x_f}) = j \mid f \in F_n(\mathbb{F}_q) \right] := \frac{\#\{f \in F_n(\mathbb{F}_q) \mid \dim_{\mathbb{F}_p} \text{Sel}_\pi(E^{x_f}) = j\}}{\#F_n(\mathbb{F}_q)} \quad (5)$$

**Theorem 1.2. Main Theorem.** Fix a prime number $p$. Let $K = \mathbb{F}_q(t)$ be a global function field whose characteristic is coprime to 2,3, and $q \equiv 1 \mod p$. Let $E : y^2 = F(x) = x^3 + Ax + B$ be an elliptic curve over $K$ which satisfies the following conditions.

1. $E$ is non-isotrivial.
2. $E$ contains a place of split multiplicative reduction.
3. The Galois group $\text{Gal}(\overline{K(E[p])}/K)$ is isomorphic to $\text{SL}_2(\mathbb{F}_p)$.

Let $\alpha(p)$ be a constant defined as

$$\alpha(p) := \sup_{0 < \rho < 1} \left( \min \left( \rho \log \rho + 1 - \rho, -\rho \log \left( 1 - \frac{p}{p^2 - 1} \right), -\rho \log \left( \frac{p}{p^2 - 1} \right) \right) \right)$$

Then for any small $\delta > 0$, there exist sufficiently large $n$ and a fixed constant $A_{E,p,q} > 0$ that depends only on $E$, $p$, and $q$ such that

$$\left| \mathbb{P} \left[ \dim_{\mathbb{F}_p} \text{Sel}_\pi(E^{x_f}) = j \mid f \in F_n(\mathbb{F}_q) \right] - \left( \prod_{m=0}^{\frac{1}{p^m}} \frac{1}{1 + p^{-m}} \right) \left( \prod_{m=1}^{j} \frac{p}{p^m - 1} \right) \right| < \frac{A_{E,p,q}}{n^{\alpha(p) - \delta}}$$

We hence obtain that under certain mild conditions, the distribution of 2-Selmer ranks of quadratic twist families of non-isotrivial elliptic curves $E$ conforms to the Poonen-Rains conjecture over any global function field $K = \mathbb{F}_q(t)$. The values of $\alpha$ for some values of $p = 2, 3, 5, 7$ are computed as below.

- $\alpha(2) \sim 0.185242$ where $\rho \sim 0.456864$. (Note that $1 - \frac{2}{2^2 - 1} = \frac{1}{3}$ whereas $\frac{2}{2^2 - 1} = \frac{2}{3}$)
- $\alpha(3) \sim 0.203893$ where $\rho \sim 0.433811$
- $\alpha(5) \sim 0.126457$ where $\rho \sim 0.541305$
- $\alpha(7) \sim 0.0943249$ where $\rho \sim 0.598398$.

**Remark 1.3.** The condition that $E$ is non-isotrivial further implies that condition (ii) in the statement of Theorem 1.2 can be obtained after taking a finite separable extension of any global function field $K = \mathbb{F}_q(t)$ [BLV09, Proposition 3.4].

As a corollary, we are able to obtain a partial answer to Question 1.1. We would like to thank Douglas Ulmer for enlightening discussions, from which an error of the previous version of the corollary was discovered.

**Corollary 1.4.** Assume the conditions and notations as in Theorem 1.2. We denote by

$$\mathbb{P} \left[ \text{rank}_\mathbb{Z} E(L^f) - \text{rank}_\mathbb{Z} E(K) = j \mid f \in F_n(\mathbb{F}_q) \right] := \frac{\#\{f \in F_n(\mathbb{F}_q) \mid \text{rank}_\mathbb{Z} E(L^f) - \text{rank}_\mathbb{Z} E(K) = j\}}{\#F_n(\mathbb{F}_q)}$$
Then for any non-negative integer \( j \geq 0 \), we have
\[
\lim_{n \to \infty} \mathbb{P} \left[ \text{rank}_\mathbb{Z} E(L^j) - \text{rank}_\mathbb{Z} E(K) \leq (p - 1) \cdot j \mid f \in F_n(\mathbb{F}_q) \right] \leq \sum_{j=0}^{\infty} \left( \prod_{m=0}^{J} \frac{1}{1 + p^{\chi(m)}} \right) \left( \prod_{m=1}^{J} \frac{p^m - 1}{p^m} \right)
\]

In particular, for sufficiently large \( p \), the rank of \( E(L^j) \) increases by at most \( p - 1 \) from the rank of \( E(K) \) for almost all \( f \in \mathbb{F}_q[t] \), and the rank of \( E(L^j) \) is identical to that of \( E(K) \) for at least approximately 50% of \( f \in \mathbb{F}_q[t] \).

Proof. The corollary follows from the proof of [MR07, Proposition 2.1, Proposition 6.3], where one uses the inequality \( \text{corank}_{\mathbb{Z}[\sigma]} \text{Sel}_{p^\infty}(E^j) \leq \dim_{\mathbb{Z}_p} \text{Sel}_p(E^j) \). \( \square \)

Remark 1.5. We warn the readers, however, that the given upper bound is not binding for any values of \( p \geq 3 \) unlike the case for quadratic twist families of elliptic curves. This is because the \( \pi \)-torsion subgroup of the Tate-Shafarevich group of the abelian variety \( E^j \) is not necessarily of an even dimension, as explicitly constructed by William Stein [Ste02] and discussed in detail by Howe [How01]. Specific conditions which can guarantee the Tate-shafarevich groups to be of even dimension are provided in [MR07, Chapter 6]. Indeed, there are conjectural statements by David, Fearnley, and Kisilevsky [DFK07] and Mazur and Rubin [MR23] who suggested that it is very unlikely that the ranks of the elliptic curves will increase by at least 1 with respect to cyclic order-\( p \) extensions over \( \mathbb{Q} \). The function field analogue was carefully studied in a recent work by Comeau-Lapointe, David, Lalin, and Li [CLDLL22], where they show that the conjecture fails for isotrivial cyclic twist families of elliptic curves, whereas numerical data suggests that the conjecture may hold for non-isotrivial cyclic twist families of elliptic curves.

2. Remarks and Outlines

2.1. Key Ingredients. The three key ingredients utilized in proving the main theorem are as follows, all three of which contribute to the three terms for \( \alpha(\rho) \) which determine the rate of convergence of the desired probability distribution to the Poonen-Rains distribution.

1. **Effective Chebotarev Density Theorem**
   - **Relevant results:** Theorem 3.1, Corollary 3.2, Corollary 4.16, Proposition 5.4
   - **Error term:** \( -\rho \log \left( \frac{p}{p^\chi - 1} \right) \), arising from the density that the Frobenius element of a place of \( K \) has order prime to \( p \) inside \( \text{Gal}(K(E[p])/K) \cong \text{SL}_2(\mathbb{F}_p) \).

2. **Effective Erdős-Kac Theorem**
   - **Relevant results:** Theorem 3.6, Proposition 4.13, Proposition 4.14
   - **Error term:** \( \rho \log \rho + 1 - \rho \), arising from the probability that a degree \( n \) polynomial has at least \( \rho \log n + \log \log q \) and at most \( 2(\log n + \log \log q) \) many distinct irreducible factors.

3. **Geometric Convergence of Markov Chains**
   - **Relevant results:** Corollary 6.7
   - **Error term:** \( -\rho \log \left( 1 - \frac{p}{p^\chi - 1} \right) \), arising from geometric rate of convergence of the constructed Markov chain to the stationary distribution.

2.2. Outline of the proof. We provide the outline of the proof of the main theorem along with the organization of this manuscript. We let \( \rho \) to be a parameter whose value is between 0 and 1. The motivation for the proof originates from the previous work by Swinnerton-Dyer [SD08] and Klagsbrun, Mazur, and Rubin [KMR14] who studied Lagrangian Markov operators over \( \mathbb{Z}_{\geq 0} \) which govern the distribution of dimensions of \( \pi \)-Selmer groups over number fields.

1. **Effective theorems:** In Section 3 we discuss the effective versions of Chebotarev density theorem and Erdős-Kac theorem used in the rest of the manuscript.
(2) Finding a nice subset of polynomials: Let \( f \in F_n(\mathbb{F}_q) \). Suppose that \( f \) admits a factorization \( f = f_1 \cdots f_m \), where \( f_i \) is a product of irreducible factors of \( f \) (including multiplicities) of degree greater than \( \frac{d(\log n)^2}{\log q} \). In Section 4.2 we define the notion of splitting partitions and show using Mertens’s theorem and the effective Erdős-Kac theorem that for almost all \( f \in F_n(\mathbb{F}_q) \) the following three conditions are satisfied:

- The number of distinct irreducible factors of \( f \) is between \( \rho(\log n + \log \log q) \) and \( 2(\log n + \log \log q) \).
- The number of distinct irreducible factors of \( f_i \) is at least \( (1 - \epsilon) \rho(\log n + \log \log q) \) for small enough \( \epsilon > 0 \).
- There is an irreducible factor of \( f_i \) whose Frobenius element in \( \text{Gal}(K(E[p])/K) \cong \text{SL}_2(\mathbb{F}_p) \) has order prime to \( p \).

(3) Equidistribution: In Section 4.3 we prove equidistribution of \( l \)-th power residue symbols associated to a fixed number of irreducible polynomials over \( \mathbb{F}_q \).

(4) Local Selmer groups: In Section 5.1 we recall the definition of local Selmer groups of \( E \) associated to cyclic order \( p \) local characters as shown in [KMR14]. We use the ideas from [KMR14, Proposition 9.4] and the effective Chebotarev theorem to identify Chebotarev conditions that govern the image of the global cohomology group \( H^1_{\text{ét}}(K, E[p]) \) with respect to the localization map at a place \( v \) of \( K \).

(5) Auxiliary Place: In Section 5.2 we define the notion of the auxiliary place of \( f \) satisfying the aforementioned three conditions, which is an irreducible factor of highest degree whose Frobenius element in \( \text{Gal}(K(E[p])/K) \cong \text{SL}_2(\mathbb{F}_p) \) has order prime to \( p \). Using the equidistribution results from Section 4.3 and the Chebotarev conditions from Section 5.1 we construct a Markov operator defined over \( \mathbb{Z}_{\geq 0} \) which governs the distribution of the dimensions of local Selmer groups of \( E \) associated to cyclic order \( p \) characters. This proves the effective version of the construction of governing Markov operators, as stated in [KMR14, Theorem 4.3, Theorem 9.5] and [SD08, Theorem 1].

(6) Lagrangian Markov operators: In Section 6.1 we analyze the stochastic properties of the governing Markov operator, such as its stationary distribution and effective rates of convergence.

(7) Combining all ingredients: In Section 6.2 we prove the main theorem by approximating the desired probability distribution with the distribution of dimensions of local Selmer groups over the set of polynomials satisfying the three aforementioned conditions from Section 4. Combined with the rate of convergence of the governing Markov operator from Section 6.1 we prove that each ingredient gives rise to the rate of convergence of the desired probability distribution to the Poonen-Rains distribution.

2.3. Relevant works. The statements of the Poonen-Rains conjecture are known for certain large families of elliptic curves, such as the universal family of elliptic curves ordered by height, or quadratic twist families of elliptic curves ordered by the norm of the twist.

Suppose \( K = \mathbb{Q} \). We list some previous studies which focused on computing the probability distribution of Selmer groups over certain families of elliptic curves.

- Bhargava and Shankar compute the first moments of 2,3,4 and 5-Selmer groups over the universal family of elliptic curves, see for example [BST15].
- Heath-Brown, Swinnerton-Dyer, and Kane compute the probability distribution of 2-Selmer groups over the quadratic twist families of elliptic curves with full 2-torsions and no cyclic subgroup of order 4 over \( \mathbb{Q} \) [HB91, SD08, Kan13].
- Klagsbrun, Mazur, and Rubin generalized the construction of Markov chains suggested by Swinnerton-Dyer [SD08] to compute the probability distribution of 2-Selmer groups over the quadratic twist families of elliptic curves with \( \text{Gal}(K(E[2])/K) = S_3 \). Note that the
elliptic curves are ordered in a non-canonical manner using Fan structures. They obtain the probability distribution of prime Selmer groups over non-canonically ordered cyclic order-$p$ twist families of elliptic curves with $\text{Gal}(K(E[p])/K) = SL_2(\mathbb{F}_p)$ as well [KMR14].

- Smith successfully calculates the probability distribution of 2-Selmer groups over quadratic twist families of elliptic curves of bounded height $H$ except for some cases where $E(2)(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. As the upper bound on the height $H$ grows to infinity, the error bounds of the probability distribution is given by an order of $O(e^{-c(\log \log \log H)^{i/3}})$ for some constant $c > 0$. Smith utilizes Markov chains which govern the variations of kernel ranks of alternating square matrices whose entries are values of the Cassels-Tate pairings. Note that the Markov chains Smith utilized are different from those constructed by Swinnerton-Dyer and Klagsbrun, Mazur, and Rubin [Smi17, Smi20, Smi22a, Smi22b].

- The Markov chains suggested by Smith can be utilized to prove the Cohen-Lenstra heuristics on $l^\infty$-torsion subgroups of class groups of cyclic $l$-extensions of $\mathbb{Q}$ (assuming the generalized Riemann hypothesis) [KP21], and Stevenhagen’s conjecture on the asymptotic behavior of the solubility of negative Pell equations [KP22].

Consider the case where $K = \mathbb{F}_q(t)$ is of characteristic coprime to 2 and 3. Previous studies computed the probability distribution of $p$-Selmer groups of families of elliptic curves over global function fields $\mathbb{F}_q(t)$ under different conditions. Denote by $\mathcal{M}_n(\mathbb{F}_q)$ a finite subfamily of elliptic curves $E$ over $\mathbb{F}_q(t)$ of a fixed height $n$. The height of an elliptic curve is determined by the degrees of coefficient terms of $E$. (Of course, the choice of the height depends on over which families of elliptic curves the probability distribution of $p$-Selmer groups is computed.)

Given a non-negative integer $j$, denote by $\mathbb{P}\left[\dim_{\mathbb{F}_p} \text{Sel}_p(E) = j \mid E \in \mathcal{M}_n(\mathbb{F}_q)\right]$ the probability that the dimensions of $p$-Selmer groups of finitely many elliptic curves of fixed height $n$ are equal to $j$. Below we list three probability distributions of $p$-Selmer groups of elliptic curves that can be computed over global function fields:

\begin{align*}
\lim_{n\to\infty} \mathbb{P}\left[\dim_{\mathbb{F}_p} \text{Sel}_p(E) = j \mid E \in \mathcal{M}_n(\mathbb{F}_q)\right] &= \text{ (6)} \\
\lim_{q\to\infty} \lim_{n\to\infty} \mathbb{P}\left[\dim_{\mathbb{F}_p} \text{Sel}_p(E) = j \mid E \in \mathcal{M}_n(\mathbb{F}_q)\right] &= \text{ (7)} \\
\lim_{n\to\infty} \lim_{q\to\infty} \mathbb{P}\left[\dim_{\mathbb{F}_p} \text{Sel}_p(E) = j \mid E \in \mathcal{M}(\mathbb{F}_q)\right] &= \text{ (8)}
\end{align*}

As before, we list some previous studies which focused on computing the desired probability distribution over $\mathbb{F}_q(t)$.

- For the second limit (large-height, then large-$q$ limit), Ho, Le Hung, and Ngo [QH14] compute the average size of 2-Selmer groups over the universal family of elliptic curves, whereas de Jong [dJ02] computes that of 3-Selmer groups over the same family.

- Feng, Landesman, and Rains [FLR23] prove that the third limit (large-$q$, then large-height limit) is equal to the Poonen-Rains distribution for any $m$-Selmer groups over universal families of elliptic curves, under the condition that $q$ is coprime to $2m$. They propose a Markov chain constructed from random kernel models, which governs the variation of $m$-Selmer groups over global function fields $\mathbb{F}_q(t)$. Using this Markov chain, they successfully prove the Poonen-Rains conjecture for $m$-Selmer groups of universal families of elliptic curves under the large $q$-limit.

- Landesman [Lan21] demonstrates that the third limit of the average size of $m$-Selmer groups of universal families of elliptic curves conforms to the Poonen-Rains conjecture.

- The average size of $p$-Selmer groups of quadratic twist families of non-isotrivial elliptic curves under the third limit is computed by the author of this paper and Wang [PW24].
The key ingredient behind computing these distributions is a careful and rigorous determination of images of monodromy over algebraic spaces whose geometric fibers parametrize $p$-Selmer groups over a prescribed family of elliptic curves, see for instance [4][1][6]. Theorem [2] proves that the first limit (large-height limit) is equal to the Poonen-Rains distribution for $p = 2$ over quadratic twist families of elliptic curves.

Remark 2.1. We finally note that it is not always the case that the probability distribution of 2-Selmer groups over quadratic twist families of elliptic curves over a global field $K$ can be formulated. Wang extends their results to global function fields $K = \mathbb{F}_q(t)$ in his Ph.D. thesis for arbitrary number of elements of the constant field $\mathbb{F}_q$ [Wan21].

3. Effective theorems from the Riemann hypothesis

We review some of the preliminary results on global function fields $K$ which will be utilized in computing the probability distribution of prime Selmer groups associated to cyclic prime twists of elliptic curves. Given a place $v$ over $K$, we denote by $\text{Frob}_v$ the Frobenius element at $v$. Denote by $g_L$ the genus of a finite separable field extension $L/K$.

3.1. Effective Chebotarev density theorem. The effective version of Chebotarev density theorem over global function fields can be formulated as follows:

**Theorem 3.1 (Effective Chebotarev density theorem).** [4][1][8] Proposition 6.4.8

Let $L/K$ be a Galois extension of global function fields over $\mathbb{F}_q(t)$. Pick a conjugacy class $C \subset G = \text{Gal}(L/K)$. If the constant fields of $L$ and $K$ are both equal to $\mathbb{F}_q$, then

$$\left| \text{\#\{v a place over K | \text{Frob}_v \in C, \text{dim}_{\mathbb{F}_q}(O_K/v) = n\}} \right| - \frac{|C|q^n}{|G|n}$$

$$\leq \frac{2|C|}{n|G|} \left[ (|G| + g_L)q^{\frac{n}{2}} + |G|(2g_K + 1)q^{\frac{n}{2}} + (|G| + g_L) \right]$$

The constraint that the constant fields of $L$ and $K$ are identical allows one to reconstruct an analogue of the Chebotarev density theorem with explicit error bounds for function fields. Suppose the constant field of $L$, say $\mathbb{F}_{q'}$, is a non-trivial extension of the constant field $\mathbb{F}_q$ of $K$. Then to compute the equation stated in Theorem 3.1 one is required to compare whether the restriction of the conjugacy class $C$ to $\text{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q)$ agrees with the $n$-th power of the arithmetic Frobenius $\tau : x \mapsto x^q$ as a cyclic generator of $\text{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q)$. If not, then there are no places of degree $n$ whose Frobenius element lives inside the conjugacy class $C$. Note that the secondary error term is of $O(q^{\frac{n}{2}})$, which is obtained from the validity of the generalized Riemann hypothesis over $K = \mathbb{F}_q(t)$. For the analogous effective statements over number fields, see for example [LO75]. We note that Galois extensions of global function fields with non-trivial constant field extensions also satisfy the following equation:

$$\lim_{s \to 1^+} \sum_{v \text{ a place over K}} \frac{\text{\#\{O_K/v\}^{-s}}}{\text{\#\{O_K/v\}^{-s}}} = \frac{|C|}{|G|}$$

where $s \to 1^+$ implies that $s$ approaches 1 from above over the real values.

Using the explicit bounds obtained above, the density theorem can be obtained for any two conjugacy classes of the Galois group of the extension $L/K$ of function fields.
Corollary 3.2. Let $L/K$ be a Galois extension of global function fields over $\mathbb{F}_q(t)$. Pick two non-empty subsets $S, S' \subset G = \text{Gal}(L/K)$ stable under conjugation. Suppose the following two conditions hold.

1. The constant fields of $L$ and $K$ are both equal to $\mathbb{F}_q$.
2. The size of the constant field $q$ satisfies

$$q^{\frac{n}{2}} - q^{\frac{n}{2}} > 2(|G| + g_L + 2g_K)$$

Then the following inequality holds.

$$|\{v, \text{ a place over } K | \text{Frob}_v \in S, \dim_{\mathbb{F}_q}(\mathcal{O}_K/v) = n\} - |S| |\{v, \text{ a place over } K | \text{Frob}_v \in S', \dim_{\mathbb{F}_q}(\mathcal{O}_K/v) = n\} - |S'|| \leq 4\frac{|S|}{|S'|}(|G| + g_L + 2g_K) \left[\frac{1}{q^{\frac{n}{2}} - q^{\frac{n}{2}} - 2(|G| + g_L + 2g_K)}\right]$$

In particular, if $n \geq 2\log \frac{\log(|G| + g_L + 2g_K)}{\log q}$, then

$$\left|\frac{|S|}{|S'|} - 1\right| < 16\frac{|S|}{|S'|}(|G| + g_L + 2g_K)q^{-\frac{n}{2}}$$

Remark 3.3. We note that Deligne’s proof of the Weil conjectures determines the error bounds of the effective Chebotarev density theorem. We refer to [Ros02, Theorem 9.13B] for further discussions.

3.2. Erdös-Kac Theorem. Let $m$ be an integer. We denote by $w(m)$ the number of distinct irreducible factors of $m$. The Erdös-Kac Theorem states that the normal order of $w(m)$ is $\log \log m$.

Definition 3.4. From this section and onwards, given two positive integers $n$ and $q \geq 5$, we denote by $m_{n,q}$ the quantity

$$m_{n,q} := \log n + \log \log q \quad (10)$$

The Erdös-Kac Theorem over global function fields $K$ can be formulated as follows.

Theorem 3.5 (Erdös-Kac Theorem for Function Fields). [Liu04, Theorem 1]

Denote by $w(f)$ the number of distinct irreducible factors dividing a polynomial $f \in F_n(\mathbb{F}_q)$ of degree $n$. Then for any $a \in \mathbb{R}$,

$$\lim_{n \to \infty} \frac{\# \left\{ f \in F_n(\mathbb{F}_q) | \frac{w(f) - m_{n,q}}{\sqrt{m_{n,q}}} \leq a \right\}}{\# F_n(\mathbb{F}_q)} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{a} e^{-\frac{t^2}{2}} dt$$

Fix positive integers $\alpha, \beta$. We denote by

$$P[\alpha < w(f) < \beta | f \in F_n(\mathbb{F}_q)]$$

the probability that the number of irreducible factors of a square-free polynomial $f$ of degree $n$ over $\mathbb{F}_q$ is greater than $\alpha$ and less than $\beta$. In other words,

$$P[\alpha \leq w(f) \leq \beta | f \in F_n(\mathbb{F}_q)] := \frac{\# \{ f \in F_n(\mathbb{F}_q) | \alpha \leq w(f) \leq \beta \}}{\# \{ f \in F_n(\mathbb{F}_q) \}} \quad (11)$$

Let $\rho$ be a positive number such that $0 < \rho < 1$. For sufficiently large $n$, the number of distinct prime divisors $w(f)$ for almost every polynomial $f \in F_n(\mathbb{F}_q)$ satisfies

$$\rho m_{n,q} \leq w(f) \leq 2m_{n,q}.$$

The effective upper bound on the number of polynomials in $F_n(\mathbb{F}_q)$ that do not satisfy the condition above can be obtained as follows.
Theorem 3.6 (Effective Erdös-Kac). For sufficiently large $n$, there exists a fixed constant $0 < C_{EK} < 4$ such that
\[ \mathbb{P}[w(f) < pm_{n,q} \text{ or } w(f) > 2m_{n,q} \mid f \in F_n(\mathbb{F}_q)] < C_{EK}(n \log q)^{-\rho \log \rho - 1 + \rho}. \] (12)

Proof. We thank the reviewer for suggesting the following idea of the proof. From [FWY20 Theorem 1], we obtain that there exists a constant $0 < C_1 < 2$ such that
\[ \mathbb{P}[w(f) > 2m_{n,q} \mid f \in F_n(\mathbb{F}_q)] < C_1(n \log q)^{-2 \log^2 - 1}. \] (13)
From [FWY20 Theorem 1] and [Liu04, Theorem 1], we also obtain that there exists a constant $0 < C_2 < 2$ such that
\[ \mathbb{P}[w(f) < pm_{n,q} \mid f \in F_n(\mathbb{F}_q)] < C_2(n \log q)^{-\rho \log \rho + \rho - 1}. \] (14)
Combining two inequalities and the fact that for any $0 < \rho < 1$,
\[ \rho \log \rho + 1 - \rho < 1 < 2 \log 2 + 1, \]
we obtain that there exists $0 < C_{EK} < 4$ such that
\[ \mathbb{P}[w(f) < pm_{n,q} \text{ or } w(f) > 2m_{n,q} \mid f \in F_n(\mathbb{F}_q)] < C_{EK}(n \log q)^{-\rho \log \rho + \rho - 1}. \] (15)
\[ \square \]

Remark 3.7. Theorem 3.6 can also be obtained from using the results by Cohen, see for instance [Coh69 Theorem 6] and [CLNY22 Theorem 1.1].

4. Splitting partitions of polynomials

The objective of this section is to find a suitable subset of polynomials in $F_n(\mathbb{F}_q)$ over which the behavior of $\text{Sel}_s(E[\nu])$ can be well understood. For this purpose, we introduce the notion of splitting partitions of polynomials. Our goal is to show that almost all $f \in F_n(\mathbb{F}_q)$ satisfies:
- The number of distinct irreducible factors of $f$ is between $pm_{n,q}$ and $2m_{n,q}$.
- The number of distinct irreducible factors of degree at least $[\frac{4m_{n,q}^2}{\log q}]$ is at least $(1 - \epsilon)pm_{n,q}$ for some small enough $\epsilon > 0$.
- There is an irreducible factor of degree at least $[\frac{4m_{n,q}^2}{\log q}]$ whose Frobenius element in $\text{Gal}(K(E[p])/\mathbb{F}_p)$ has order prime to $p$.

4.1. Some sets of places.

Definition 4.1. From this section and onwards, we assume the following conditions on $K = \mathbb{F}_q(t)$, prime $p$, and a fixed choice of an elliptic curve $E$ over $K$.
- $E$ is a non-isotrivial elliptic curve over $K$.
- $E$ contains a place of split multiplicative reduction.
- The constant field $\mathbb{F}_q$ has characteristic coprime to 2, 3, $p$, and contains $\mu_p$. \hspace{1cm} (16)
- The image of $\text{Gal}(\overline{K}/K) \to \text{Aut}(E[p])$ contains $\text{SL}_2(\mathbb{F}_p)$.

By Igusa’s theorem, for any non-isotrivial elliptic curve $E$, there exists a prime $p$ and a finite separable extension of $K = \mathbb{F}_q(t)$ such that $E$ satisfies the first three conditions [Igu59, BLV09].

Definition 4.2. The following notations are used to denote a set of places of $K$ whose definitions depend on the choice of the elliptic curve $E$. We follow the style of notations as stated in [KMR14, Section 3].
- $\Sigma$: a set of places of $K$ that includes places of bad reduction of $E$.
- $\Sigma_E$: a subset of $\Sigma$ consisting only of places of bad reduction of $E$.
- $\sigma$: a square-free product of places $\nu$ of $K$ such that $\nu \notin \Sigma$.
Let \( v \) satisfies the condition that \( Gal(E) \) element associated to \( v \) where \( f \) that we wish to impose on irreducible factors of \( n \), \( w \) splitting partition with respect to a tuple of integers \( (i, j, k) \).

Definition 4.5. Let \( \lambda_{[m,n]} := \{(\lambda_{i,j,k}, i, j, k) \}_{m \leq i \leq n, 1 \leq j \leq n, 0 \leq k \leq 2} \) a set of \( 3n(m - n + 1) \) many 4-tuples. We also use the abbreviation \( \lambda_n := \lambda_{[1,n]} \).

Definition 4.6. Throughout the rest of the manuscript, we denote by \( n \) the positive integer

\[
\frac{4(m_n q)^2}{\log q} = \left\lfloor \frac{4(\log n + \log \log q)^2}{\log q} \right\rfloor.
\]
Definition 4.7. Fix two positive integers \( n \) and \( w \). We say that \( \lambda_n \) is a splitting partition with respect to \( (n, w) \) if it satisfies the following two conditions.

1. \( \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=0}^{2} \lambda_{i, j, k} \cdot i \cdot j = n. \)
2. \( \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=0}^{2} \lambda_{i, j, k} = w. \)

For example, if the irreducible factorization of a degree 6 polynomial \( f \) over \( \mathbb{F}_q \) is given by \( f = g_1^2 g_2 g_3 \) such that \( g_1 \in \mathcal{P}_1(1) \) and \( g_2, g_3 \in \mathcal{P}_2(2) \), then \( f \) admits a splitting partition \( \lambda_6 := \{(\lambda_{i, j, k}, i, j, k)\} \) that satisfies

\[
\lambda_{i, j, k} = \begin{cases} 
2 & \text{if } i = 2, j = 1, k = 2 \\
1 & \text{if } i = 1, j = 2, k = 1 \\
0 & \text{otherwise}
\end{cases}
\] (20)

We introduce four properties of splitting partitions with respect to \( (n, w) \) which will be of use in subsequent sections.

Definition 4.8. Let \( \lambda_n \) be a splitting partition with respect to \( (n, w) \).

1. We say that \( \lambda_n \) is \( p \)-th power free if

   \[
   \lambda_{i, j, k} = 0 \text{ whenever } j \geq p
   \] (21)

   In other words, any polynomial \( f \in F_n(\mathbb{F}_q) \) admitting a \( p \)-th power free partition \( \lambda_n \) is a \( p \)-th power free polynomial over \( \mathbb{F}_q \).

2. We say that \( \lambda_n \) is admissible if it satisfies

   \[
   \lambda_{i, j, k} = 0 \text{ whenever } i \leq n
   \] (22)

   In other words, any polynomial \( f \in F_n(\mathbb{F}_q) \) admitting an admissible partition \( \lambda_n \) is not divisible by irreducible polynomials of degree at most \( n \).

3. We say that \( \lambda_n \) is forgettable if

   \[
   \lambda_{i, j, k} = 0 \text{ whenever } i > n
   \] (23)

   In other words, any polynomial \( f \in F_n(\mathbb{F}_q) \) admitting a forgettable partition \( \lambda_n \) is not divisible by irreducible polynomials of degree greater than \( n \).

4. We say that an admissible partition \( \lambda_n \) is locally arrangeable if

   \[
   \lambda_{i, j, 0} \neq 0 \text{ for some } i > N \text{ and } j \neq 0 \text{ mod } p
   \] (24)

Any polynomial \( f \in F_n(\mathbb{F}_q) \) admitting a locally arrangeable partition has an irreducible factor in \( \mathcal{P}_0 \) of degree greater than \( n \) and of multiplicity coprime to \( p \).

Definition 4.9. We define the following set of splitting partitions with respect to a tuple of positive integers \( (n, w) \).

- \( \Lambda_{n,w} := \{\lambda_n \mid \lambda_n \text{ is a splitting partition with respect to } (n, w)\} \)
- \( \Lambda_{n,w}^{ad} := \{\lambda_n \in \Lambda_{n,w} \mid \lambda_n \text{ is a } p \text{-th power free admissible partition}\} \)
- \( \Lambda_{n,w}^{for} := \{\lambda_n \in \Lambda_{n,w} \mid \lambda_n \text{ is a forgettable partition}\} \)
- \( \Lambda_{n,w}^{la} := \{\lambda_n \in \Lambda_{n,w}^{ad} \mid \lambda_n \text{ is a locally arrangeable partition}\} \)

Using these splitting partitions, we further decompose the set \( F_n(\mathbb{F}_q) \) of monic polynomials of degree \( n \) as follows.

Definition 4.10. Given a polynomial \( f \in F_n(\mathbb{F}_q) \) and an irreducible polynomial \( g \) over \( \mathbb{F}_q \), denote by \( v_g(f) \) the multiplicity of \( g \) as an irreducible factor of \( f \). We define

\[
\begin{align*}
    f^* := \prod_{g \in \cup_{i=n+1}^{n} \mathcal{P}(d)} g^{v_g(f)}, & \quad f_* := \prod_{g \in \cup_{i=n+1}^{n} \mathcal{P}(d)} g^{v_g(f)}
\end{align*}
\] (25)
We note that \( f = f^* f_* \), where the irreducible factors of \( f^* \) are all of degree greater than \( n \) (and likewise for \( f_* \)).

**Definition 4.11.** Let \( n, w \) be two positive integers. Given a polynomial \( f \in F_n(\mathbb{F}_q) \), denote by \( w(f) \) the number of distinct irreducible factors of \( f \).

1. Given a positive integer \( w' < w \), we denote by
   \[
   F_{n, (w, w')} (\mathbb{F}_q) := \{ f \in F_n(\mathbb{F}_q) \mid w(f) = w \text{ and } w(f^*) = w' \}
   \]  
   (26)

2. Given a positive integer \( N < n \), we denote by
   \[
   F_{n, (N, w')}(\mathbb{F}_q) := \{ f \in F_{n, (N, w')}(\mathbb{F}_q) \mid \deg f^* = N \text{ and } f^* \text{ is } p\text{-th power free} \}
   \]  
   (27)

3. Given a locally arrangeable partition \( \lambda \in \Lambda^\text{in}_{N, w'} \) and a forgettable partition \( \eta \in \Lambda^\text{for}_{n-N, w-w'} \), we denote by
   \[
   F^{(\lambda, \eta)}_{n, (N, w')}(\mathbb{F}_q) := \{ f \in F_{n, (N, w')}(\mathbb{F}_q) \mid f^* \text{ admits } \lambda, f_* \text{ admits } \eta \}.
   \]  
   (28)

4. We denote by \( \hat{F}_{n, (N, w')}(\mathbb{F}_q) \) the following subset of \( F_{n, (N, w')}(\mathbb{F}_q) \):
   \[
   \hat{F}_{n, (N, w')}(\mathbb{F}_q) := \bigcup_{\lambda \in \Lambda^\text{in}_{N, w'}} \bigcup_{\eta \in \Lambda^\text{for}_{n-N, w-w'}} F^{(\lambda, \eta)}_{n, (N, w')}(\mathbb{F}_q).
   \]  
   (29)

**Remark 4.12.** The construction of \( F^{(\lambda, \eta)}_{n, (N, w')}(\mathbb{F}_q) \) is closely related to the construction of fan structure from [KMR14, Chapter 2,3,4]. Given two sets \( B \) and \( C \), denote by
   \[
   B \ast C := \{ \delta \cup \{ q \} \mid \delta \in B, q \in C \setminus \{ q \} \},
   \]  
   as stated in [KMR14, Chapter 4, Page 1085]. Note that if \( B \cap C = \emptyset \), then \( B \ast C = B \times C \). For any positive integer \( m > 0 \), inductively define
   \[
   \mathcal{P}_k(i)^{1} = \mathcal{P}_k(i),
   \]
   \[
   \mathcal{P}_k(i)^{m} = \mathcal{P}_k(i)^{(m-1)} \ast \mathcal{P}_k(i)
   \]  
   (31)

Then one has
   \[
   F^{(\lambda, \eta)}_{n, (N, w')}(\mathbb{F}_q) = \left[ \prod_{i,j,k} \mathcal{P}_k(i)^{\lambda_{i,j,k}} \right] \times \left[ \prod_{i,j,k} \mathcal{P}_k(i)^{\eta_{i,j,k}} \right]
   \]  
   (32)

To understand how the sizes of four types of subsets of \( F_n(\mathbb{F}_q) \) are related to each other, we prove the following proposition, which shows that for sufficiently large \( n \), any monic polynomial of degree \( d \) cannot have too many factors whose degree is at most \( n \).

**Proposition 4.13.** Suppose \( m_{n,q} := \log n + \log \log q \) satisfies the condition that \( m_{n,q} > e^{e^\epsilon} \). Let \( \epsilon = \frac{1}{\log \log m_{n,q}} \). Then
   \[
   \# \{ f \in F_n(\mathbb{F}_q) \mid w(f_*) > \epsilon m_{n,q} \} < 4 \cdot q^n \cdot (n \log q)^{-\left(\log m_{n,q}\right)^{1-\sqrt{\epsilon}}}. \]  
   (33)

**Proof.** We thank the reviewer for suggesting the following strategy of the proof. Let \( \mathcal{Q} \) be a set of irreducible monic polynomials of degree at most \( n \). By Mertens’s theorem for global function fields, the number of monic polynomials of degree \( n \) with at least \( r \) distinct irreducible factors from \( \mathcal{Q} \) is at most
   \[
   q^n \cdot \frac{1}{r!} \cdot \left( \sum_{g \in \mathcal{Q}} q^{-\deg(g)} \right)
   \]  
   (34)

For our purposes, we let
   \[
   \mathcal{Q} := \cup_{i=1}^{n} \mathcal{P}(i)
   \]  
   (35)
where we recall that \( m_{n,q} := \log n + \log \log q \) and \( n := \lfloor \frac{4(\log n + \log\log q)^2}{\log q} \rfloor = \lfloor \frac{4m_{n,q}^2}{\log q} \rfloor \). Then
\[
\sum_{g \in \mathbb{Q}} q^{-\deg g} = \sum_{i=1}^{n} \# \mathcal{P}(i) \cdot q^{-i} \leq 2 \cdot \sum_{i=1}^{n} \frac{1}{i} \leq 2 \log(n) + 2 \leq 4 \log m_{n,q} + 4 \log 2 + 2. \tag{36}
\]

Suppose that \( m_{n,q} > e^{e^e} \). We let
\[
r := \epsilon m_{n,q}, \quad \epsilon := \frac{1}{\log \log m_{n,q}} \tag{37}
\]
Sterling’s approximation theorem shows that for such \( n \) satisfying \( m_{n,q} > e^{e^e} \),
\[
\frac{1}{r!} < \frac{1}{\sqrt{2\pi r} \left( \frac{r}{e} \right)^r} = \frac{1}{\sqrt{2\pi \epsilon m_{n,q}}} \cdot (n \log q)^{-\epsilon \log m_{n,q} - \epsilon \log \epsilon + \epsilon} \tag{38}
\]
We note that because \( 0 < \epsilon < 1 \), it follows that \( 0 < \epsilon - \epsilon \log \epsilon < 1 \). Hence, the above equation can be simplified as
\[
\frac{1}{r!} < \frac{1}{\sqrt{\pi m_{n,q}}} \cdot (n \log q)^{-\epsilon \log m_{n,q} + 1} \tag{39}
\]
Combining with equation (34), we obtain
\[
\# \{ f \in F_n(\mathbb{F}_q) \mid w(f) > \epsilon m_{n,q} \} < q^n \cdot \frac{4 \log m_{n,q} + 4 \log 2 + 2}{\sqrt{\pi m_{n,q}}} \cdot (n \log q)^{-\epsilon \log m_{n,q} + 1}
\]
\[
< q^n \cdot 4 \cdot (n \log q)^{-\epsilon \log m_{n,q} + 1} \tag{40}
\]
The statement of the proposition follows from the inequality that whenever \( m_{n,q} > e^{e^e} \), we have \( \epsilon \log m_{n,q} - 1 \) is at least \( (\log m_{n,q})^{1-\sqrt{\epsilon}} \).

We now show that the set \( F_n(\mathbb{F}_q) \) can be approximated by disjoint union of subsets of form \( F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) \) where \( \lambda \) is a locally arrangeable splitting partition, and \( \eta \) is a forgettable splitting partition.

**Proposition 4.14.** Let \( \rho \in (0,1) \) be a positive number. Suppose \( n \) is a positive integer such that \( m_{n,q} > \max \{ e^{e^e}, \log 6 + \log(\rho^3 + g_{E[p]}) \} \). Let \( \epsilon = \frac{1}{\log \log m_{n,q}} \). Then
\[
\# F_n(\mathbb{F}_q) - \sum_{w=\rho m_{n,q}}^{2m_{n,q}} \sum_{w'=1}^{w} \sum_{N=w/n}^{n} \# F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q)
\]
\[
\leq 4 \cdot q^n \cdot \max \left( n^{-\rho \log \rho - 1 + \rho}, 3m_{n,q}^2 \cdot \left( \frac{p}{p^2 - 1} \right)^{(1-\epsilon)\rho m_{n,q}} \right) \tag{41}
\]
In other words, the above proposition shows that given \( \rho \in (0,1) \), almost every monic polynomial \( f \) of degree \( n \) satisfies:

1. The number of distinct irreducible factors of \( f \) is between \( \rho m_{n,q} \) and \( m_{n,q} \).
2. The number of distinct irreducible factors of \( f \) of degree at most \( n \) is at most \( (1-\epsilon)\rho m_{n,q} \) for some small enough \( \epsilon > 0 \).
3. The polynomial \( f^* \) is \( p \)-th power free, and has at least 1 irreducible factor inside \( \mathcal{P}_0 \) of degree at least \( n \).

The two error terms appearing in Proposition 4.14 correspond to two of the error terms constituting the constant \( \alpha(p) \) defined in Theorem 1.2.
Proof. By Theorem 3.6 and Proposition 4.13, for any small enough $\epsilon > 0$,
\[
\#F_n(F_q) - \sum_{w=\rho m_{n,q}}^{2m_{n,q}} \sum_{w'=1-\epsilon}^{w} \#F_{n,(w,w')}(F_q) \leq 4 \cdot q^n \cdot n^{-\rho \log \rho - 1 + \rho} \tag{42}
\]
Using the definition of $f^*$, it follows that if $f^*$ is not $p$-th power free, then the degree of the $p$-th power free part of $f^*$ is at most $n - pn$. Therefore, one obtains that
\[
\#F_{n,(w,w')}(F_q) - \sum_{N=\rho m_{n,q}}^{n} \#F_{n,N,(w,w')}(F_q) \leq q^n \cdot n^{-4(p-1)(\log n)^2} \tag{43}
\]
Using the definition of $\Lambda_n$ it follows that for any four integers $n > N$ and $w > w'$,
\[
F_{n,N,(w,w')}(F_q) = \bigcup_{\lambda \in \Lambda_{n,w'}} \bigcup_{\eta \in \Lambda_{n,N,w-w'}} F_{\lambda,n}(F_q) \tag{44}
\]
Recall that $g_E[p]$ is the genus of the global function field $K(E[p])/K$. Because we assumed that $m_{n,q} > \max\{e^{\epsilon n}, \log 6 + \log(p^3 + g_E[p])\}$, we obtain that
\[ q^{\frac{m_{n,q}}{n}} > (n \log q)^{m_{n,q}} > e^{m_{n,q}} > 6(p^3 + g_E[p]). \]
Suppose that $w' \leq 2m_{n,q}$. Apply Theorem 3.1 with respect to the field $K(E[p])/K$ to get
\[
\sum_{N=\rho m_{n,q}}^{n} \left( \sum_{\lambda \in \Lambda_{n,w}} \sum_{\eta \in \Lambda_{n,N,w-w'}} \#F_{\lambda,n}(F_q) \right) \leq q^n \cdot \left( \left( \frac{p}{p^2 - 1} \right)^{w'} + \sum_{k=1}^{\infty} (n \log q)^{-m_{n,q}+2} \right) \leq q^n \cdot \left( \left( \frac{p}{p^2 - 1} \right)^{w'} + 2 \cdot (n \log q)^{-m_{n,q}+2} \right) \leq 3 \cdot q^n \cdot \left( \frac{p}{p^2 - 1} \right)^{w'}. \tag{45}
\]
The quantity $\left( \frac{p}{p^2 - 1} \right)^{w'}$ is the leading term of the probability that none of the irreducible factors of $f^*$ are in $P_0$, and the rest of the terms are obtained from the rate of convergence of the Chebotarev density theorem and binomial theorem, in particular equation (17). Combining equations (42), (43), and (45), we obtain the statement of the proposition. \hfill \Box

4.3. Equidistribution of local characters. In this subsection, we prove that for sufficiently large $n$, the probability distribution that the set of global cyclic order-$p$ characters induced from the set of irreducible polynomials of degree $n$ restricts to a uniform distribution over the set of finite Cartesian products of local unramified cyclic order-$p$ characters at finitely many places of degree strictly less than $n$.

Theorem 4.15. [Hsu98, Theorem 2.1] Let $h$ be any square-free polynomial over $F_q$. Let $\chi_h$ be a non-trivial character $\chi : (F_q[t]/h)^\times \to \mathbb{C}^\times$. Then
\[
\sum_{v \in P(i)} \chi(v) \leq (\deg h + 1) q^{\frac{1}{2}} \frac{q^{\frac{1}{2}}}{i}. \tag{46}
\]
An immediate corollary of the theorem above is that the effective error bounds of the density of whether the restriction of a global cyclic order-$p$ character associated to an irreducible polynomial forms a uniform distribution over the set of finite cartesian products of local unramified cyclic characters is given by the order of $q^{-\frac{1}{2}}$. 
**Corollary 4.16.** Let $K = \mathbb{F}_q(t)$ be a global function field such that $\mu_p \subset \mathbb{F}_q$. Let $h_1, h_2, \ldots, h_w$ be irreducible polynomials over $\mathbb{F}_q$. Given a place $v$ of degree $i$, denote by $\left( \frac{w}{h_k}_p \right)$ in $\mu_p$ the $p$-th power residue symbol. Then for any $a \in \mu_p^{\geq w}$,

$$
\left| \frac{\# \{ v \in \mathcal{P}(i) | \left( \frac{w}{h_k}_p \right)_{k=1}^w = a \in \mu_p^{\geq w} \}}{\# \mathcal{P}(i)} - \frac{1}{p^w} \right| < \left( \sum_{k=1}^w \deg(h_k) + 1 \right) \cdot q^{-i/2} / i. \tag{47}
$$

**Proof.** We thank the reviewer for suggesting the strategy of the proof outlined as follows.

For any abelian group $H$ and $\Omega := \{ \chi : H \to \mathbb{C} \}$ the set of characters of $H$, the orthogonality of characters imply that

$$
\sum_{\chi \in \Omega} \frac{\chi(g_1)}{\chi(g_2)} = \begin{cases} |H| & \text{if } g_1 = g_2 \\ 0 & \text{otherwise} \end{cases} \tag{48}
$$

We let $H$ to be the abelian group isomorphic to $\mu_p^{\geq w}$ generated by the Legendre symbols

$$
\left\{ \left( \frac{.}{h_1}_p, \frac{.}{h_2}_p, \ldots, \frac{.}{h_w}_p \right) \right\} \tag{49}
$$

Suppose $g_2 = a \in \mu_p^{\geq w}$. Using the orthogonality of characters, we obtain

$$
\sum_{v \in \mathcal{P}(i)} \sum_{\chi \in \Omega} \frac{\chi(\left( \frac{w}{h_1}_p \right)_{k=1}^w \cdots \left( \frac{w}{h_w}_p \right)_{k=1}^w)}{\chi(a)} = \# \left\{ v \in \mathcal{P}(i) | \left( \frac{w}{h_k}_p \right)_{k=1}^w = a \right\} \cdot p^w \tag{50}
$$

The left hand side of the above equation can be rewritten as

$$
= \# \mathcal{P}(i) + \sum_{\chi \in \Omega} \sum_{v \in \mathcal{P}(i)} \frac{\chi(\left( \frac{w}{h_1}_p \right)_{k=1}^w \cdots \left( \frac{w}{h_w}_p \right)_{k=1}^w)}{\chi(a)} \tag{51}
$$

Using Theorem 4.15, the summands of the second terms have absolute values bounded above by $(\sum_{k=1}^w \deg(h_k) + 1) \cdot q^{-i/2} / i$. Hence, we obtain that

$$
\left| \frac{\# \{ v \in \mathcal{P}(i) | \left( \frac{w}{h_k}_p \right)_{k=1}^w = a \in \mu_p^{\geq w} \}}{\# \mathcal{P}(i)} - \frac{1}{p^w} \right| < \left( \sum_{k=1}^w \deg(h_k) + 1 \right) \cdot q^{-i/2} / i \tag{52}
$$

We also prove that given a choice of an elliptic curve $E/K$, the equidistribution of characters still holds for subsets of places $v$ inside $\mathcal{P}_0(i)$, $\mathcal{P}_1(i)$, and $\mathcal{P}_2(i)$.

**Corollary 4.17.** Let $E$ be an elliptic curve over $K$ satisfying conditions in (16). Suppose that $h_1, h_2, \ldots, h_w$ are irreducible polynomials over $\mathbb{F}_q$. Let $n$ be an integer such that $\sum_{\ell=1}^w \deg h_{\ell} \leq n$ and $w \leq 2m_{n,q}$.

1. Suppose $p \geq 5$, or $K(\sqrt{h_1}, \ldots, \sqrt{h_w}) \cap K(E[p]) = K$. Then for any element $a \in \mu_p^{\geq w}$, and $i > n$, there exists a constant $\hat{C}_{E,p,q} > 0$ depending only on $E$, $p$, $q$ such that

$$
\left| \frac{\# \{ v \in \mathcal{P}_k(i) | \left( \frac{w}{h_{\ell}}_p \right)_{\ell=1}^w = a \in \mu_p^{\geq w} \}}{\# \mathcal{P}_k(i)} - \frac{1}{p^w} \right| < \hat{C}_{E,p,q} \cdot (n \log q)^{-2m_{n,q} + 2 \log p} \tag{53}
$$


Suppose $p = 2, 3$ and $K(\sqrt[3]{h_1}, \ldots, \sqrt[3]{h_w}) \cap K(E[p]) \neq K$. Then for any $i > n$, there are $p^w - p^{w-1}$ many elements $a \in \mu_p^{\oplus w}$ such that $\left( \left( \frac{v}{h_i} \right)_p \right)_{i=1}^w \neq a$ for all $v \in \mathcal{P}_k(i)$. For the other $p^{w-1}$ many elements $a \in \mu_p^{\oplus w}$, there exists a constant $\hat{C}_{E,p,q} > 0$ depending only on $E$, $p$, $q$ such that
\[
\left| \frac{\# \{ v \in \mathcal{P}_k(i) | \left( \frac{v}{h_i} \right)_p \right)_{i=1}^w = a \in \mu_p^{\oplus w} \}}{\# \mathcal{P}_k(i)} - \frac{1}{p^{w-1}} \right| < \hat{C}_{E,p,q} \cdot (n \log q)^{-2m_{n,q}+2\log p}.
\]

Proof. Given an irreducible polynomial $h$ over $\mathbb{F}_q$, consider the cyclic order-$p$ abelian extension $K(\sqrt{h})/K$. Then if $v$ is coprime to $h$, then the $p$-th power residue symbol $\left( \frac{v}{h} \right)_p$ defines the action of the Frobenius element $\text{Frob}_v$ on $\sqrt{h}$ via
\[
\text{Frob}_v(\sqrt{h}) = \left( \frac{v}{h} \right)_p \sqrt{h},
\]
which in fact originates from the definition of the Artin reciprocity map, see [Ros02, Chapter 3, Chapter 10] for a detailed description.

With the irreducible polynomials $h_1, h_2, \ldots, h_w$ as stated, consider the field extension $L := K(E[p], \sqrt{h_1}, \ldots, \sqrt{h_w})$. Suppose that $K(\sqrt{h_1}, \ldots, \sqrt{h_w}) \cap K(E[p]) = K$. Note that this condition always holds for any choice of irreducible polynomials $h_i$ if $p \geq 5$, because $\text{SL}_2(\mathbb{F}_p)$ has no normal subgroup of index $p$. It hence follows that
\[
\text{Gal}(L/K) \cong \text{SL}_2(\mathbb{F}_p) \times \mu_p^{\oplus w}
\]
and its conjugacy classes are of form $C \times \{ a \}$, where $C \subset \text{SL}_2(\mathbb{F}_p)$ is a conjugacy class and $a \in \mu_p^{\oplus w}$ is an element. Recall that
\[
\# \text{Gal}(L/K) = p^w \cdot (p^3 - p).
\]

By Riemann-Hurwitz theorem,
\[
g_L \leq p^w \cdot (2g_{E[p]} - 2 + p^3),
\]
where $g_{E[p]}$ is the genus of the global function field $K(E[p])$. Applying Corollary 3.2 and Corollary 4.16 proves the first statement of the theorem, where we set $\hat{C}_{E,p,q} := 6(2g_{E[p]} + 2p^3 - p - 2)$.

The case where $K(\sqrt{h_1}, \ldots, \sqrt{h_w}) \cap K(E[p]) \neq K$ occurs when $p = 2$ or $3$. In such cases, the field extension $K(\sqrt{h_1}, \ldots, \sqrt{h_w}) \cap K(E[p])$ is a non-trivial cyclic Galois extension over $K$ of degree $p$, which corresponds to the normal subgroup of $\text{SL}_2(\mathbb{F}_p)$ of index $p$. It then follows that
\[
\text{Gal}(L/K) \cong \text{SL}_2(\mathbb{F}_p) \times \mu_p^{\oplus w-1}.
\]

Applying the analogous argument for proving the first statement of the theorem yields the rest of the results. \hfill \square

Remark 4.18. Suppose that $p = 2$. The criterion to determine which elements $a \in \mu_p^{\oplus w}$ satisfy $\left( \left( \frac{v}{h_i} \right)_p \right)_{i=1}^w \neq a$ for all $v \in \mathcal{P}_k(i)$ can be determined by what is called the “sign function”, see [KMR14, Definition 10.6] for further details.

5. Local Selmer groups

The objective of this section focuses on defining what is called the local Selmer groups of $E$ associated to a cyclic order $p$ local character, and understanding their dimensions over the subset of polynomials $F_{(n,N)}(\mathbb{F}_q)$. These results will be of relevant use in Section 6 where we will understand the dimensions of $\text{Sel}_\pi(E^\lambda)$ as $f$ ranges over $F_n(\mathbb{F}_q)$. 
5.1. Local twists. The constructions and properties of the local Selmer groups, as explored in [MR07, KMR13, KMR14], rests upon utilizing results regarding Galois cohomology groups and Poitou-Tate duality theorems over number fields, the theories of which also hold valid over global function fields \( F_q(t) \), see for example Chapter 1 of [Mil06] for a rigorous treatment of Poitou-Tate duality theorems for global function fields. We further enrich these results by using the properties that hold over \( F_q(t) \) explored from Section 3 which are not necessarily proven for number fields.

**Definition 5.1.** We introduce the following notations regarding cyclic order \( p \) characters \( \chi \in \text{Hom}(\text{Gal}(K_v/K_v, \mu_p)) \), some of which are as stated in [KMR14, Sections 5, 7, 9]. We recall the sets of primes \( \Sigma \) and \( \Sigma_E \) associated to choices of \( E \) from Definition 4.2. Given a set \( \Sigma \), we let \( \sigma \) be a square-free product of places coprime to elements in \( \Sigma \).

- \( \Omega_\sigma \): the set of finite Cartesian products of local characters
  \[ \chi := (\chi_v)_v \in \Omega_\sigma := \prod_{v \in \Sigma(\sigma)} \text{Hom}(\text{Gal}(K_v/K_v), \mu_p) \]
  such that the component \( \chi_v \) is ramified if \( v \mid \sigma \). For the sake of convenience, we will denote by \( \text{Hom}_{\text{unr}}(\text{Gal}(K_v/K_v), \mu_p) \) the set of unramified local characters at place \( v \), and by \( \text{Hom}_{\text{ram}}(\text{Gal}(K_v/K_v), \mu_p) \) the set of ramified local characters at place \( v \). Assuming that \( \mu_p \subset K_v \), there are \( p \) distinct unramified local characters at \( v \), and \( p(p-1) \) distinct ramified local characters at \( v \).
- \( \Omega_E \): the set of finite Cartesian products of local characters
  \[ \chi := (\chi_v)_v \in \Omega_E := \prod_{v \in \Sigma_E} \text{Hom}(\text{Gal}(K_v/K_v), \mu_p) \]

Fix an element \( \chi \in \Omega_\sigma \). Let \( \mathfrak{v} \) be a place over \( K \) such that \( \mathfrak{v} \not\in \Sigma(\sigma) \). Let \( \chi' \in \Omega_{\sigma \mathfrak{v}} \) be an element such that

- For any \( v \in \Sigma(\sigma) \), \( \chi'_v = \chi_v \).
- At \( \mathfrak{v} \), \( \chi'_\mathfrak{v} \) is ramified.

Denote by \( \Omega_{\chi, \mathfrak{v}} \) the set of local characters \( \chi' \) satisfying the two conditions above. Note that

\[ \Omega_{\sigma \mathfrak{v}} = \bigsqcup_{\chi \in \Omega_\sigma} \Omega_{\chi, \mathfrak{v}}. \]

**Definition 5.2.** We introduce the following notations regarding local Selmer groups of \( E \) associated to cyclic order \( p \) characters \( \chi \in \text{Hom}(\text{Gal}(K_v/K_v, \mu_p)) \), some of which are as stated in [KMR14, Sections 5, 7, 9].

- Given a Cartesian product of local characters \( \chi \in \Omega_\sigma \), the local Selmer group of \( E \) associated to \( \chi \) is denoted as
  \[ \text{Sel}(E[p], \chi) := \text{Ker} \left( H^1_{\text{ét}}(K, E[p]) \to \prod_v H^1_{\text{ét}}(K_v, E[p])/\mathcal{H}^\chi_v \right) \]

where

\[ \mathcal{H}^\chi_v := \begin{cases} \text{im} (\delta^\chi_v : E^{\times}(K_v)/\pi E^{\times}(K_v) \to H^1(K_v, E[p])) & \text{if } v \in \Sigma(\sigma) \\ H^1(\mathcal{O}_{K_v}, E[p]) & \text{if } v \not\in \Sigma(\sigma) \end{cases} \]

Under all but the third assumption stated in (16), we use the isomorphism

\[ H^1_{\text{ét}}(K, E[p]) \cong H^1_{\text{ét}}(K, E^{\times}_[\pi]), \]
\[ H^1_{\text{ét}}(K_v, E[p]) \cong H^1_{\text{ét}}(K_v, E^{\times}_{v}_[\pi]) \]

to define the local Selmer group \( \text{Sel}(E[p], \chi) \), see in particular [MR07, Proposition 4.1, Definition 4.3]. Even though the reference particularly constructs these groups over number fields, the relevant results extend to global function fields as well.
• If \( v \in \mathcal{P}_0 \), then \( \mathcal{H}_v^1 \) is trivial. If \( v \in \mathcal{P}_1 \cap \Sigma(\sigma) \), then there is a unique 1-dimensional ramified subspace, denoted as \( \mathcal{H}_v^{1,ram} \). If \( v \in \mathcal{P}_2 \cap \Sigma(\sigma) \), then there are \( p \) distinct 2-dimensional ramified subspaces \( \mathcal{H}_v^2 \), each corresponding to a tamely totally ramified cyclic \( p \)-extension \( \overline{K_v}^{\text{Ker}(\chi_v)} \) over \( K_v \). As stated in [KMR14, Definition 5.10], for such a \( v \) we have a set-theoretic bijection

\[
\alpha_v : \frac{\text{Hom}_{\text{ram}}(\text{Gal}(K_v/K_v), \mu_p)}{\text{Aut}(\mu_p)} \rightarrow \{ \mathcal{H}_v^\chi \}_{\chi \in \text{Hom}_{\text{ram}}(\text{Gal}(K_v/K_v), \mu_p)}.
\]

These identifications allow us to rewrite the subspaces \( \mathcal{H}_v^\chi \) appearing in equation (60) as

\[
\mathcal{H}_v^\chi := \begin{cases} 
\alpha_v(\overline{K_v}^{\text{Ker}(\chi_v)}) & \text{if } v \in \mathcal{P}_2 \cap \Sigma(\sigma) \\
\mathcal{H}_v^{1,\text{ram}} & \text{if } v \in \mathcal{P}_1 \cap \Sigma(\sigma) \\
0 & \text{if } v \in \mathcal{P}_0 \cap \Sigma(\sigma) \\
\text{im}\delta_v^\chi & \text{if } v \in \Sigma \setminus \mathcal{P} \text{ and } \mathcal{H}_v = \overline{K_v}^{\text{Ker}(\chi_v)} \\
H^1(\mathcal{O}_{K_v}, E[p]) & \text{if } v \notin \Sigma(\sigma)
\end{cases}
\]

(61)

• Given a set of local characters \( \chi \in \Omega_\sigma \), we denote by \( \text{rk}(\chi) \) the dimension of \( \text{Sel}(E[p], \chi) \) as an \( \mathbb{F}_p \)-vector space. By the identification of \( \mathcal{H}_v^\chi \) above, we have \( \text{rk}(\chi) = \text{rk}(\chi') \) if the following two conditions are satisfied:

\[\begin{align*}
&\text{1. } \text{Ker}(\chi_v) = \text{Ker}(\chi'_v) \subset \text{Gal}(\overline{K_v}/K_v) \text{ for every } v \in \mathcal{P}_2 \cap \Sigma(\sigma) \\
&\text{2. } \text{rk}(\chi) = \text{rk}(\chi'), \text{ where } \chi := (\chi_v)_{v \in \Sigma} \in \Omega_{E} \text{ (and likewise for } \chi').
\end{align*}\]

Any changes in local conditions over places \( v \in \mathcal{P}_0 \) do not affect the values of \( \text{rk}(\chi) \).

• Denote by \( t_\chi(v) \) the dimension of the image of the local Selmer group \( \text{Sel}(E[p], \chi) \) with respect to the localization map at \( v \), i.e.

\[t_\chi(v) := \dim_{\mathbb{F}_p} \text{im} \left( \text{loc}_v : \text{Sel}(E[p], \chi) \rightarrow H^1(\mathcal{O}_{K_v}, E[p]) \right)\]

(62)

We note that if \( v \in \mathcal{P}_i \), then \( 0 \leq t_\chi(v) \leq i \). Furthermore, we have \( t_\chi(v) = t_{\chi'}(v) \) if \( \text{Ker}(\chi_v) = \text{Ker}(\chi'_v) \subset \text{Gal}(\overline{K_v}/K_v) \) for every \( v \in \Sigma(\sigma) \).

The relation between \( t_\chi(v) \) and the differences between ranks of local Selmer groups associated to characters \( \chi \in \Omega_\sigma \) and \( \chi' \in \Omega_{\chi,v} \) is stated in [KMR14, Proposition 7.2].

Proposition 5.3. Let \( E \) be a non-isotrivial elliptic curve over \( K \) satisfying the conditions from equation (10). Fix a square-free product of places \( \sigma \) coprime to elements in \( \Sigma \), and let \( v \) be a place of \( K \) such that \( v \notin \Sigma(\sigma) \). Fix a character \( \chi \in \Omega_\sigma \). Then for any \( \chi' \in \Omega_{\chi,v} \),

\[
\text{rk}(\chi') - \text{rk}(\chi) = \begin{cases} 
2 & \text{if } v \in \mathcal{P}_2 \text{ and } t_\chi(v) = 0 \text{ for exactly } p - 1 \text{ many } \chi' \in \Omega_{\chi,v} \\
1 & \text{if } v \in \mathcal{P}_1 \text{ and } t_\chi(v) = 0 \\
-1 & \text{if } v \in \mathcal{P}_1 \text{ and } t_\chi(v) = 1 \\
-2 & \text{if } v \in \mathcal{P}_2 \text{ and } t_\chi(v) = 2 \\
0 & \text{otherwise}
\end{cases}
\]

(63)

We note that the \( p - 1 \) many \( \chi' \in \Omega_{\chi,v} \) that satisfies \( \text{rk}(\chi') - \text{rk}(\chi) = 2 \) share an identical cyclic degree \( p \)-ramified extension over \( K_v \).

Proof. The proof follows from adapting the proof of [KMR14, Proposition 7.2]. The two conditions required in the statement of [KMR14, Proposition 7.2], which are

1. \( \text{Pic}(\mathcal{O}_{K,\Sigma}) = 0 \)
2. The map \( \mathcal{O}_{K,\Sigma}^X/(\mathcal{O}_{K,\Sigma})^p \rightarrow \prod_{v \in \Sigma} K_v^X/(K_v^X)^p \) is injective

hold regardless of the choice of \( \Sigma \) because \( \mathcal{O}_K = \mathbb{F}_q[t] \) is a Euclidean domain. \( \square \)
The probability that $t_\chi(v)$ achieves a certain value can be obtained from a Chebotarev condition over $K$ obtained from $\text{Sel}(E[p], \chi)$, as shown in [KMR14, Proposition 9.4].

**Proposition 5.4** (Local twists of $\pi$-Selmer groups). Let $E$ be a non-isotrivial elliptic curve over $K$ satisfying the conditions from equation (16). Fix a square-free product of places $\sigma$ coprime to elements in $\Sigma$. Fix a local character $\chi \in \Omega_\sigma$.

Let $d_{i,j}$ be given by the following table:

| $d_{i,j}$ | $i = 0$ | $i = 1$ | $i = 2$ |
|-----------|---------|---------|---------|
| $j = -2$  | $\times$ | $\times$ | $1 - (p + 1)p^{-rk(\chi)} + p^{-2rk(\chi)}$ |
| $j = -1$  | $\times$ | $1 - p^{-rk(\chi)}$ | $\times$ |
| $j = 0$   | $1$     | $\times$ | $(p + 1)(p^{-rk(\chi)} - p^{-2rk(\chi)})$ |
| $j = 1$   | $\times$ | $p^{-rk(\chi)}$ | $\times$ |
| $j = 2$   | $\times$ | $\times$ | $p^{-2rk(\chi)}$ |

Here, the term $\times$ denotes the case where such a difference of ranks cannot occur. Let $D_{E,p,q} > 0$ be a constant defined as

$$D_{E,p,q} := p^{\max_{e \in \Omega_E} (rk(\chi))}$$

(64)

Then there exists a fixed constant $C_{E,p,q} > 0$ which depends only on the elliptic curve $E$, $p$, and $q$ such that for every $d > \frac{12 \log p + 2 \log D_{E,p,q} + (6 \log p) \cdot \#(\Sigma(\sigma))}{\log q}$,

$$\frac{\#\{v \in P_{i}(d) \mid v \not\in (\Sigma(\sigma)) \text{ and } t_\chi(v) = j\}}{\#\{v \in P_{i}(d) \mid v \not\in (\Sigma(\sigma))\}} - d_{i,j} < C_{E,p,q} \cdot p^{3\#(\Sigma(\sigma)) \cdot q^{-\frac{d}{2}}}.$$  

(65)

**Proof.** The theorem can be proved in an analogous way to how [KMR14, Proposition 9.4] was proved over number fields. Nevertheless, it is necessary to apply the effective Chebotarev density theorem to calculate the explicit error bounds.

[[**Governing field extension for** $t_\chi(v)$]]

We first review the ideas presented in [KMR14, Proposition 9.4]. Denote by $\text{Res}$ the restriction morphism of cohomology groups:

$$H^1_{\text{ét}}(K, E[p]) \to H^1_{\text{ét}}(K(E[p]), E[p])^{\text{Gal}(K(E[p])/K)} = \text{Hom}(\text{Gal}(\overline{K(E[p])}/K(E[p])), E[p])^{\text{Gal}(K(E[p])/K)}.$$  

Let $F_{\sigma,\chi}$ be the fixed field of the following subgroup of $\text{Gal}(\overline{K(E[p])}/K(E[p]))$:

$$\bigcap_{c \in \text{Sel}(E[p], \chi)} \text{Ker} \left(\text{Res}(c) : \text{Gal}(\overline{K(E[p])}/K(E[p])) \to E[p]\right)$$

The field $F_{\sigma,\chi}$ satisfies the following properties, as shown in [KMR14, Proposition 9.3]:

1. $F_{\sigma,\chi}$ is Galois over $K$.
2. There is a $\text{Gal}(K(E[p])/K)$-module isomorphism $\text{Gal}(F_{\sigma,\chi}/K(E[p])) \cong (E[p])^{\text{rk}(\chi)}$.
3. $F_{\sigma,\chi}/K$ is unramified outside of places in $\Sigma(\sigma)$

The aforementioned condition holds for $p = 2$ whenever $E$ is a non-isotrivial elliptic curve such that $\text{Gal}(K(E[2])/K) \cong S_3$.

[[**Constant field of** $F_{\sigma,\chi}$]]

Suppose that $E$ has a place $v$ of split multiplicative reduction. Then the constant field of $F_{\sigma,\chi}$ is equal to $\mathbb{F}_q$. It suffices to show that any basis element $c \in \text{Sel}(E[p], \chi)$ maps the arithmetic Frobenius $\tau \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ to the identity element of $E[p]$. Consider the local Kummer map $\im \delta_e$ at the place $v$. Then $E$ is a Tate curve at $v$. There exists an element $q \in K_v^\times$ with positive valuation such that the $\mathbb{K}_v$-rational points of $E$ is given by

$$E(\mathbb{K}_v) \cong \mathbb{K}_v^\times /\langle q \rangle.$$
which implies for any positive number \( n \),
\[
E[n](\mathbb{Q}_v) \cong \langle q^{-\frac{1}{n}}, \mu_n \rangle / \langle q \rangle,
\]
see for example [Section 3.3] [BLV09] for a detailed discussion on these results. To analyze the condition that the basis element \( c \in \text{Sel}(E[p], \chi) \) maps the arithmetic Frobenius \( \tau \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_q) \) to the identity element of \( E[p] \), it suffices to verify that \( Q' - Q = O \) for \( Q \in E[p](\mathbb{Q}_v) \), which follows from the assumption that the constant field of \( K_v \) contains the primitive \( p \)th-root of unity.

**[Frobenius conjugacy class]**

Using the techniques of the proof from [KMR14] Proposition 9.4, one can show that the non-zero values of \( d_{i,j} \) from the table of the statement of the proposition are ratios of two non-empty subsets \( S_{i,j}, S'_{i,j} \subset \text{Gal}(F_{\sigma,\chi}/K) \) stable under conjugation, i.e. \( d_{i,j} = \frac{\# S'_{i,j}}{\# S_{i,j}} \). These subsets satisfy the condition that
\[
\begin{cases}
v \in P_i(d) & \iff \text{Frob}_v \in S'_{i,j} \\
\dim_{\mathbb{F}_p} \dim_{\mathbb{F}_p} v = j \text{ and } v \in P_i(d) & \iff \text{Frob}_v \in S_{i,j}
\end{cases}
\]
We refer to [KMR14] Proposition 9.4 for a detailed description of what these subsets are in \( \text{Gal}(F_{\sigma,\chi}/K) \).

**[Effective error bounds]**

Because the constant field of \( F_{\sigma,\chi} \) is \( \mathbb{F}_q \), we can use Theorem 3.1 to bound the error terms of the following equation:
\[
\left| \frac{\# \{ v \in P_i(d) \mid v \not\in \Sigma(\sigma) \text{ and } t_\chi(v) = j \} - \# \{ v \in P_i(d) \mid v \not\in \Sigma(\sigma) \} }{\# \{ v \in P_i(d) \mid v \not\in \Sigma(\sigma) \}} \right|.
\]

To apply Theorem 3.1, one needs to understand how the groups \( G \) as well as the genus \( g_{F_{\sigma,\chi}} \) grow in terms of \( \deg \sigma \). Recall that \( D_{E,p,q} > 0 \) is a constant defined as
\[
D_{E,p,q} := p^{\max_{\chi \in \Omega_E}(\text{rk}(\chi))}.
\]
Proposition 5.3 shows that
\[
\# \text{Gal}(F_{\sigma,\chi}/K) = [F_{\sigma,\chi} : K(E[p])] \leq D_{E,p,q} \cdot p^{2\# \Sigma(\sigma)} \cdot (p^3 - p)
\]
is a constant that only depends on the choice of the elliptic curve \( E, q, \) and \( p \). Recall that \( F_{\sigma,\chi}/K \) is unramified away from \( v \in \Sigma(\sigma) \). Hence, the Riemann-Hurwitz theorem implies that
\[
g_{F_{\sigma,\chi}} \leq D_{E,p,q} \cdot p^{2\# \Sigma(\sigma)} \cdot (p^3 - p) \cdot \# \Sigma(\sigma).
\]
Then one obtains that
\[
\# \text{Gal}(F_{\sigma,\chi}/K) + g_{F_{\sigma,\chi}} \leq D_{E,p,q} \cdot p^{2\# \Sigma(\sigma)} \cdot (p^3 - p) \cdot (1 + \# \Sigma(\sigma)) \\
\leq D_{E,p,q} \cdot p^{2\# \Sigma(\sigma)+4} \cdot \# \Sigma(\sigma)
\]
\[
\leq D_{E,p,q} \cdot p^{3\# \Sigma(\sigma)+4}
\]
Corollary 5.2 implies that for any \( d \) satisfying
\[
d > \frac{12 \log p + 2 \log D_{E,p,q} + (6 \log p) \cdot \# \Sigma(\sigma)}{\log q}
\]
the following inequality holds:
\[
\left| \frac{\# \{ v \in P_i(d) \mid v \not\in \Sigma(\sigma) \text{ and } t_\chi(v) = j \} }{\# \{ v \in P_i(d) \mid v \not\in \Sigma(\sigma) \}} - d_{i,j} \right| < \frac{16 \cdot D_{E,p,q} \cdot p^{3\# \Sigma(\sigma)+4} \cdot q^{-4}}{\log q}.
\]
Letting \( C_{E,p,q} = 16 \cdot D_{E,p,q} \cdot p^4 \) proves the statement of the theorem. \( \square \)
We will show that for almost all variation of 2-Selmer groups of certain subfamilies of quadratic twists of elliptic curves are governed by auxiliary places.

5.2. Given positive integers \( n > N \) and \( w > w' \), let \( \lambda \in \Lambda_{N,w}^{la} \) and \( \eta \in \Lambda_{n,N,w-w'}^{for} \). To do so, we introduce the notion of an auxiliary place of a polynomial \( f \in F_{n,w}(\mathbb{F}_q) \).

Definition 5.7. Let \( f \in F_n(\mathbb{F}_q) \). Denote by \( \overline{f} \), \( \overline{f}_* \), and \( \overline{f}^* \) the square-free polynomial over \( \mathbb{F}_q \) defined as

\[
\overline{f} := \prod_{g \in P_1 \cup P_2} g, \quad \overline{f}_* := \prod_{g \in P_1 \cup P_2} g \quad \text{and} \quad \overline{f}^* := \prod_{g \in P_1 \cup P_2} g
\]

(72)
i.e. they are products of irreducible factors of \( f \) (and \( f_* \) and \( f^* \), respectively) of degree greater than \( n \) which lies in \( P_1 \) or \( P_2 \).

Definition 5.8 (Auxiliary place). Given positive integers \( n > N \) and \( w > w' \), let \( \lambda \in \Lambda_{N,w}^{la} \) and \( \eta \in \Lambda_{n,N,w-w'}^{for} \) be splitting partitions.

- Given a degree \( n \) polynomial \( f \in F_{n,w}(\mathbb{F}_q) \), an auxiliary place of \( f \) is an irreducible polynomial \( g \in P_0 \) of maximal degree dividing \( f \). We denote by \( d_a \) the degree of an auxiliary place of any \( f \in F_{n,w}(\mathbb{F}_q) \). In particular, \( d_a \) is the maximal degree that guarantees \( \lambda_{i,0} = 0 \) for every \( i > d_a \).
- We denote by \( f_a \) the auxiliary factor of \( f \) defined as

\[
f_a := \prod_{g \in P_0(d_a)} g^{r_a(f)}.
\]

(73)
It is the product of all auxiliary places of $f$.

- We denote by $d_{a^*}$ the degree of the auxiliary factor of $f$, which can be written as
  \[ d_{a^*} := d_a \cdot \left( \sum_{j=1}^{n-1} \lambda_{d_a,j,0} \right). \]  

- Fix a polynomial $h \in F_{n-d_{a^*}}(\mathbb{F}_q)$. We define the following subset of $F_{(n,N),(w,w')}(\mathbb{F}_q)$:
  \[ F_{(n,N),(w,w')}(\mathbb{F}_q) := \left\{ f \in F_{(n,N),(w,w')}(\mathbb{F}_q) \mid \frac{f}{f_a} = h \right\} \]  

The above subset is empty if $h$ does not divide any polynomial in $F_{(n,N),(w,w')}(\mathbb{F}_q)$. By definition, the following relation holds:

\[ F_{(n,N),(w,w')}(\mathbb{F}_q) = \bigcup_{h \in F_{n-d_{a^*}}(\mathbb{F}_q)} F_{(n,N),(w,w')}(\mathbb{F}_q) \]

**Definition 5.9.** Let $f \in F_{n}(\mathbb{F}_q)$. We denote by $\Sigma_f$ the set of places

\[ \Sigma_f := \Sigma_E \cup \{ v \in \mathcal{P} \mid v \text{ divides } f_a \} \]

We note that if $f \in F_{(n,N),(w,w')}$, then $\#\Sigma_f = \#\Sigma_E + (w - w')$.

**Definition 5.10.** Given a polynomial $f \in F_{(n,N),(w,w')}(\mathbb{F}_q)$, we use the abbreviation $\Omega_T$ to denote the set of finite Cartesian products of local characters

\[ \Omega_1 = \prod_{v \in \Sigma_f} \text{Hom}(\text{Gal}(\overline{K_v}/K_v), \mu_p) \]

\[ \Omega_T = \prod_{v \in \Sigma_f} \text{Hom}(\text{Gal}(\overline{K_v}/K_v), \mu_p) \times \prod_{v \mid f^*_a \text{ and } v \mid f_a} \text{Hom}_{\text{ram}}(\text{Gal}(\overline{K_v}/K_v), \mu_p) \]

such that the component $\chi_v$ is ramified if $v | f^*$, and we ignore the local characters at any places $v$ dividing the auxiliary factor $f_a$ of $f$. In particular, we enlarge the set $\Sigma$ from Definition 5.1 to include places $v | f_a$ and set $\Sigma = \Sigma_f$, even though $\chi_{f,v}$ is ramified at such places.

In order to make this reformulation more concrete, we present an alternative way to define the subset $F_{(n,N),(w,w')}(\mathbb{F}_q)$ given partitions $\lambda := \{ (\lambda_{i,j,k}, i, j, k) \} \in \Lambda_{N,w}^{ad}$ and $\eta := \{ (\eta_{i,j,k}, \hat{i}, \hat{j}, \hat{k}) \} \in \Lambda_{n,N,w-w'}^{for}$. Given a set $X$, we denote by

\[ \text{PConf}_n(X) := \{ (x_1, \cdots, x_n) \in X^{\otimes n} \mid x_i \neq x_j \text{ for all } 1 \leq i < j \leq n \} \]

the set-theoretic ordered configuration set of $n$ elements in $X$. There is a transitive action of the symmetric group $S_n$ on $\text{PConf}_n(X)$, which prompts us to define

\[ \text{Conf}_n(X) := \text{PConf}_n(X)/S_n \]

the set-theoretic unordered configuration set of $n$ elements in $X$. Using these notations, we can define the subset $F_{(n,N),(w,w')}(\mathbb{F}_q)$ as

\[ F_{(n,N),(w,w')}(\mathbb{F}_q) := \prod_{i \neq j} \text{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i)) \times \prod_{\hat{i} \neq \hat{j}} \text{Conf}_{\eta_{i,j,k}}(\mathcal{P}_{\hat{k}}(\hat{i})) \]
where we regard \( \text{Conf}_0(X) = \{0\} \). In particular, if a polynomial \( f \in F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) \) admits an irreducible factorization via

\[
f^* := \prod_{i,j,k} \lambda_{i,j,k} \prod_{m=1} \phi_{i,j,k,m}^m \quad f_* := \prod_{i,j,k} \eta_{i,j,k} \prod_{m=1} h_{i,j,k,m}^m
\]

where \( \{\phi_{i,j,k,m}\} \) and \( \{h_{i,j,k,m}\} \) are sets of irreducible factors of \( f \), then under this identification a polynomial \( f \in F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) \) can be represented as an element

\[
\left( \prod_{i,j,k} \phi_{i,j,k}^{\lambda_{i,j,k}} \right) \times \left( \prod_{i,j,k} h_{i,j,k}^{\eta_{i,j,k}} \right)
\]

(83)

Using this identification, we can reformulate Definition 5.8 as follows. There is a natural projection map

\[
\phi_{da} : \prod_{i,j,k} \text{Conf}_{\lambda_{i,j,k}}(P_k(i)) \times \prod_{i,j,k} \text{Conf}_{\eta_{i,j,k}}(P_k(i)) \to \prod_{i,j,k} \text{Conf}_{\lambda_{i,j,k}}(P_k(i)) \times \prod_{i,j,k} \text{Conf}_{\eta_{i,j,k}}(P_k(i))
\]

which forgets all the irreducible factors of \( f \in F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) \) lying in \( \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{da},j,0}(P_0(d_a)) \). Then

\[
F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) = \phi_{da}^{-1}(h),
\]

(84)

where \( h \in F_{n-d_a}(\mathbb{F}_q) \) such that \( h \mid f \) for some \( f \in F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) \).

Using the notations introduced in this subsection, an immediate result of Corollary 4.17 can be stated as follows.

**Corollary 5.11.** Fix a locally arrangeable partition \( \lambda \in \Lambda_{n,w'}^{for} \) and a forgettable partition \( \eta \in \Lambda_{n,N,w-w'}^{for} \). Fix a polynomial \( h \in F_{n-d_a}(\mathbb{F}_q) \). Suppose the set \( F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) = \phi_{da}^{-1}(h) \) is non-empty and \( w \leq 2m_{n,q} \). Denote by \( h_1, h_2, \ldots, h_w(h) \) the irreducible factors of \( h \). Denote by \( \hat{w}(h) \) the quantity

\[
\hat{w}(h) := \begin{cases} 
\frac{w(h)}{2} & \text{if } K(\sqrt[w_1]{h}, \ldots, \sqrt[w_w(h)]{h}) \cap K(E[p]) = K \text{ or } p \geq 5 \\
\frac{w(h) - 1}{2} & \text{if } K(\sqrt[w_1]{h}, \ldots, \sqrt[w_w(h)]{h}) \cap K(E[p]) \neq K \text{ and } p \leq 3
\end{cases}
\]

Let \( \chi := (\chi_v)_v \in \Omega_{\text{T}} \) be any product of local characters, whose components are ramified at places \( v \mid h \) and unramified elsewhere such that there exists \( f \in \phi_{da}^{-1}(h) \) such that \( \text{Ker}(\chi_{f,x}) = \text{Ker}(\chi_v) \) for all \( v \in \Sigma(h) \). Then we have

\[
\left| \frac{\{f \in \phi_{da}^{-1}(h) \mid \text{Ker}(\chi_{f,v}) = \text{Ker}(\chi_v) \forall v \in \Sigma(h)\}}{\#\phi_{da}^{-1}(h)} \right| - \frac{1}{p^{\hat{w}(h)}} < \hat{C}_{E,p,q} \cdot (n \log q - 2m_{n,q} + 2 \log p),
\]

where \( \hat{C}_{E,p,q} > 0 \) is the constant introduced from Corollary 4.17.

The condition that \( \text{Ker}(\chi_{f,v}) = \text{Ker}(\chi_v) \) as subgroups of \( \text{Gal}(K_v/K_v) \) for each place \( v \in \Sigma(h) \) implies that the fixed fields \( K_v^{\text{Ker}(\chi_{f,v})} \) and \( K_v^{\text{Ker}(\chi_v)} \), which are cyclic ramified extensions of degree \( p \) over \( K_v \), are equal to each other.
Proof. We note that there exists a bijection between the following sets:

\[
\phi_{d_a^{-1}}(h) \rightarrow \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{d_a},j,0}(\mathcal{P}_0(d_a))
\]

\[
f = hf_a \mapsto f_a
\]

There is an \(\prod_{j=1}^{p-1} S_{\lambda_{d_a},j,0}\)-equivariant covering map

\[
F : \prod_{j=1}^{p-1} \text{PConf}_{\lambda_{d_a},j,0}(\mathcal{P}_0(d_a)) \rightarrow \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{d_a},j,0}(\mathcal{P}_0(d_a))
\]

where for any fixed \(f_a\), every element in \(F^{-1}(f_a)\) restricts to an identical character in \(\Omega_T\). It hence suffices to compute the desired probability over the ordered configuration set \(\text{PConf}_{\lambda_{d_a},j,0}(\mathcal{P}_0(d_a))\). This can be achieved by applying Corollary \[4.11\] and using the fact that every ramified cyclic degree \(p\) extension of \(K_v\) is obtained from adjoining to \(K_v\) the \(p\)-th roots of elements of form \(\pi_v u^i\), where \(\pi_v\) is a uniformizer of \(K_v\). \(u \in K_v^\times/(K_v^\times)^p\) is non-trivial, and \(0 \leq i \leq p - 1\). \(\square\)

Definition 5.12. Given a locally arrangeable partition \(\lambda \in \Lambda^a_{n-N,w-w'}\) and a forgettable partition \(\eta \in \Lambda^l_{n-N,w-w'}\), consider the set of polynomials \(F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)\).

Fix \(1 \leq j^* \leq p - 1\) and \(0 \leq k^* \leq 2\). Let \(d\) be an integer such that \(d \neq d_a\) and \(\lambda_{d,j^*,k^*} \neq 0\).

1. We denote by \(\phi_{d,j^*,k^*}\) the canonical projection map

\[
\phi_{d,j^*,k^*} : F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) \rightarrow \prod_{i,j,k} \text{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(1)) \times \prod_{i,j,k} \text{Conf}_{\eta_{i,j,k}}(\mathcal{P}_k(1))
\]

which forgets the irreducible factors of \(f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)\) lying in the set

\[
\text{Conf}_{\lambda_{d,j^*,k^*}}(\mathcal{P}_k(d)) \times \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{d,a,j,0}}(\mathcal{P}_0(d_a)).
\]

2. Denote by \(D := n - d_a - d \cdot j^* \cdot \lambda_{d,j^*,k^*}\). Let \(h \in F_D(\mathbb{F}_q)\) be a polynomial such that \(h \mid f\) for some \(f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)\). Denote by \(\phi_{d,j^*,k^*}(h) \subset F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)\) the set of fibers of \(\phi_{d,j^*,k^*}\) at \(h\). This set admits the following bijection:

\[
\phi_{d,j^*,k^*}(h) \cong \text{Conf}_{\lambda_{d,j^*,k^*}}(\mathcal{P}_k(d)) \times \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{d,a,j,0}}(\mathcal{P}_0(d_a))
\]

The upcoming proposition combines equidistribution of characters from Corollary \[5.11\] and the Chebotarev conditions from Proposition \[5.3\] and Proposition \[5.4\]. This allows us to obtain the distribution of changes in dimensions of local Selmer groups of \(E\) associated to consecutive twists of local characters.

Proposition 5.13. Assume the notations and conditions as stated in Definition \[5.12\]. Let \(E/K\) be an elliptic curve satisfying conditions in \[5.10\]. Given \(f \in \phi_{d,j^*,k^*}^{-1}(h)\), let \(\omega_f\) and \(\omega'_f\) be defined as

\[
\omega_f := (\chi_f,v)_{v \in \Sigma_f(\mathcal{P})} \in \Omega^\mathcal{P}_h, \quad \omega'_f := (\chi_f,v)_{v \in \Sigma_f(\mathcal{P})} \in \Omega^\mathcal{P}
\]
Denote by $\delta_h : \mathbb{Z}_{\geq 0} \to [0, 1]$ the probability distribution
\[
\delta_h(J) := \frac{\#\{ f \in \phi_{d,j^*,k^*}^{-1}(h) \mid rk(\omega_f) = J \}}{\#\phi_{d,j^*,k^*}^{-1}(h)}.
\] (88)

Let $k := \lambda_{d,j^*,k^*} \cdot k^*$. Then for any $n$ such that $m_{n,q} > \max\{\deg E, 3 \cdot \log p\}$, there exists a fixed constant $B_{E,p,q} > 0$ dependent only on $E, p, q$ such that
\[
\frac{\#\{ f \in \phi_{d,j^*,k^*}^{-1}(h) \mid rk(\omega'_f) = J \}}{\#\phi_{d,j^*,k^*}^{-1}(h)} - (M_k^p \delta_h)(J) < \lambda_{d,j^*,k^*} \cdot B_{E,p,q} \cdot (n \log q)^{-2m_{n,q} + 6 \log p + 1}.
\] (89)
where $M_k := [p_{r,s}]$ is the Markov operator over $\mathbb{Z}_{\geq 0}$ given by
\[
p_{r,s} = \begin{cases} 1 - p^{-r} & \text{if } s = r - 1 \geq 0 \\ p^{-r} & \text{if } s = r + 1 \\ 0 & \text{else} \end{cases}
\]

**Proof.** We prove by induction on the values of $\lambda_{d,j^*,k^*}$. The induction step becomes straightforward once one shows the base cases, where $\lambda_{d,j^*,k^*} = 1$.

[[Base Case]]

Definition [5.12] implies that
\[
\phi_{d,j^*,k^*}^{-1}(h) = \mathcal{P}_{k^*}(d) \times \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{d,j^*,0}(\mathcal{P}_0(d_a))} = \mathcal{P}_{k^*}(d) \times \phi_{d_a}^{-1}(h).
\]

By Corollary [5.11] and the condition that $w \leq 2m_{n,q}$, for any fixed $g \in \mathcal{P}_{k^*}(d)$ and any $\omega := (\omega_0) \in \Omega_T$, there exists an explicit constant $\hat{C}_{E,p,q} > 0$ such that
\[
\frac{\#\{ f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \frac{f}{f_a \cdot h} = g, \text{Ker}(\chi_{f,g}) = \text{Ker}(\omega_g) \}}{\#\phi_{d_a}^{-1}(h)} - \frac{1}{p} < \hat{C}_{E,p,q} \cdot (n \log q)^{-2m_{n,q} + 2 \log p}.
\] (90)

We note that
\[
\#\{ f \in \phi_{d,j^*,k^*}^{-1}(h) \mid rk(\omega'_f) = J_1, rk(\omega_f) = J_0 \}
= \sum_{g \in \mathcal{P}_{k^*}(d)} \#\{ f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \frac{f}{f_a \cdot h} = g, rk(\omega'_f) = J_1, rk(\omega_f) = J_0 \}
\] (91)

Each summand
\[
\#\{ f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \frac{f}{f_a \cdot h} = g, rk(\omega'_f) = J_1, rk(\omega_f) = J_0 \}
\] (92)

can be evaluated as
\[
\begin{cases} \#\phi_{d_a}^{-1}(h) \cdot \delta_{h,g}(J_0) & \text{if } rk(\omega'_f) - rk(\omega_f) = J_1 - J_0 \\ 0 & \text{otherwise} \end{cases}
\]

where $\delta_{h,g} : \mathbb{Z}_{\geq 0} \to [0, 1]$ is a probability distribution defined as
\[
\delta_{h,g}(J) := \frac{\#\{ f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \frac{f}{f_a \cdot h} = g, rk(\omega_f) = J \}}{\#\phi_{d_a}^{-1}(h)}.
\] (93)

By definition, the following equation holds for all $J \in \mathbb{Z}_{\geq 0}$:
\[
\delta_h(J) = \frac{1}{\#\mathcal{P}_{k^*}(d)} \sum_{g \in \mathcal{P}_{k^*}(d)} \delta_{h,g}(J).
\] (94)
Suppose we have two products of local characters \( \omega = (\omega_v)_v \) and \( \omega' = (\omega'_v)_v \) in \( \Omega_T \). The definitions of local Selmer groups \( \text{Sel}(E[p], \omega) \) and \( \text{Sel}(E[p], \omega') \) and the fact that the local conditions at \( v \in \mathcal{P}_0 \) do not affect the dimensions of local Selmer groups imply that if \( \text{Ker}(\omega_v) = \text{Ker}(\omega'_v) \) for all \( v \in \Sigma_f(\mathcal{P}_0) \), then

\[
\text{rk}(\omega_v)_{v \in \Sigma_f(\mathcal{P}_0)} = \text{rk}(\omega'_v)_{v \in \Sigma_f(\mathcal{P}_0)}. \tag{95}
\]

(And if in addition \( \text{Ker}(\omega_v) = \text{Ker}(\omega'_v) \) for the given \( g \in \mathcal{P}_k(d) \), then we can further guarantee that the dimensions of \( \text{Sel}(E[p], \omega) \) and \( \text{Sel}(E[p], \omega') \) are equal to each other.)

Equation (95) and Corollary 5.11 imply that for any \( g \in \mathcal{P}_k(d) \),

\[
\sup_{J \in \mathbb{Z}_{\geq 0}} |\delta_h(J) - \delta_{h,g}(J)| < \hat{C}_{E,p,q} \cdot (n \log q)^{-2m_{n,q}+4\log p}. \tag{96}
\]

We note that the exponent for \( n \log q \) changes from \(-2m_{n,q} + 2\log p\) to \(-2m_{n,q} + 4\log p\) because there are at most \( p^{2m_{n,q}} \leq (n \log q)^{2\log p} \) many ramified cyclic extensions over local fields one needs to consider to determine the dimensions of local Selmer groups.

Combining equations (90), (91), and (96), we obtain for any given \( g \in \mathcal{P}_k(d) \) and \( J_0 \in \mathbb{Z}_{\geq 0} \),

\[
\left| \left( \sum_{g \in \mathcal{P}_k^*(d)} \frac{\#\{\omega' \in \Omega_{\omega,f,g} \mid \text{rk}(\omega') - \text{rk}(\omega_f) = J_1 - J_0\}}{\#\Omega_{\omega,f,g}} \right) \right| < \#\phi^{-1}_{d_0}(h) \cdot \phi^{-1}_{d_0}(h) \cdot \delta_h(J_0). \tag{97}
\]

where the notations \( \Omega_{\omega,g} \) were introduced in Definition 5.2. Regardless of the choice of \( g \in \mathcal{P}_k(d) \), we have \( \#\Omega_{\omega,f,g} = p(p - 1) \). Hence, we have

\[
\sum_{g \in \mathcal{P}_k^*(d)} \frac{\#\{\omega' \in \Omega_{\omega,f,g} \mid \text{rk}(\omega') - \text{rk}(\omega_f) = J_1 - J_0\}}{\#\Omega_{\omega,f,g}} = \#\mathcal{P}_k(d) \cdot \sum_{g \in \mathcal{P}_k^*(d)} \frac{\#\{\omega' \in \Omega_{\omega,f,g} \mid \text{rk}(\omega') - \text{rk}(\omega_f) = J_1 - J_0\}}{\#\Omega_{\omega,f,g}}.
\]

Take summation of variants of equations (97) over all \( g \in \mathcal{P}_k(d) \) and use equation (94) to obtain

\[
\left| \left( \sum_{g \in \mathcal{P}_k^*(d)} \frac{\#\{\omega' \in \Omega_{\omega,f,g} \mid \text{rk}(\omega') - \text{rk}(\omega_f) = J_1 - J_0\}}{\#\Omega_{\omega,f,g}} \right) \right| < \#\phi^{-1}_{d_{0},k} \cdot \phi^{-1}_{d_{0},k} \cdot \delta_h(J_0) \cdot (n \log q)^{-2m_{n,q}+4\log p} \tag{98}
\]

Because we assume that \( d > n = \frac{4m_{n,q}^2}{\log q} \) and \( w \leq 2m_{n,q} \), it follows that as long as \( m_{n,q} > \deg \Delta_E \), the conditions for applying Proposition 5.3 hold. Fix \( w \in \Omega_T^* \) such that \( \text{rk}(\omega) = J_0 \). Proposition 5.3 and Proposition 5.4 show that there exists a fixed constant \( C_{E,p,q} > 0 \) depending only on the elliptic curve \( E \), \( p \), and \( q \) such that

\[
\left| \sum_{g \in \mathcal{P}_k^*(d)} \frac{\#\{\omega' \in \Omega_{\omega,g} \mid \text{rk}(\omega') - \text{rk}(\omega) = J_1 - J_0\}}{\#\mathcal{P}_k(d)} \right| < C_{E,p,q} \cdot (n \log q)^{-2m_{n,q}+6\log p+1}. \tag{99}
\]

The constants \( c_{k^*,J_1-J_0} \) are probabilities obtained from this table, see for example [KMTR14, Proposition 9.5] on how the table from Proposition 5.4 is related to the table provided below.
It is straightforward to show that the above entries are represented by probabilities obtained from the Markov operator $M_L$ and $M_L^2$. To elaborate,

\[
\begin{align*}
    c_{1,-1} &= p_{J_0, J_0-1} \\
    c_{1,1} &= p_{J_0, J_0+1} \\
    c_{2,-2} &= p_{J_0, J_0-1} \cdot p_{J_0-1, J_0-2} \\
    c_{2,0} &= p_{J_0, J_0-1} \cdot p_{J_0-1, J_0} + p_{J_0, J_0+1} \cdot p_{J_0+1, J_0} \\
    c_{2,2} &= p_{J_0, J_0+1} \cdot p_{J_0+1, J_0+2}.
\end{align*}
\]

Combining equations (98) and (99) and summing up $\delta_h(J_0)$ over 5 possible values of $J_0$, we obtain

\[
\frac{|\#\phi_{d,j,k^*}^{-1}(h)|}{\#\phi_{d,j,k^*}(h)} = (M_L^{k^*} \delta_h)(J_1) < B_{E,p,q} \cdot ((n \log q)^{-2m_n,q} + 6 \log p + 1),
\]

where $B_{E,p,q} = 5 \cdot (2p \cdot \hat{C}_{E,p,q} + C_{E,p,q})$. This proves the base case of the proposition.

\[[\text{Induction Step}]\]

To prove the cases where $\lambda_{d,j^*, k^*} > 1$, we note that

\[
\phi_{d,j^*, k^*}^{-1}(h) = \text{Conf}_{\lambda_{d,j^*, k^*}}(\mathcal{P}(d)) \times \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{d,a,j,0}}(\mathcal{P}_0(d_a))
\]

There is a natural $S_{\lambda_{d,j^*, k^*}}$-equivariant projection map

\[
F : \text{PConf}_{\lambda_{d,j^*, k^*}}(\mathcal{P}(d)) \times \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{d,a,j,0}}(\mathcal{P}_0(d_a)) \to \phi_{d,j^*, k^*}^{-1}(h)
\]

Note that for any fixed $f \in \phi_{d,j^*, k^*}^{-1}(h)$, every element in $F^{-1}(f)$ restricts to an identical character in $\Omega_T$. Therefore, it suffices to compute the desired probability over the set

\[\text{PConf}_{\lambda_{d,j^*, k^*}}(\mathcal{P}(d)) \times \prod_{j=1}^{p-1} \text{Conf}_{\lambda_{d,a,j,0}}(\mathcal{P}_0(d_a)).\]

By definition, we have the equation

\[
\#\text{PConf}_{\lambda_{d,j^*, k^*}}(\mathcal{P}(d)) = \prod_{m=1}^{\lambda_{d,j^*, k^*}} (\mathcal{P}_k^*(d) - m + 1)
\]

Hence, by iterating the base case $\lambda_{d,j^*, k^*}$ many times, we obtain that

\[
\frac{|\#\{f \in \phi_{d,j^*, k^*}^{-1}(h) \mid \text{rk}(\omega_f) = J_1, \text{rk}(\omega_f) = J_0\}|}{\#\phi_{d,j^*, k^*}^{-1}(h)} = (M_L^{k^*} \delta_h)(J_1)
\]

\[
< \lambda_{d,j^*, k^*} \cdot B_{E,p,q} \cdot ((n \log q)^{-2m_n,q} + 6 \log p + 1).
\]

\]
Remark 5.14. One may regard Proposition 5.13 as an effective version of [KMR14, Theorem 4.3, Theorem 9.5]. Instead of using fan structures, we consider a subset of polynomials over $\phi_{d,j,k}(h)$ to show that the Markov chain $M_L$ governs the probability distribution of ranks of local Selmer groups with explicitly computable rate of convergence.

6. Global Selmer groups

The goal of this section is to use the probability distribution of $\text{rk}((\chi_{f,v})_v)$ ranging over $F_{(n,N),(w,w')}^\kappa(\mathbb{F}_p)$ (Proposition 5.13) to prove the statement of the main theorem.

6.1. Governing Markov operator. We will use the Markov operator constructed from [KMR14], known as the mod $p$ Lagrangian operator, to analyze variations of $\pi$-Selmer ranks of a subfamily of global quadratic twists of elliptic curves over $K$ satisfying the conditions from Theorem 1.2.

Definition 6.1. Let $M_L = [p_{r,s}]$ be the operator over the state space of non-negative integers $\mathbb{Z}_{\geq 0}$ given by

$$p_{r,s} = \begin{cases} 1 - p^{-r} & \text{if } s = r - 1 \geq 0 \\ p^{-r} & \text{if } s = r + 1 \\ 0 & \text{else} \end{cases}$$

Remark 6.2. The construction of the mod $p$ Lagrangian Markov operator dates back to previous works by [SD08] and [KMR14]. Other references such as [Smi17], [Smi20], and [FLR23] also use Markov chains to obtain the probability distribution of $p$-Selmer groups of certain families of elliptic curves.

We list some crucial properties the operator $M_L$ satisfies, the proof of which can be found in [KMR14, Section 2].

Definition 6.3. Let $\mu : \mathbb{Z}_{\geq 0} \to [0, 1]$ be a probability distribution over the state space of non-negative integers $\mathbb{Z}_{\geq 0}$. The parity of $\mu$ is the sum of probabilities at odd state spaces, i.e.

$$\rho(\mu) := \sum_{n \text{ odd}} \mu(n)$$

Proposition 6.4. [KMR14 Proposition 2.4]

Let $E^+, E^- : \mathbb{Z}_{\geq 0} \to [0, 1]$ be probability distributions such that

$$E^+(n) = \begin{cases} \prod_{j=1}^\infty (1 + p^{-j})^{-1} \prod_{j=1}^n \frac{p^j}{p^j - 1} & \text{if } n \text{ even} \\ 0 & \text{if } n \text{ odd} \end{cases}$$

$$E^-(n) = \begin{cases} 0 & \text{if } n \text{ even} \\ \prod_{j=1}^\infty (1 + p^{-j})^{-1} \prod_{j=1}^n \frac{p^j}{p^j - 1} & \text{if } n \text{ odd} \end{cases}$$

Let $\mu : \mathbb{Z}_{\geq 0} \to [0, 1]$ be a probability distribution. Then

$$\lim_{k \to \infty} M_L^{2k}(\mu) = (1 - \rho(\mu))E^+ + \rho(\mu)E^-$$

$$\lim_{k \to \infty} M_L^{2k+1}(\mu) = \rho(\mu)E^+ + (1 - \rho(\mu))E^-.$$ 

In particular, if $\rho(\mu) = \frac{1}{2}$, then

$$\lim_{k \to \infty} M_L^k(\mu)(n) = \prod_{j=0}^\infty (1 + p^{-j})^{-1} \prod_{j=1}^n \frac{p^j}{p^j - 1}$$ (106)
Remark 6.5. Note that $M_L^2$ is an aperiodic, irreducible, and positive-recurrent Markov chain over the state space of positive odd integers $\mathbb{Z}_{odd,\geq 0}$ and non-negative even integers $\mathbb{Z}_{even,\geq 0}$. The unique stationary distributions of the Markov chain are $E^-(n)$ and $E^+(n)$, respectively.

Given that $M_L^2$ is aperiodic, irreducible, and positive-recurrent, it is natural to ask what the rate of convergence of $M_L$ is. Assuming certain conditions on the initial probability distribution over the state space and the stationary distribution of $M$, the geometric rate of convergence of $M$ can be verified using the following theorem.

Theorem 6.6 (Geometric ergodic theorem for Markov chains). [MT93 Theorem 15.0.1]

Let $M$ be an irreducible, aperiodic, and positive-recurrent Markov chain over a countable state space $\mathcal{X} := (x_n)_{n\in\mathbb{Z}}$. Let $X_1, X_2, \ldots, X_n, \cdots : \mathcal{X} \to [0,1]$ be a sequence of random variables which satisfies

$$X_{n+1} = M(X_n)$$

for all $n$. Let $\pi$ be an invariant probability distribution of $M$ (not necessarily unique). Suppose $V : X \to [1, \infty)$ is a function such that $\lim_{n\to\infty} V(x_n) = \infty$. If there exists $0 < \rho < 1$ and $\kappa > 0$ such that for all but finitely many $x_n \in \mathcal{X}$,

$$\mathbb{E}[V(M(X_n))] | X_n = x_k] - V(x_k) \leq -\rho V(x_k) + \kappa$$

then there exists a constant $0 \leq \gamma < 1$ and a constant $c > 0$ such that for any probability distribution $\mu$ over $X$ and every $n \in \mathbb{N}$,

$$\sup_{z \in \mathcal{X}} |M^n(\mu)(z) - \pi| < c\gamma^n(\mu V + 1)$$

where the term $\mu V$ is the expected value of $V$ under the probability distribution $\mu$, i.e. $\mu V := \mathbb{E}[V(x) | x \in \mu]$. In fact, one can choose $\gamma = 1 - \rho$.

Let $I$ be the identity operator over the countable state space $\mathbb{Z}_{\geq 0}$. Proposition 5.4 implies that the Markov chain

$$\left(1 - \frac{p}{(p^2 - 1)}\right) \cdot I + \frac{1}{p} M_L + \frac{1}{(p^3 - p)} M_L^2$$

over the state space $\mathbb{Z}_{\geq 0}$ governs the differences between the dimensions of two local Selmer groups $\text{Sel}(E[p],\chi')$ and $\text{Sel}(E[p],\chi)$ where $\chi' \in \Omega_{\chi',\mathfrak{v}}$ for some place $\mathfrak{v}$, i.e. except at the place $\mathfrak{v}$, the Cartesian product of local characters $\chi'$ is identical to $\chi$. Proposition 6.4 also shows that regardless of the parity of the initial probability distribution over the state space $\mathbb{Z}_{\geq 0}$, the stationary distribution of the Markov chain from (108) is given by the Poonen-Rains distribution as stated in (106). One can also show that given a fixed prime number $p$, the Markov chain of our interest is an irreducible aperiodic Markov chain over the countably infinite state space $\mathbb{Z}_{\geq 0}$. In fact, it is geometrically ergodic over $\mathbb{Z}_{\geq 0}$ (without requiring the restriction that $p = 2$).

Corollary 6.7. Let $\mu : \mathbb{Z}_{\geq 0} \to [0,1]$ be a probability distribution over the state space $\mathbb{Z}_{\geq 0}$. Denote by $\pi$ the stationary probability distribution of the Markov operator given by

$$M := \left(1 - \frac{p}{(p^2 - 1)}\right) \cdot I + \frac{1}{p} M_L + \frac{1}{(p^3 - p)} M_L^2.$$ (110)

for some fixed prime number $p$ and a finite cyclic group $T$. Fix any positive number $\beta > 1$. Then for every $n \in \mathbb{N}$, there exists a constant $0 \leq \gamma < 1$ and a constant $c > 0$ such that

$$\sup_{z \in \mathcal{X}} \left| \left(\left(1 - \frac{p}{(p^2 - 1)}\right) \cdot I + \frac{1}{p} M_L + \frac{1}{(p^3 - p)} M_L^2\right)^n(\mu) - \pi \right| < c\gamma^n(\beta\mu + 1)$$ (111)
where the term \( \beta^\mu \) is the expected value of the function \( V(x) = \beta^x \) under the probability distribution \( \mu \), i.e. \( \beta^\mu := \mathbb{E}[\beta^x \mid x \in \mu] \). Explicitly, the rate of convergence \( \gamma \) satisfies

\[
1 - \frac{p}{p^2 - 1} < \gamma < 1
\]  

(112)

Proof. Fix any positive number \( \beta > 1 \). Set \( V(x) = \beta^x \). Computational results then show that there exists a fixed constant \( \kappa > 0 \) such that for every \( x \in \mathbb{Z}_{\geq 0} \),

\[
\mathbb{E} \left[ \beta^{X_n} \mid X_{n-1} = x \right] - \beta^x = - \left( \frac{p}{(p^2 - 1)} - \frac{1}{p\beta} - \frac{1}{(p^3 - p)\beta^2} \right) \cdot \beta^x + \kappa.
\]

Setting \( \gamma = 1 - \frac{p}{(p^2 - 1)} + \frac{1}{p\beta} + \frac{1}{(p^3 - p)\beta^2} \), the corollary follows from Theorem 6.6.

The rate of convergence of the Markov chain \( M \) from (109) is hence given by \( 1 - \frac{p}{(p^2 - 1)} + \epsilon \) for some positive number \( \epsilon > 0 \). We note that this rate of convergence corresponds to the other error term (that does not appear in Proposition 4.14) constituting the constant \( \alpha(p) \) defined in Theorem 1.2. A common choice of \( \beta \) is to take \( \beta = p \), which yields the rate of convergence to be equal to \( \gamma = 1 - \frac{p^2 - p + 1}{p^3 - p} \). For example, when \( p = 2 \), the rate of convergence of \( M \) is greater than \( \frac{1}{3} \), and is given by \( \frac{5}{8} \) when one chooses \( \beta = 2 \).

It now remains to show that the stationary distribution of the desired Markov chain (109) is the probability distribution conjectured by Poonen-Rains [BKJ+15].

Lemma 6.8. Let \( p \) be any fixed prime number. Then the probability distribution

\[
PR(j) := \prod_{j \geq 0}^\infty (1 + p^{-j})^{-1} \prod_{j=1}^n \frac{p}{p^j - 1}
\]  

(113)

is the unique stationary distribution of the Markov chain

\[
M := \left( 1 - \frac{p}{(p^2 - 1)} \right) \cdot I + \frac{1}{p} M_L + \frac{1}{(p^3 - p)} M_L^2.
\]  

(114)

Proof. Note that the operators \( I \) and \( M_L^2 \) are parity preserving Markov operators, whereas \( M_L \) is a parity reversing Markov operator. Because \( M \) is aperiodic and irreducible, it follows that \( M \) has a unique stationary distribution \( \pi \). The following relation holds for the parity of \( \pi \), which is obtainable by comparing the parity between \( \pi \) and \( M(\pi) \).

\[
\rho(\pi) = \left( 1 - \frac{1}{p} \right) \rho(\pi) + \frac{1}{p} (1 - \rho(\pi)) = \left( 1 - \frac{2}{p} \right) \rho(\pi) + \frac{1}{p}.
\]  

(115)

Therefore, we obtain that \( \rho(\pi) = \frac{1}{2} \). Using Proposition 6.4 and the fact that the Markov chain \( M \) is aperiodic and irreducible, we immediately obtain the statement of the lemma.

Remark 6.9. One crucial result from using Corollary 6.7 and Lemma 6.8 is that the stationary distribution of applying the Markov chain from (109) is equal to the Poonen-Rains distribution regardless of the initial probability distribution. Furthermore, as long as the initial probability distribution is finitely supported, we can also ensure that the Markov chain converges to the stationary distribution at a geometric convergence rate.

Remark 6.10. We note that the Markov chain constructed from Smith’s work is different from the Markov chain presented in this manuscript [Sm22a, Sm22b]. The sequence of random variables \( X_n \) Smith considers correspond to the empirical probability distribution of the subspace

\[
\dim_{\mathbb{F}_p} \pi^{n-1} \text{Sel}_{\pi^n}(E^X) \subset \text{Sel}_{\pi}(E)
\]  

(116)
where $\chi$ ranges over grids of twists [Smi22a, Chapter 6]. Here, the grids of twists are defined as a finite Cartesian product of collections of prime ideals, where each collection contains prime ideals whose symbols are equal to each other [Smi22a, Definition 4.13].

To elaborate, this manuscript regards the variable $n$ from a sequence of random variables $\{X_n\}_{n \in \mathbb{Z}}$ as the number of distinct irreducible places, whereas Smith’s work regards the variable $n$ from a sequence of random variables $\{X_n\}_{n \in \mathbb{Z}}$ as a quantifier for detecting elements inside higher $\pi^n$-Selmer groups which also lie inside the $\pi$-Selmer group of $E$.

6.2. **Relating global and local Selmer groups.** We now obtain the desired probability distribution of dimensions of $\text{Sel}_\pi(E^{x_f})$ over $f \in F_n(\mathbb{F}_q)$ by approximating it with distribution of dimensions of local Selmer groups of $E$ associated to restrictions of $\chi_f$, as stated in Proposition 5.13.

**Proposition 6.11.** Let $n > N$ and $w < 2m_{n,q}$ be positive integers. Let $w'$ be a positive integer such that $w' = (1 - \epsilon)w$ for some small enough $0 < \epsilon < 1$.

Suppose that $n$ satisfies the following inequality

$$m_{n,q} > \max\left(e^{e^e}, \deg \Delta_E, 6 \log p + 2\right)$$

(117)

Then for any $\beta > 1$, there exists a fixed constant $\tilde{B}_{E,p,q,\beta}$ depending only on $E, p, q, \beta$ such that

$$\left| \frac{\# \{f \in \tilde{F}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \dim_{\mathbb{F}_p} \text{Sel}_\pi(E^{x_f}) = J \} - PR(J)}{\# \tilde{F}_{(n,N),(w,w')}(\mathbb{F}_q)} \right|$$

$$< \tilde{B}_{E,p,q,\beta} \cdot (n \log q)^{4t \log \beta} \cdot \left((n \log q)^{-m_{n,q}} + \left(1 - \frac{p}{p^2 - 1} + \frac{1}{p\beta} + \frac{1}{(p^3 - p)\beta^2}\right)^{w'-1}\right)$$

(118)

where $\tilde{F}_{(n,N),(w,w')}(\mathbb{F}_q)$ is a subset of $F_n(\mathbb{F}_q)$ as stated in Definition 4.11.

As stated in previous sections, the error term appearing in Proposition 6.11 corresponds to one of the error terms constituting the constant $\alpha(p)$ defined in Theorem 1.2.

**Proof.** [[Setup]]

Before presenting the proof of the proposition, we first outline the set of notations utilized in the proof. We recall that there exists a $\text{Gal}(\overline{K}/K)$-equivariant isomorphism

$$E^{x_f}\mid_\pi \cong E[p]$$

(119)

see [MR07] Proposition 4.1] for the proof. This implies that the $\pi$-Selmer group of $E^{x_f}$ satisfies

$$\text{Sel}_\pi(E^{x_f}) \subset H^1_\text{ét}(K, E[p])$$

(120)

and the image of the local Kummer maps $\text{im} \delta^\pi_v$ are Lagrangian subspaces of $H^1_\text{ét}(K_v, E[p])$ for each place $v$ of $K$. The $\pi$-Selmer group of $E^{x_f}$ is hence the local Selmer group of $E$ associated to the Cartesian product $\chi_{f,v}$ arising from restrictions of the global character $\chi_f$ to cyclic order-$p$ local characters over some local fields $K_v$. We concretely have

$$\text{Sel}_\pi(E^{x_f}) = \text{Sel}(E[p], (\chi_{f,v})_{v \in \Sigma_f}^{\mathcal{T}}) \in \Omega^{\mathcal{T}}.$$  

(121)

The relation between $\pi$-Selmer groups and local Selmer groups also holds over number fields as well, see for example [KM01] Chapter 10.

For each positive integer $1 \leq z \leq w'$, let

$$d_z := \min\{d > n \mid \sum_{i=n+1}^{d} \sum_{j=1}^{p-1} \sum_{k=0}^{2} \lambda_{i,j,k} < z\}$$

(122)
In other words, it is the $z$-th lowest degree of distinct irreducible factors of $f^*$. We define polynomials $f_{\partial x}$ as follows:

$$f_{\partial x} := \prod_{g \in \bigcup_{i=0}^{d_{\partial x}} \mathcal{P}_x(i) \cup \mathcal{P}_y(i)} g^{y_0(f)}$$

i.e. it is the product of irreducible factors of $f \in F_{(n,N),(w,w')}(\mathbb{F}_q)$ (including multiplicities) up to $z$-th lowest degree exceeding $n$ that do not lie in $\mathcal{P}_0$. We now define the following abbreviation of local characters for each $1 \leq z \leq w'$:

$$\chi_{f,0} := (\chi_{f,v})_{v \in \Sigma_f}, \quad \chi_{f,z} := (\chi_{f,v})_{v \in \Sigma_f \cup (\mathcal{F}_z)}$$

In other words, $\chi_{f,z}$ is the Cartesian product of restriction of the global character $\chi_f$ over places in $\Sigma_f$ and places of degree at most the $z$-th lowest degree of distinct irreducible factors of $f^*$. Using these notations, we have

$$\text{Sel}_\pi(E^{\chi_f}) = \text{Sel}(E[p], \chi_{f,w'}).$$

Let $\lambda \in \Lambda_{N,w}$ and $\eta \in \Lambda_{n,N,w-w'}$. There is a projection map which forgets all irreducible factors of degree greater than $n$:

$$\Phi : F_{(n,N),(w,w')}(\mathbb{F}_q) = \prod_{i,j,k} \text{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i)) \times \prod_{i,j,k} \text{Conf}_{\eta_{i,j,k}}(\mathcal{P}_k(i)) \rightarrow \prod_{i,j,k} \text{Conf}_{\eta_{i,j,k}}(\mathcal{P}_k(i))$$

[[Statistics over fibers of $\Phi$]]

Suppose that $h_* \in F_{n-N}(\mathbb{F}_q)$ such that $h_*$ admits the forgetful partition $\eta$. Given such a choice of $h_*$, we will pay particular focus to the set of fibers $\Phi^{-1}(h_*)$. We then have:

$$\#\{f \in \Phi^{-1}(h_*) \mid \dim_{\mathbb{F}_p} \text{Sel}_\pi(E^{\chi_f}) = J\} \quad = \quad \#\{f \in \Phi^{-1}(h_*) \mid \text{rk}(\chi_{f,w'}) = J\}$$

$$= \sum_{J_0=0}^{\infty} \# \left\{ f \in \Phi^{-1}(h_*) \mid \text{rk}(\chi_{f,0}) = J_0, \sum_{z=1}^{w'} \text{rk}(\chi_{f,z}) - \text{rk}(\chi_{f,z-1}) = J \right\}$$

Denote by $\Omega_{\mathcal{F}_N}$ the following set of Cartesian product of local characters

$$\Omega_{\mathcal{F}_N} := \prod_{v \in \Sigma_F} \text{Hom}(\text{Gal}(K_v/K_v), \mu_p) \times \prod_{v|h_*} \text{Hom}(\text{Gal}(K_v/K_v), \mu_p) \subset \Omega_1$$

Let $\delta_{h_*} : \mathbb{Z}_{\geq 0} \rightarrow [0, 1]$ be the probability distribution defined as

$$\delta(J) := \frac{\#\{\omega \in \Omega_{\mathcal{F}_N} \mid \text{rk}(\omega) = J\}}{\#\Omega_{\mathcal{F}_N}}$$

Let $d_{\lambda}$ be an integer associated to a choice of a splitting partition $\lambda$ defined as

$$d_{\lambda} := \sum_{i,j} (\lambda_{i,j,1} + 2 \cdot \lambda_{i,j,2}).$$

Note that there exists a bijection

$$\Phi^{-1}(h) \cong \prod_{i,j,k} \text{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i))$$

Inductively applying Proposition $5.13$ to each term $\text{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i))$, we obtain that

$$\left| \frac{\#\{f \in \Phi^{-1}(h_*) \mid \dim_{\mathbb{F}_p} \text{Sel}_\pi(E^{\chi_f}) = J\} - (M_{\lambda} \delta_{h_*})(J)}{\#\Phi^{-1}(h_*)} \right| < B_{E,p,q} \cdot d_{\lambda} \cdot (n \log q)^{-2m_{n,q}+6 \log p+1} < B_{E,p,q} \cdot (n \log q)^{-2m_{n,q}+6 \log p+2}.$$
where $B_{E,p,q} > 0$ is the explicit constant constructed in Proposition 5.13.

[[Statistics over unions of fibers of $\Phi$]]

Denote by $F^{h_{*}}_{(n,N),(w,w')}(\mathbb{F}_q)$ the disjoint union of subsets

$$F^{h_{*}}_{(n,N),(w,w')}(\mathbb{F}_q) := \bigcup_{\Lambda \in \Lambda_{N,w}^f} \Phi^{-1}(h_{*})$$

(131)

Recall that we defined the Markov operator $M$ over $\mathbb{Z}_{\geq 0}$ as

$$M := \left(1 - \frac{p}{p^2 - 1}\right) \cdot J + \frac{1}{p} M_L + \frac{1}{p^3 - p} M^2_L.$$  

(132)

Summing variants of equation (130) over the set of locally arrangeable partitions $\Lambda_{N,w}^f$, we obtain

$$\left| \frac{\# \{ f \in F^{h_{*}}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \dim \mathcal{F}_p \text{ Sel}_E(E^{x_{e}}) = J \} - (M^{w'-1}\delta_{h_{*}}(J)) }{\# F^{h_{*}}_{(n,N),(w,w')}(\mathbb{F}_q)} \right| < B_{E,p,q} \cdot (n \log q)^{-2m_{n,q} + 6 \log p + 2}$$

(133)

$$< B_{E,p,q} \cdot (n \log q)^{-m_{n,q}}.$$  

Note that we iterate the Markov chain $M$ by $w' - 1$ times, rather than $w'$ times, because we are using one of the auxiliary places of $f$ to obtain an equidistribution of characters $\{\chi_{f,w'}\}$ inside $\Omega_{E}(\mathcal{F})$, hence allowing us to apply Proposition 5.13.

[[Incorporating ergodicity of Markov chains]]

Recall the Poonen-Rains distribution

$$PR(J) = \prod_{j \geq 0} \frac{1}{1 + p^{-j}} \prod_{j=1}^{J} \frac{p}{p^j - 1}.$$  

Because we set $w - w' = \epsilon w$ for small enough $0 < \epsilon < 1$, it follows that

$$\max_{J \in \mathbb{Z}_{\geq 0}} \{ J \mid \delta_{h_{*}}(J) \neq 0 \} \leq \max_{\chi \in \Omega_E} \text{rk}(\chi) + 2 \epsilon w.$$  

(134)

By Corollary 6.7, we obtain that there exists a fixed constant $c > 0$ such that

$$\sup_{J \in \mathbb{Z}_{\geq 0}} \left| (M^{w'-1}\delta_{h_{*}})(J) - PR(J) \right| < c \cdot \left(1 - \frac{p}{p^2 - 1} + \frac{1}{p\beta} + \frac{1}{(p^3 - p)\beta^2}\right)^{w'-1} \cdot \mathbb{E}[\beta^x \mid x \in \delta]$$

(135)

for any positive $\beta > 1$. Because $w \leq 2m_{n,q}$, it follows that

$$\mathbb{E}[\beta^x \mid x \in \delta] \leq \beta^{\text{rank}_{\chi \in \Omega_E} \text{rk}(\chi)} \cdot (n \log q)^{4 \epsilon \log \beta}$$

(136)

By letting $c_\beta := c \cdot \beta^{\text{rank}_{\chi \in \Omega_E} \text{rk}(\chi)}$, we obtain:

$$< c_\beta \cdot \left(1 - \frac{p}{p^2 - 1} + \frac{1}{p\beta} + \frac{1}{(p^3 - p)\beta^2}\right)^{w'-1} \cdot (n \log q)^{4 \epsilon \log \beta}$$

(137)

Using triangle inequality with equation (130), we obtain for all $J \geq 0$ and for any small enough $0 < \epsilon < 1$, there exists an explicit constant $\tilde{B}_{E,p,q,\beta} := B_{E,p,q} + c_\beta$ such that

$$\left| \frac{\# \{ f \in F^{h_{*}}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \dim \mathcal{F}_p \text{ Sel}_E(E^{x_{e}}) = J \} - PR(J)}{\# F^{h_{*}}_{(n,N),(w,w')}(\mathbb{F}_q)} \right| < \tilde{B}_{E,p,q,\beta} \cdot (n \log q)^{4 \epsilon \log \beta} \cdot (n \log q)^{-m_{n,q} + \left(1 - \frac{p}{p^2 - 1} + \frac{1}{p\beta} + \frac{1}{(p^3 - p)\beta^2}\right)^{w'-1}}$$

(138)
Denote by $F_{(n,N),(w,w')}^\eta(\mathbb{F}_q)$ the following disjoint union of subsets

$$F_{(n,N),(w,w')}^\eta(\mathbb{F}_q) := \bigcup_{h \in F_{n-N}(\mathbb{F}_q)} F_{(n,N),(w,w')}^{h \ast}(\mathbb{F}_q)$$

(139)

By ranging over all $h \ast \in F_{n-N}(\mathbb{F}_q)$ such that $h \ast$ admits the forgettable splitting partition $\eta$, we obtain that

$$\left| \# \{ f \in F_{(n,N),(w,w')}^\eta(\mathbb{F}_q) \mid \dim_{\mathbb{F}_q} \text{Sel}_p(E^{\chi}) = J \} \right| - PR(J)$$

(140)

$$< \tilde{B}_{E,p,q,\beta} \cdot (n \log q)^{4 \epsilon \log \beta} \cdot \left( (n \log q)^{-\rho \log \rho - 1 + \rho} \cdot 3 \cdot m_{n,q}^2 \cdot \left( \frac{p}{p^2 - 1} \right) \left( 1 - \frac{p}{p^2 - 1} \right)^{-1} \right)$$

(141)

Recall that $\tilde{F}_{(n,N),(w,w')}^\eta(\mathbb{F}_q)$ is the following disjoint union of sets:

$$\tilde{F}_{(n,N),(w,w')}^\eta(\mathbb{F}_q) := \bigcup_{\lambda \in \Lambda_{n,N}^q} \bigcup_{\eta \in \Lambda_{n-N,w-w'}^\text{for}} F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) = \bigcup_{\eta \in \Lambda_{n-N,w-w'}^\text{for}} F_{(n,N),(w,w')}^\eta(\mathbb{F}_q)$$

By ranging over all possible forgettable splitting partitions $\eta \in \Lambda_{n-N,w-w'}^\text{for}$, we obtain the desired proposition.

We now prove the main theorem of this manuscript.

Proof of Theorem 1.2 Suppose that $m_{n,q} > \max \{ e^\epsilon, \log 6 + \log(p^3 + g_{E[p]}), \deg E, 6 \log p + 2 \}$. Let $\rho \in (0, 1)$ be any fixed number. From Proposition 4.14, we obtain that

$$\# F_n(\mathbb{F}_q) - \sum_{w = \rho m_{n,q}}^{2 m_{n,q}} \sum_{w' = (1-\epsilon)w}^{n} \# \tilde{F}_{(n,N),(w,w')}^\eta(\mathbb{F}_q)$$

$$\leq 4 \cdot q^n \cdot \max \left( (n \log q)^{-\rho \log \rho - 1 + \rho}, 3 \cdot m_{n,q}^2 \cdot \left( \frac{p}{p^2 - 1} \right) \left( 1 - \frac{p}{p^2 - 1} \right)^{-1} \right)$$

(142)

$$\leq 4 \cdot q^n \cdot \max \left( (n \log q)^{-\rho \log \rho - 1 + \rho}, 3 \cdot m_{n,q}^2 \cdot (n \log q)^{-1 + \rho} \cdot \left( \frac{p}{p^2 - 1} \right) \left( 1 - \frac{p}{p^2 - 1} \right)^{-1} \right)$$

where $\epsilon = \frac{1}{\log \log m_{n,q}}$. Letting $w$ to satisfy $\rho m_{n,q} \leq w < 2 m_{n,q}$, and $(1 - \epsilon)w \leq w' \leq w$, we obtain from Proposition 4.14 that

$$\left| \# \{ f \in \tilde{F}_{(n,N),(w,w')}^\eta(\mathbb{F}_q) \mid \dim_{\mathbb{F}_q} \text{Sel}_p(E^{\chi}) = J \} \right| - PR(J)$$

$$< \tilde{B}_{E,p,q,\beta} \cdot (n \log q)^{4 \epsilon \log \beta} \cdot \left( (n \log q)^{-m_{n,q} + 3 \cdot (n \log q)^{1 - \rho \log \rho - 1 + \rho}}, 3 \cdot m_{n,q}^2 \cdot (n \log q)^{-1 + \rho} \cdot \left( \frac{p}{p^2 - 1} \right) \left( 1 - \frac{p}{p^2 - 1} \right)^{-1} \right)$$

(143)

$$< 6 \cdot \tilde{B}_{E,p,q,\beta} \cdot (n \log q)^{(1 - \rho \log \rho - 1 + \rho) \cdot \left( \frac{p}{p^2 - 1} \right) \left( 1 - \frac{p}{p^2 - 1} \right)^{-1} + 4 \epsilon \log \beta}$$

Combine two equations to obtain

$$\left| \# \{ f \in F_n(\mathbb{F}_q) \mid \dim_{\mathbb{F}_q} \text{Sel}_p(E^{\chi}) = J \} \right| - PR(J) < \frac{12 \cdot m_{n,q}^2 \cdot \tilde{B}_{E,p,q,\beta}}{(n \log q)^{\alpha(\rho,p,\beta,\epsilon)}}$$

(144)
where
\[
\alpha(p, \rho, \beta, \epsilon) := \min \left\{ \frac{\rho \log \rho + 1 - \rho}{\delta}, \frac{-\rho \log \left(\frac{p^\rho}{p^{\rho-1}}\right)}{1 - \rho \log \left(1 - \frac{p^\rho}{p^{\rho-1}} + \frac{1}{p^\beta} + \frac{1}{(p^\beta)^{\beta\epsilon}}\right) + 4\epsilon \log \beta} \right\}
\]

We now choose \( \beta = \frac{1}{\epsilon} = \log \log m_{n,q} > e \). Then we have
\[
\tilde{B}_{E,p,q,\beta} := B_{E,p,q} + c_\beta \leq (B_{E,p,q} + c) \cdot (\log \log m_{n,q})^{\max_{\chi \in \mathcal{A}_E} \text{rk}(\chi)},
\]
\[
\alpha(p, \rho, \beta, \eta) = \min \left\{ \frac{\rho \log \rho + 1 - \rho}{\delta}, \frac{-\rho \log \left(\frac{p^\rho}{p^{\rho-1}}\right)}{1 - \rho \log \left(1 - \frac{p^\rho}{p^{\rho-1}} + \frac{1}{p^\beta} + \frac{1}{(p^\beta)^{\beta\epsilon}}\right) + 4\epsilon \log \beta} \right\}
\]

Then for any small enough \( \delta > 0 \) (for example, pick \( \delta < \frac{\alpha(p, \rho)}{2} \)), there exists sufficiently large \( n \) and an explicit constant \( \tilde{A}_{E,p,q} := 12 \cdot (B_{E,p,q} + c) \) such that
\[
\left| \frac{\#\{ f \in F_n(\mathbb{F}_q) \mid \dim_{\mathbb{F}_p} \text{Sel}_\pi(E^{x_f}) = J \}}{\# F_n(\mathbb{F}_q)} - PR(J) \right| < \frac{\tilde{A}_{E,p,q}}{(n \log q)^{\alpha(p, \rho) - \delta}},
\]
(145)
where \( \alpha(p, \rho) \) is a function obtained from \( \alpha(p, \rho, \beta, \epsilon) \) by letting \( m_{n,q} \) to grow arbitrarily large:
\[
\alpha(p, \rho) := \min \left\{ \frac{\rho \log \rho + 1 - \rho}{\delta}, \frac{-\rho \log \left(\frac{p^\rho}{p^{\rho-1}}\right)}{1 - \rho \log \left(1 - \frac{p^\rho}{p^{\rho-1}} + \frac{1}{p^\beta} + \frac{1}{(p^\beta)^{\beta\epsilon}}\right) + 4\epsilon \log \beta} \right\}.
\]

We then define \( \alpha(p) := \sup_{0 < p < 1} \alpha(p, \rho) \) and set \( A_{E,p,q} := \frac{\tilde{A}_{E,p,q}}{(\log q)^{\alpha(p, \rho)}} \) to obtain the statement of the main theorem.

\[ \square \]

Acknowledgements

My apologies in advance that the acknowledgement section may be longer than what one may read from other manuscripts.

This research was conducted during my compulsory military service as a research personnel in National Institute for Mathematical Sciences (NIMS) and during my graduate studies at the University of Wisconsin-Madison after returning from leave of absence. The progress I made on this project during my military service (which comprises most of the ideas covered in this manuscript) was primarily done at the end of the day after my usual working hours as a research personnel.

I would like to express my sincerest and most immense gratefulness to my PhD advisor Jordan Ellenberg for suggesting various helpful references, giving crucial and enlightening insights, and investing valuable time and effort for having regular Skype meetings during my leave of absence. I would also like to thank him for suggesting to understand the role of generalized Riemann hypothesis in computing the desired probability distributions. Without his continuous and immensely enthusiastic and patient support, this work would not have led to its fruition.

I would like to thank Zev Klagsbrun, Aaron Landesman, Jungin Lee, Wanlin Li, Mark Shusterman, Alex Smith, and Niudun Wang for carefully explaining their works on probability distributions of families of elliptic curves, suggesting valuable references which are relevant to this paper [KMR14, FLR23, Wan21, CLDL12, Smi22a], and for engaging in very helpful discussions. I would like to thank Jungin Lee and Zev Klagsbrun for comments on improving the exposition of this paper. I would like to thank U Jin Choi and Yongsul Won for helpful discussions on Markov chains, and many other researchers at NIMS for shaping enjoyable experiences during my service. I would like to thank Douglas Ulmer for enlightening discussions, from which an error from from the previous...
version of this manuscript was discovered. I would like to thank Max Planck Institute for Mathematics for providing a wonderful environment to delve into research and actively interact with other mathematicians, especially from which the discussions with Douglas Ulmer were made possible.

I would like to sincerely thank anonymous reviewer for giving extensive comments, pointed out several mathematical errors in the previous version of this draft, and suggested a number of ways to further improve the exposition of this paper. The current state of this manuscript would not have been achievable without ample support from the referee.

Lastly, I would like to sincerely thank my parents for their wholehearted continuous support throughout my military service and in the midst of the COVID-19 global pandemic. Without their unconditional love and continuous support, the experiences I had with preparing this manuscript would not have been as enjoyable.

References

[AP58] A. Rényi and P. Turán. On a theorem of Erdős-Kac. Acta Arithmetica, 4(1):71–84, 1958.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BK77] Armand Brumer and Kenneth Kramer. The rank of elliptic curves. Duke Mathematical Journal, 44(4):715–743, 1977.

[BKJ+15] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra Jr., Bjorn Poonen, and Eric Rains. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. Cambridge Journal of Mathematics, 3(3):275–321, 2015.

[BLV09] Andrea Bandini, Ignazio Longhi, and Stefano Vigni. Torsion points on elliptic curves over function fields and a theorem of Igusa. Expositiones Mathematicae, 27(3):175–209, 2009.

[BS15] Manjul Bhargava and Arul Shankar. Binary quadratic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. Annals of Mathematics, 181:191–242, 2015.

[BSGKS20] Lior Bary-Soroker, Ofer Gorodetsky, Taelin Karidi, and Will Sawin. Chebotarev density theorem in short intervals for extensions of \( \mathbb{F}_q(t) \). Transactions of the American Mathematical Society, 373:597–628, 2020.

[CCN05] Brian Conrad, Keith Conrad, and Harald Helfgott. Root numbers and ranks in positive characteristic. Advances in Mathematics, 198(2):684–731, 2005.

[CLDLL22] Antoine Comeau-Lapointe, Chantal David, Matilde Lalin, and Wanlin Li. On the vanishing of twisted L-functions of elliptic curves over rational function fields. Research in Number Theory, 8(76), 2022.

[CLNY22] Gilyoung Cheong, Jungin Lee, Hanbyul Nam, and Myungjun Yu. Jordan–Landau theorem for matrices over finite fields. Linear Algebra and its Applications, 655:100–128, 2022.

[Coh69] Stephen D. Cohen. Further arithmetical functions in finite fields. Proceedings of the Edinburgh Mathematical Society, 16:349–363, 1969.

[Del80] Pierre Deligne. La conjecture de Weil, II. Publications Mathématiques de l’IHÉS, 52:137–252, 1980.

[DFK07] Chantal David, Jack Fearnley, and Hershy Kisilevsky. Vanishing of L-functions of elliptic curves over number fields, ranks of elliptic curves and random matrix theory. London Math. Soc. Lecture Note Series, 341:247–259, 2007.

[dJ02] A.J. de Jong. Counting elliptic surfaces over finite fields. Moscow Mathematical Journal, 2(2):281–311, 2002.

[dJF11] A.J. de Jong and Robert Friedman. On the geometry of principal homogeneous spaces. American Journal of Mathematics, 133(3):753–796, 2011.

[DW85] G. Dueck and H.C. Williams. Computation of the Class Number and Class Group of a Complex Cubic Field. Mathematics of Computation, 45(171):223–231, 1985.

[EH91] Gove Effinger and David Hayes. Additive number theory of polynomials over a finite fields. Oxford Mathematical Monographs, pages 75–88, 1991.

[EK40] Paul Erdős and Mark Kac. The Gaussian laws of errors in the theory of additive number theoretic functions. American Journal of Mathematics, 62(1/4):738–742, 1940.

[EVW16] Jordan Ellenberg, Akshay Venkatesh, and Craig Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. Annals of Mathematics, 183:729–786, 2016.

[FJ08] Michael D. Fried and Moshe Jarden. Field Arithmetic. Springer, Berlin, Germany, 2008.
PROB. DIST. $\pi$-SELMER RANKS OF CYC. ORD. $p$-TWISTS OF $E/\mathbb{F}_q(t)$

[FJ24] Daniel Fiorilli and Florent Jouve. Distribution of Frobenius elements in families of Galois extensions. *Journal of the Institute of Mathematics of Jussieu*, 23(3):1169–1258, 2024.

[FLR23] Tony Feng, Aaron Landesman, and Eric Rains. The geometric distribution of Selmer groups of elliptic curves over function fields. *Mathematische Annalen*, 387:615–687, 2023.

[FWY20] Tingting Feng, Shaochen Wang, and Guangyu Yang. Large and moderate deviation principles for the Erdös-Kac theorem in function fields. *Statistics and probability letters*, 163, 2020.

[Hal06] Chris Hall. Big symplectic or orthogonal monodromy modulo $l$. *Duke mathematics journal*, 141(1):179–203, 2006.

[HB94] D.R. Heath-Brown. The size of Selmer groups for the congruent number problem, II. *Inventiones mathematicae*, 118:331–370, 1994.

[How01] Everett W. Howe. Isogeny classes of abelian varieties with no principal polarizations. *Moduli of Abelian Varieties (Texel Island, 1999)*, Birkhauser Progress in Mathematics, pages 203–216, 2001.

[Hsu98] Chih-Nung Hsu. On certain character sums over $\mathbb{F}_q[t]$. *Proceedings of the American Mathematical Society*, 126(3):647–652, 1998.

[Igu59] J. I. Igusa. Fibre systems of Jacobian varieties (II I. Fibre systems of elliptic curves). *American Journal of Mathematics*, 81:453–476, 1959.

[Imp03] Chris Impens. Stirling’s series made easy. *The American Mathematical Monthly*, 110(8):730–735, 2003.

[Kan13] Daniel Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Algebra and Number Theory*, 7(5):1253–1279, 2013.

[KMR13] Zev Klagsbrun, Barry Mazur, and Karl Rubin. Disparity in Selmer ranks of quadratic twists of elliptic curves. *Annals of Mathematics*, 178(1):287–320, 2013.

[KMR14] Zev Klagsbrun, Barry Mazur, and Karl Rubin. A markov model for Selmer ranks in families of twists. *Annals of Mathematics*, 178(1):287–320, 2013.

[KO15] Zev Klagsbrun and Robert J. Lemke Oliver. The distribution of 2-Selmer ranks of quadratic twists of elliptic curves with partial two-torsion. *Mathematika*, 62(1):67–78, 2015.

[KP21] Peter Koymans and Carlo Pagano. On the distribution of $\text{Cl}(K)[l]\infty$ for degree $l$ cyclic fields. *Journal of the European Mathematical Society*, 24(4):1189–1283, 2021.

[KP22] Peter Koymans and Carlo Pagano. On Stevenhagen’s conjecture. Preprint available at https://arxiv.org/pdf/2201.13424.pdf, 2022.

[Lan21] Aaron Landesman. The geometric average size of Selmer groups over function fields. *Algebra and Number Theory*, 15(3):673–709, 2021.

[Li19] Chao Li. 2-Selmer groups, 2-class groups and rational points on elliptic curves. *Transactions of the American Mathematical Society*, 371:4631–4653, 2019.

[Liu04] Yu-Ru Liu. A generalization of the Erdös-Kac theorem and its applications. *Canadian Mathematical Bulletin*, 47(4):589–606, 2004.

[LO75] J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. *Proceedings of Symposia in Pure Mathematics*, pages 409–464, 1975.

[Mil06] J.S. Milne. *Arithmetic Duality Theorems*. BookSurge, LLC, second edition, 2006.

[Mon96] P. Monsky. Generalizing the Birch-Stephens theorem. I. Modular curves. *Mathematische Zeitschrift*, 221(3):415–420, 1996.

[MP22] Adam Morgan and Ross Paterson. On 2-Selmer groups of twists after quadratic extension. *Journal of the London Mathematical Society*, 105(2):1110–1166, 2022.

[MR07] Barry Mazur and Karl Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Annals of Mathematics*, 166:579–612, 2007.

[MR23] Barry Mazur and Karl Rubin. Arithmetic conjectures suggested by the statistical behavior of modular symbols. *Experimental Mathematics*, 32(4):657–672, 2023.

[MRS07] Barry Mazur, Karl Rubin, and Alice Silverberg. Twisting commutative algebraic groups. *Journal of Algebra*, 314(1):419–438, 2007.

[MT93] Sean Meyn and Richard Tweedie. *Markov chains and stochastic stability*. Springer-Verlag, Berlin, Germany, 1993.

[MZ16] Behzad Mehrdad and Lingjoing Zhu. Moderate and large deviations for Erdös-Kac theorem. *Quarterly Journal of Mathematics*, 67(1):147–160, 2016.

[Pit74] J.W. Pitman. Uniform rates of convergence for Markov chain transition probabilities. *Zeitschrift fur Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 29:193–227, 1974.

[Poo13] Bjorn Poonen. Average rank of elliptic curves, after Manjul Bhargava and Arul Shankar. *Séminaire Bourbaki volume 2011/2012*, 352(1049):1043–1058, 2013.
Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *Journal of the American Mathematical Society*, 25(1):245–269, 2012.

[PTBW20] Lilian B. Pierce, Caroline L. Turnage-Butterbaugh, and Melanie Matchett Wood. An effective Chebotarev density theorem for families of number fields, with an application to $l$-torsion in class groups. *Inventiones mathematicae*, 219:701–778, 2020.

Sun Woo Park and Niudun Wang. On the average of $p$-Selmer rank in quadratic twist families of elliptic curves over function field. *International Mathematics Research Notices*, 2024:4516–4540, 2024.

B.C. Ngo Q.P. Ho, V.B. Le Hung. Average size of $2$-Selmer groups of elliptic curves over function fields. *Mathematical research letters*, 21(6):1305–1339, 2014.

Ottavio G. Rizzo. Average root numbers for a nonconstant family of elliptic curves. *Compositio Mathematica*, 136(1):1–23, 2003.

Michael Rosen. *Number theory in function fields*. Springer, Berlin, Germany, 2002.

Peter Swinnerton-Dyer. The effect of twisting on the $2$-Selmer group. *Mathematical Proceedings of the Cambridge Philosophical Society*, 145(3):513–526, 2008.

J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publications Mathématiques de l'IHÉS*, 54:123–201, 1981.

Alexander Smith. $2^\infty$-Selmer groups, $2^\infty$-class groups, and Goldfeld’s conjecture. *Preprint available at https://arxiv.org/abs/1702.02295*, 2017.

Alexander Smith. $l^\infty$-Selmer groups in degree $l$ twist families. *Doctoral dissertation, Harvard University*, 2020.

Alexander Smith. The distribution of $l^\infty$ Selmer groups in degree $l$ twist families I. *Preprint available at https://arxiv.org/abs/2207.05674*, 2022.

Alexander Smith. The distribution of $l^\infty$ Selmer groups in degree $l$ twist families II. *Preprint available at https://arxiv.org/pdf/2207.05143.pdf*, 2022.

Daniel Barrera Salazar, Ariel Pacetti, and Gonzal Tornaria. On $2$-Selmer groups and quadratic twists of elliptic curves. *Mathematical Research Letters*, 28(6):1633–1659, 2021.

William Stein. Shafarevich-Tate groups of nonsquare order. *Modular Curves and Abelian Varieties 2002 Barcelona Conference Proceedings, Birkhauser Progress in Mathematics*, 224:277–289, 2002.

Fabien Trihan and Seidai Yasuda. The $l$-parity conjecture for abelian varieties over function fields of characteristic $p > 0$. *Compositio Mathematica*, 150(4):507–522, 2014.

Niudun Wang. $2$-Selmer groups of quadratic twists of elliptic curves. *Ph.D. Thesis available at https://depot.library.wisc.edu/repository/fedora/1711.dl:ITQ5IQCZ72U6I8H/datastreams/REF/content*, 2021.

Email address: spark483@wisc.edu, s.park@mpim-bonn.mpg.de

480 Lincoln Drive, Madison, WI, USA 53706, Vivatsgasse 7, 53111 Bonn, Germany