Arithmetic statistics of Selmer groups of twist families of elliptic curves over global fields

A proposal for an interplay between arithmetic, geometry, and probability theory

by

Sun Woo Park

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Mathematics

at the
University of Wisconsin-Madison
2024

Date of Final Oral Exam: **2024/05/06**
The dissertation is approved by the following members of the Final Oral Committee:
Jordan Ellenberg, Professor, Mathematics
Brian Lawrence, Assistant Professor, Mathematics
Hanbaek Lyu, Assistant Professor, Mathematics
Tonghai Yang, Professor, Mathematics

Arithmetic statistics of Selmer groups of twist families of elliptic curves over global fields

A proposal for an interplay between arithmetic, geometry, and probability theory

Sun Woo Park

Abstract

Let ℓ be an odd prime number at least 5, and let $K = \mathbb{F}_q(t)$ be the global function field of characteristic coprime to 2 and 3 which contains the primitive ℓ-th roots of unity. This thesis focuses on investigating the statistics of rank growths of a non-isotrivial elliptic curve E over K with respect to a randomly chosen cyclic order-ℓ extension L/K, obtained from adjoining the ℓ-th root of an ℓ-th power free polynomial over $\mathbb{F}_q$ of degree n.

To address the problem outlined above, this thesis presents a probabilistic and a geometric approach to understand such rank growths by utilizing prime Selmer groups of some families of abelian varieties over K. The abelian varieties of our interest, as suggested from the works of Mazur and Rubin, are $\ell - 1$ dimensional abelian varieties obtained from the kernel of the norm map from the Weil restriction of E obtained from the cyclic extension L/K to E. The upper bound on rank growths of E can be understood from computing the dimensions of $1 - \sigma_{L,K}$ Selmer groups of such $\ell - 1$ dimensional abelian varieties, where $\sigma_{L,K}$ is a cyclic generator of the Galois group $\mathrm{Gal}(L/K)$.

The probabilistic approach generalizes the work by Klagsbrun, Mazur, and Rubin, who propose a Markov model over a countable state space which governs the variations of Selmer groups of non-canonically ordered $(l-1)$ dimensional abelian varieties over number fields, assuming some mild conditions on the elliptic curve E. Over global function fields, we can further utilize the applications of the Riemann hypothesis - which are the effective versions of the Chebotarev density theorem and Erdös-Kac theorem - to reorder these abelian varieties under a canonical order and obtain explicit rate of convergence to the probability distribution proposed by Bhargava, Kane, Lenstra, Poonen, and Rains. The error terms, unlike the geometric approach, depends only on the degree n of the polynomial that defines the cyclic order-ℓ extension over K, and is independent of the size of q.

The geometric approach revolves around constructing a space whose $\mathbb{F}_q$-rational points parametrize the prime Selmer groups of aforementioned families of $\ell - 1$ dimensional abelian varieties. This space is obtained from using the middle convolution functor to construct a representable étale $\mathbb{F}_\ell$-lisse sheaf $\tau_{n,\sigma_\ell,E}$ over the colored configuration space of n points with $\ell - 1$ colors defined over $\overline{\mathbb{F}}_q$, a generalization of previous work of Katz and Hall. By using the Grothendieck-Lefschetz trace formula and big monodromy results, we demonstrate that assuming some mild conditions on the elliptic curve E, the probability distribution of such Selmer groups conform to the heuristics suggested by Bhargava, Kane, Lenstra, Poonen, and Rains, up to error terms which depend on both n and q.

As an application, we demonstrate how these two approaches can lead us to obtain new properties of étale cohomology groups of the geometric space parametrizing the Selmer groups of families of abelian varieties of our interest. To elaborate, we show that the homological stability, subexponential Betti numbers, and explicitly determined absolute

values of eigenvalues of the Frobenii actions of these étale cohomology groups imply that the trace of the Frobenii acting on higher étale cohomology groups have to vanish to 0. This result hints a possibility that the étale cohomology groups themselves are trivial, a conjectural statement which requires further research.

We also propose new families of abelian varieties over global fields where both geometric and probabilistic approaches can be possibly utilized to analyze the probability distribution of their Selmer groups. These abelian varieties are obtained from Weil restriction of elliptic curves E with respect to non-abelian Galois extensions L/K with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ for any $m \mid (\ell - 1)$, whose dimensions of Selmer groups give an upper bound on rank growths of E with respect to the extension L/K.

Acknowledgements

The three works presented in this thesis encompasses some of the research I focused on during my leave of absence due to compulsory military service in Korea (during which all the work presented here was done during evenings after usual working hours), and the last two years of my graduate studies Park 2022; Park 2024a; Park 2024b.

I would like to sincerely thank my PhD advisor, professor Jordan Ellenberg, for all the guidance and enlightenment - both mathematically and personally - followed with immense patience he has kindly shown throughout my graduate studies. In fact, no simple words can possibly express my sincerest gratefulness to Jordan. Jordan, thank you so much for kindly suggesting all the great mathematical insights and giving constructive and heartfelt encouragements in times when I was struggling mathematically. I would not have enjoyed the beauty of mathematics without your unwavering and heartwarming support.

I would like to thank professor Brian Lawrence, professor Hanbaek Lyu, and professor Tonghai Yang for becoming committee members for my PhD thesis defense and giving constructive feedback and comments for improving the thesis. I would like to thank professor Nigel Boston and professor Daniel Erman, who were previously at University of Wisconsin-Madison, for becoming committee members for my specialty exam, and for giving encouragements and mathematical suggestions.

I would like to thank Dr. Melissa Lindsey, Dr. Travis Olson, Dr. Kaitlyn Phillipson, and Dr. Cassie Williams for giving constructive feedback and encouragements to enhance my teaching experiences during my graduate studies. I would like to thank both the University of Wisconsin-Madison and the National Institute for Mathematical Sciences for providing wonderful environments and opportunities to conduct various interesting research in mathematics.

I would like to sincerely thank all the mathematical interactions I have had which have been incredibly crucial for developing the ideas presented in this thesis and other mathematical works conducted during my graduate studies, which were not included due to the scope of the paper. I would like to thank Levent Alpöge, Santiago Arango-Pinẽros, U Jin Choi, Changho Han, Dosang Joe, Daniel Keliher, Zev Klagsbrun, Peter Koymans, Aaron Landesman, Jungin Lee, Robert Lemke-Oliver, Wanlin Li, Melanie Matchett-Wood, Oana Padurariu, Ross Paterson, Alex Smith, Ari Shnidman, Jiuya Wang, Youngho Woo, John Voight, David Zureick-Brown, and many others for sharing profound mathematical insights and helpful feedback, followed along with incredible amount of patience and encouragements.

I would like to thank all my friends, both during my graduate studies (Ivan Aidun, Michel Alexis, Tejasi Bhatnagar, Asvin G, Kaiyi Huang, Qiao He, Logan Heath, Alex Hof, Jiwoong Jang, Ruofan Jiang, Hyun Jong Kim, Jiho Kim, Yu Luo, Haran Mouli, Gautam

Memana Neelakantan, Patrick Nicodemus, Eiki Norizuki, Soumya Sankar, John Spoerl, Karan Srivastava, Jin Woo Sung, Taylor Tan, Niudun Wang, Yifan Wei, Liding Yao, John Yin, Yeonggyu Yun, and many others that I may not have stated here) and during my military service (Junhong Cho, Yun Young Choi, Woo Hyuk Huh, Mee-Yeon Joo, Junhwa Jung, Byeongchun Kim, Namyoung Kim, Hyunju Lee, Yongsul Won, and many others). My apologies that I may not have listed all the names here, but I thank everyone for making such an enjoyable experience both at my graduate school and my military service.

I would like to sincerely thank my parents, Ki Won Park and Sung Bong Cho, for their wholehearted continuous support throughout my graduate studies, military service, and in the midst of the Covid19 pandemic. Their unconditional love and support made the journey of pursuing research in arithmetic geometry more enjoyable. Especially, during occasional times when I was not confident and in serious doubt with my mathematical capabilities of contributing to mathematical research, their kind words and encouragements helped me regain my focus and overcome some emotional hardships I faced at the time.

And above all, thank you my Lord and Savior.

Contents

Chapter 1

Introduction

1.1 Motivation

The overarching theme this manuscript focuses on revolves around the following question:

Question 1.1.1. Understand the interplay between the following two approaches of obtaining asymptotic statistical behaviors of some countable families of mathematical objects $\mathcal{M} := \{A_n\}_{n\in\mathcal{A}}$, whose arithmetic properties depend on distinct prime factors of their indices $n \in \mathcal{A}$.

- A geometric approach utilizing topological invariants of geometric spaces parametrizing the desired family $\mathcal{M}$.
- A probabilistic approach utilizing stochastic processes which govern the dynamics of the desired family $\mathcal{M}$.

To understand the coupling between geometric and probabilistic approaches, it is crucial to find potential candidates of mathematical objects whose statistical behaviors can be obtained from both approaches. One potential candidate we may consider is the problem of understanding the arithmetic properties of families of elliptic curves E over a global field K. There is a wealth of previous research which suggest that there is potential for observing this interplay of two techniques. To name a few, the theory of interpreting

families of elliptic curves as geometric spaces, for example the theory of moduli spaces of elliptic curves, is a classical area of research in arithmetic geometry that has garnered deep insights on uncovering their arithmetic properties N. M. Katz and Mazur 1985; N. Katz 1998. Recent progress in applying techniques from data science to families of elliptic curves indicate potential advantages in regarding families of elliptic curves as murmuration structures.

What are some families of elliptic curves whose ordering indices indicate their arithmetic properties? One family we can consider is the family of quadratic twists of a fixed elliptic curve E over a global field K. Assuming that the characteristic of K is coprime to 2 and 3, we may write the Weierstrass model for the quadratic twist of E twisted by a square-free element $f \in K$ as

$$E_f := fy^2 = x^3 + Ax + B$$

for some $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$. The Mordell-Weil theorem states that the set of K-rational points of an elliptic curve E, denoted as $E(K)$, is a finitely generated abelian group. There is a decomposition $E(K) \cong \mathbb{Z}^r \oplus T$ for some non-negative integer $r \geq 0$, known as the rank of E over K, and a finite group T, known as the K-rational torsion subgroup of E. One of the classical questions focuses on understanding arithmetic properties of these families of elliptic curves, in particular the distribution of their ranks as carefully researched from a number of remarkable previous studies.

The rest of the subsequent paragraphs of this introduction closely follows Chapter 1 of Park 2022. Let A be a principally polarized abelian variety over K. Without loss of generality, we will assume that A/K is non-isotrivial. Let $m \in \mathrm{End}(A/K)$ be an isogeny of the abelian variety whose degree is coprime to the characteristic of K. The short exact sequence of group schemes

$$0 \to A[m] \to A \to^m A \to 0$$

induces the following commutative diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/mA(K) & \longrightarrow & H^1_{\text{ét}}(K, A[m]) & \longrightarrow & H^1_{\text{ét}}(K, A)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v A(K_v)/mA(K_v) & \longrightarrow & \prod_v H^1_{\text{ét}}(K_v, A[m]) & \longrightarrow & \prod_v H^1_{\text{ét}}(K_v, A)[m] & \longrightarrow & 0, \end{array}$$

where v varies over all places of K. The m-Selmer group of the abelian variety A is given by

$$\text{Sel}_m(A) := \text{Ker}\left(H^1_{\text{ét}}(K, A[m]) \to \prod_v H^1_{\text{ét}}(K_v, A)[m]\right). \tag{1.1}$$

Given a universal family of elliptic curves over a global field K, Bhargava, Kane, Lenstra, Poonen, and Rains made a conjecture on the distribution of ℓ-selmer groups of principally polarized abelian varieties for some prime number ℓ.

Conjecture (Poonen and Rains 2012 Bhargava, D. M. Kane, et al. 2015)**.** *Let K be a fixed global field of characteristic coprime to 2 and 3. Let p be a prime number coprime to the characteristic of K. Then as A varies over all principally polarized abelian varieties over K, ordered by a choice of a height satisfying Northcott property,*

$$\mathbb{P}\left[\dim_{\mathbb{F}_\ell} \text{Sel}_\ell(A/K) = d\right] = \left(\prod_{j\geq 0}(1+\ell^{-j})^{-1}\right)\left(\prod_{j=1}^{d}\frac{\ell}{\ell^j - 1}\right).$$

In particular, the average size of $\text{Sel}_\ell A$ over all principally polarized abelian varieties A/K is $\ell + 1$.

For example, for universal families of elliptic curves E over K, the probability is computed over finitely many elliptic curves $y^2 = x^3 + Ax + B$, where $A, B \in K$ have bounded height B, and calculating the limit of the probability as B grows arbitrarily large.

1.2 Main results

Fix a prime number ℓ. Given a polynomial $f \in \mathbb{F}_q[t]$, we denote by A_f the $(\ell - 1)$ dimensional abelian variety over $K = \mathbb{F}_q(t)$ constructed as

$$A_f/K := \text{Ker}\left(\mathbb{N} : \text{Res}_K^{K(\sqrt[\ell]{f})} E \to E\right) \tag{1.2}$$

where $\mathbb{N}$ is the norm map with respect to the Galois extension $\mathrm{Gal}(K(\sqrt[\ell]{f})/K)$. We note that A_f is not principally polarized, as every polarization of A_f is divisible by ℓ^2, as shown in Howe 2001. Nevertheless, the main contributions of this thesis, concurrent to the ideas presented in Klagsbrun, Mazur, and Rubin 2013; Klagsbrun, Mazur, and Rubin 2014, state that one can still formulate and verify an analogous statement to Bhargava-Kane-Lenstra-Poonen-Rains heuristics for such families of abelian varieties. Moreover, in lieu of Question 1.1.1, the confirmation and formulation of these statements suggest a possible interplay between arithmetic (algebraic ranks of elliptic curves), geometry (cohomology groups of local systems over configuration spaces), and probability theory (Markov operators over countable state spaces).

- Chapter 2. 3: Confirmation of Bhargava-Kane-Lenstra-Poonen-Rains heuristics for families of abelian varieties $\{A_f\}_{f\in\mathbb{F}_q[t]}$ with explicit rate of convergence computed from probabilistic and geometric approaches.

  Theorem (Theorem 2.1.2, Theorem 3.1.2)**.** *Assume Condition 3.1.1. We let*

  $$\mathbb{P}_{n,\ell} := \frac{\#\{f \in \mathbb{F}_q[t] \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K) = r,\ \deg f = n\}}{\#\{f \in \mathbb{F}_q[t] \mid \deg f = n\}}$$

  Then there exist integers $M_1, M_2 > 0$ and a fixed constant $C(\ell, E) > 0$ independent of n and q such that for every $n > M_1$ and $q > M_2$,

  $$\left|\mathbb{P}_{n,\ell} - \prod_{i=0}^{\infty} \frac{1}{1+\ell^{-i}} \prod_{i=1}^{r} \frac{\ell}{\ell^i - 1}\right| < C(\ell, E) \cdot \min\left(\frac{1}{(n\log q)^{\alpha(\ell)}}, \frac{1}{\sqrt{q}}\right) \tag{1.3}$$

  where $\alpha(\ell) = max_{0<\rho<1}\left(min\left(\rho\ln\rho + 1 - \rho, -\rho\ln\left(1 - \frac{\ell}{\ell^2-1}\right), -\rho\ln\left(\frac{\ell}{\ell^2-1}\right)\right)\right)$.

- Chapter 3: Identification of geometric conditions which ensure cohomological triviality of a representable étale sheaf $\tau_{n,\sigma_{\ell,f},E}$ over the unordered configuration space parametrizing prime Selmer groups of families of abelian varieties $\{A_f\}_{f\in\mathbb{F}_q[t]}$.

  Theorem (Thoerem 3.3.1)**.** *Suppose that the conditions provided in Theorem 3.3.1 regarding homological stability, subexponential Betti numbers, and Frobenius eigenval-*

ues of cohomology groups of $\tau_{n,\sigma_{\ell,f},E}$ are satisfied. Then for any fixed $i > 0$, there exists a large number $M(i) > 0$ such that for every $n > M(i)$,

$$H^i_{\acute{e}t}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v) = 0. \tag{1.4}$$

- Chapter 4: The construction of abelian varieties $B_{L/K}$ governing rank growths of elliptic curves over families of $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ Galois extensions L/K with $m \mid (\ell - 1)$ and a fixed Galois subextension M/K with Galois group $\mathbb{Z}/m\mathbb{Z}$ (the family of which is denoted as $\mathcal{L}_M$), the generalization of Poonen-Rains heuristics under certain conditions, and their relation to the problem of an integer expressible as a sum of two rational cubes.

  Theorem (Proposition 4.2.4, Theorem 4.3.12, Theorem 4.4.1)**.** *Denote by $B_{L/K}$ the $m(\ell-1)$ dimensional abelian variety over K defined as $B_{L/K} := Ker\Big(Res^L_K E \to Res^M_K E\Big)$.*

  - *Choose an order ℓ element $\sigma_{L/K} \in Gal(L/K)$. Then there exists a $Gal(\overline{K}/K)$-equivariant isomorphism $B_{L/K}[1 - \sigma_{L/K}] \cong (Res^M_K E)[l]$.*
  - *Assume Condition 4.3.9. Denote by $m := [M/K]$. Denote by $\mathbb{P}_{\mathcal{L}_M(X)}(d)$ the following probability:*

$$\mathbb{P}_{\mathcal{L}_M(X)}(d) := \frac{\#\{L \in \mathcal{L}_M(X) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_{L/K}}(B_{L/K}/K) = d\}}{\#\mathcal{L}_M(X)}$$

  Then assuming Condition 4.3.9, we obtain

$$\lim_{X\to\infty} \mathbb{P}_{\mathcal{L}_M(X)}(d) = \sum_{\substack{k_0,k_1,\cdots,k_{n-1}\in\mathbb{Z}_{\geq 0} \\ k_1+2k_2+\cdots+(n-1)k_{n-1}=d \\ k_0+k_1+\cdots+k_{n-1}=m}} \binom{k}{k_0, k_1, \cdots, k_{n-1}} \prod_{i=0}^{n-1} \left(\prod_{j\geq 0} \frac{1}{1+\ell^{-j}} \prod_{j=1}^{i} \frac{\ell}{\ell^j - 1} \right)^{k_i}.$$

  - *Given an integer n, denote by $w_2(n)$ the number of distinct odd prime factors of n equivalent to 2 modulo 3. Fix an elliptic curve $E : y^2 = x^3 - 432$. Let $L = \mathbb{Q}(\zeta_3, \sqrt[3]{n})$, $M = \mathbb{Q}(\zeta_3)$, and $K = \mathbb{Q}$. Then $\dim_{\mathbb{F}_3} \mathrm{Sel}_{1-\sigma_{L/K}}(B_{L/K}/K) = 2w_2(n) + \Delta(n)$ for some integer $-1 \leq \Delta(n) \leq 3$.*

1.3 Previous studies

This section closely follows Section 1, 4 of Park 2022 and Section 2 of Park 2024a.

Recall that given a polynomial $f \in \mathbb{F}_q[t]$, we denoted by A_f the $(\ell-1)$ dimensional abelian variety over $K = \mathbb{F}_q(t)$ constructed from the Kernel of the Norm map from the Weil restriction of scalars $\mathrm{Res}_K^{K(\sqrt[\ell]{f})} E$ to E. We adhere to Mazur and Rubin's treatment of the cyclic prime twists of abelian varieties with respect to cyclic prime field extensions Mazur and Rubin 2007, Chapter 3.

1.3.1 Prime twists

This subsection closely follows Section 2 of Park 2024a.

Let ℓ be a prime. Suppose K includes all the primitive ℓ-th roots of unity μ_ℓ. Given an element $f \in \mathcal{O}_K$, we denote by $\mathrm{Res}_K^{K(\sqrt[\ell]{f})} E$ the Weil restriction of scalars of the elliptic curve E_K associated to the cyclic order-ℓ Galois extension $K(\sqrt[\ell]{f})/K$. As a group scheme over $K(\sqrt[\ell]{f})$, the Weil restriction of scalars of E can be written as a product of E with indices given by elements of the Galois group $\mathrm{Gal}(K(\sqrt[\ell]{f})/K)$:

$$\mathrm{Res}_K^{K(\sqrt[\ell]{f})} E \cong \prod_{\tau \in \mathrm{Gal}(K(\sqrt[\ell]{f})/K)} E \quad (\text{over } K(\sqrt[\ell]{f})). \tag{1.5}$$

The Galois group $\mathrm{Gal}(K(\sqrt[\ell]{f})/K)$ acts on the group scheme by cyclically permuting the summands indexed by the elements τ of the Galois group. This implies that the Weil restriction of scalars of E has a canonical norm map to the elliptic curve E defined over K:

$$\mathbb{N} : \mathrm{Res}_K^{K(\sqrt[\ell]{f})} E \to E \tag{1.6}$$

Using the norm map, we may decompose the semisimple group ring $\mathbb{Q}[\mathrm{Gal}(K(\sqrt[\ell]{f})/K)]$ as

$$\mathbb{Q}[\mathrm{Gal}(K(\sqrt[\ell]{f})/K)] \cong \mathbb{Q} \oplus \mathbb{Q}\left[\left(\mathrm{Gal}(K(\sqrt[\ell]{f})/K)\right)^{\times}\right] \tag{1.7}$$

Denote by $\mathcal{I}_{f,\ell}$ the set

$$\mathcal{I}_{f,\ell} = \mathbb{Q}\left[\left(\mathrm{Gal}(K(\sqrt[\ell]{f})/K)\right)^{\times}\right] \cap \mathbb{Z}[\mathrm{Gal}(K(\sqrt[\ell]{f})/K)] \tag{1.8}$$

so that $\mathcal{I}_{f,\ell}$ is an ideal of $\mathbb{Z}[\mathrm{Gal}(K(\sqrt[\ell]{f})/K)]$ as well as a $\mathrm{Gal}(\overline{K}/K)$-module.

Definition 1.3.1. Suppose K contains all the primitive ℓ-th roots of unity μ_ℓ. Let $f \in \mathcal{O}_K^{\times}/(\mathcal{O}_K^{\times})^{\ell}$ be an ℓ-th power free integral element over K. The cyclic ℓ-twist of an elliptic curve E associated to a cyclic extension $K(\sqrt[\ell]{f})/K$ is the following $\ell-1$ dimensional abelian variety over K:

$$\mathcal{I}_{f,\ell} \otimes E \cong \mathrm{Ker}\left(\mathbb{N} : \mathrm{Res}_K^{K(\sqrt[\ell]{f})} E \to E\right). \tag{1.9}$$

Throughout this manuscript, we may use the abbreviation A_f to denote the $\ell - 1$ dimensional abelian variety $\mathcal{I}_{f,\ell} \otimes E$ over K.

Example 1.3.2. Note that if $\ell = 2$, then the 1-dimensional abelian variety $\mathcal{I}_{f,2} \otimes E$ associated to a squarefree element $f \in \mathcal{O}_K^{\times}/(\mathcal{O}_K^{\times})^2$ is isomorphic to the quadratic twist E_f of E over K. Suppose one has the Weierstrass model for the elliptic curve $E : y^2 = x^3 + Ax + B$. The Weil restriction of scalars with respect to the field extension $K(\sqrt{f})/K$ corresponds to the 2-dimensional abelian variety inside $\mathbb{A}^4 := \mathrm{Spec}\,(K[x_0, x_1, y_0, y_1])$ defined by the equation

$$(y_0 + y_1\sqrt{f})^2 = (x_0 + x_1\sqrt{f})^3 + A(x_0 + x_1\sqrt{f}) + B. \tag{1.10}$$

Note that the K-rational coefficient terms for $\sqrt{f}$ and the K-rational terms cut out the 2-dimensional abelian variety inside $\mathbb{A}^4$:

$$\begin{aligned} y_0^2 + y_1^2 f &= x_0^3 + 3f x_0 x_1^2 + A x_0 + B \\ 2y_0 y_1 &= 3x_0^2 x_1 + f x_1^3 + A x_1 \end{aligned} \tag{1.11}$$

If $y_0 = 0$, then one recovers the quadratic twist of the elliptic curve (assuming $x_1 = 0$)

$$y_1^2 f = x_0^3 + Ax_0 + B. \tag{1.12}$$

On the other hand, if $y_1 = 0$, then one recovers the elliptic curve (assuming $x_1 = 0$)

$$y_0^2 = x_0^3 + Ax_0 + B. \tag{1.13}$$

Because the action of $\mathrm{Gal}(K(\sqrt{f})/K)$ on $\mathrm{Res}_K^{K(\sqrt{f})} E$ is given by cyclic permutations of summands, it follows that as group schemes over $K(\sqrt{f})$,

$$E \oplus E_f \cong \mathrm{Res}_K^{K(\sqrt{f})} E \cong E \oplus (\mathcal{I}_{f,2} \otimes E) \tag{1.14}$$

which implies the desired isomorphism over K

$$E_f \cong (\mathcal{I}_{f,2} \otimes E) \tag{1.15}$$

because both group schemes are fixed by the action of $\mathrm{Gal}(K(\sqrt{f})/K)$. Throughout this manuscript, we will primarily use the notation E_f to denote the quadratic twist of the elliptic curve E.

Remark 1.3.3. For any prime ℓ, the short exact sequence of group schemes

$$0 \to \mathcal{I}_{f,\ell} \otimes E \to \mathrm{Res}_K^{K(\sqrt[\ell]{f})} E \to E \to 0 \tag{1.16}$$

implies that

$$\mathrm{rank}_{\mathbb{Z}}(\mathcal{I}_{f,\ell} \otimes E)(K) = \mathrm{rank}_{\mathbb{Z}} E(K(\sqrt[\ell]{f})) - \mathrm{rank}_{\mathbb{Z}} E(K) \tag{1.17}$$

Remark 1.3.4. Recall that the Galois group $\mathrm{Gal}(K(\sqrt[\ell]{f})/K)$ acts on $\mathrm{Res}_K^{K(\sqrt[\ell]{f})} E$ by cyclically permuting the summands indexed by the elements of the Galois group. This

implies that the endomorphism ring of $\mathcal{I}_{f,\ell} \otimes E$ contains the group ring

$$\mathrm{End}(\mathcal{I}_{f,\ell} \otimes E) \supset \frac{\mathbb{Z}\left[\left(\mathrm{Gal}(K(\sqrt[\ell]{f})/K)\right)^{\times}\right]}{(1 + \sigma_{\ell,f} + \cdots + \sigma_{\ell,f}^{\ell-1})}. \tag{1.18}$$

where $\sigma_{\ell,f}$ is the generator of the Galois group $\mathrm{Gal}(K(\sqrt[\ell]{f})/K)$. With abuse of notation, we denote by $\sigma_{\ell,f}$ a fixed choice of a generator of the multiplicative group $\left(\mathrm{Gal}(K(\sqrt[\ell]{f})/K)\right)^{\times}$. We warn the readers that the generator $\sigma_{\ell,f}$ is not identical to the generator of the Galois group $\mathrm{Gal}(K(\mu_\ell)/K)$ for the case when $\mu_\ell \not\subset K$.

We note that the construction of the abelian variety A_f (or $\mathcal{I}_{f,\ell} \otimes E$) appears in different notation in previous literature. For example, Klagsbrun, Mazur, and Rubin 2014 utilizes the notation E^χ for a choice of an order ℓ character $\chi \in Hom(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/\ell\mathbb{Z})$ to denote the $\ell - 1$ dimensional abelian variety A_f obtained with respect to the cyclic ℓ extension L/K. We provide below a list of notations introduced in Klagsbrun, Mazur, and Rubin 2013; Klagsbrun, Mazur, and Rubin 2014, which in particular will be used interchangeably with the notations A_f throughout the rest of the manuscript.

Definition 1.3.5. We introduce the following notations, as stated in Klagsbrun, Mazur, and Rubin 2014, Sections 5, 7, and 9.

- Σ: a set of places of K that includes places of bad reduction of E.
- Σ_E: a subset of Σ consisting only of places of bad reduction of E.
- σ: a square-free product of places v of K such that $v \notin \Sigma$.
- $\deg \sigma$: the sum of degrees of places $v \mid \sigma$, i.e. $\deg \sigma = \sum_{v|\sigma} \deg v$.
- $\Sigma(\sigma)$: a set of places of K that includes a set of places in Σ and a set of places dividing σ.
- $d_{\Sigma(\sigma)}$: the sum of degrees of elements in $\Sigma(\sigma)$, i.e. $d_{\Sigma(\sigma)} = \sum_{v \in \Sigma(\sigma)} \deg v$.
- Ω_σ: the set of finite cartesian products of local characters

$$\chi := (\chi_v)_v \in \prod_{\substack{v\in\Sigma \text{ or} \\ v|\sigma}} \mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell)$$

such that the component χ_v is ramified if $v \mid \sigma$. For the sake of convenience, we will denote by $\mathrm{Hom}_{unr}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell)$ the set of unramified local characters at place v, and by $\mathrm{Hom}_{ram}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell)$ the set of ramified local characters at place v. Assuming that $\mu_\ell \subset K_v$, there are ℓ distinct unramified local characters at v, and $\ell(\ell-1)$ distinct ramified local characters at v.

- Ω_E: the set of finite Cartesian products of local characters

$$\chi := (\chi_v)_v \in \prod_{v\in\Sigma_E} \mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_p)$$

- Given a global character $\chi \in \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_\ell)$, the twist E^χ is defined as follows (see Mazur, Rubin, and Silverberg 2007, Definition 5.1 for further details):

  Let F/K be the cyclic Galois extension of degree ℓ corresponding to the character χ. Denote by L/K the Galois closure of F with $G := \mathrm{Gal}(L/K)$. Denote by $K[G]$ the group ring of G with coefficients in K. Then $K[G]$ admits a decomposition into a direct sum of minimal two-sided ideals

$$K[G] = \oplus_\rho K[G]_\rho$$

  where ρ spans the set of irreducible K-representations of G, and $K[G]_\rho$ is the sum of all left ideals of $K[G]$ isomorphic to ρ.

  Let I_F be the sum of integral left ideals of $K[G]$ isomorphic to χ, i.e.

$$I_F := K[G]_\chi \cap \mathcal{O}_K[G]$$

Then the twist of E by χ is given by

$$E^{\chi} := I_F \otimes E.$$

Note that if χ is a quadratic character, then E^{χ} is the quadratic twist of E over K. If χ is a cyclic order-ℓ character, one can take E^{χ} to be the kernel of the norm map

$$E^{\chi} := \mathrm{Ker}\left(\mathrm{Res}_K^{L^{\chi}} E \to E\right) \tag{1.19}$$

from the Weil restriction of scalars of E/K associated to the cyclic ℓ-extension L^{χ}/K associated to the character χ. The K-rational points of $\mathrm{Res}_K^{L^{\chi}} E$ are the L^{χ}-rational points of E, and the twist E^{χ}/K (identical to A_f or $\mathcal{I}_{f,\ell} \otimes E$ if one takes $L^{\chi} = K(\sqrt[\ell]{f})$) is a $\ell - 1$ dimensional abelian variety over K.

1.3.2 Selmer groups

This subsection closely follows Chapter 2 of Park 2024a.

One of the well-studied strategies to bound the rank of an abelian variety A is to construct its Selmer group associated to a choice of an element $m \in \mathrm{End}(A)$. We recall the construction of Selmer groups from the following definition.

Definition 1.3.6. Let A_K be an abelian variety defined over a global field K. Suppose that $m \in \mathrm{End}(A_K)$ has degree coprime to the characteristic of K. The m-Selmer group of the abelian variety A_K is defined as a finite subspace of the first étale cohomology groups

$$\mathrm{Sel}_m(A_K) := \mathrm{Ker}\left(H^1_{\text{ét}}(K, A_K[m]) \to \prod_v H^1_{\text{ét}}(K_v, A_K)[m]\right), \tag{1.20}$$

where the product over local cohomology groups spans over all finite places of $\mathcal{O}_K$. We note that the m-Selmer groups are constructed from comparing the long exact sequence of global and local étale cohomology groups with respect to the following short exact sequence

of group schemes:

$$0 \to A_K[m] \to A_K \to^m A_K \to 0. \tag{1.21}$$

We achieve the following short exact sequence

$$0 \to A_K(K)/mA_K(K) \to \mathrm{Sel}_m(A_K) \to Ш(A_K)[m] \to 0 \tag{1.22}$$

where $Ш(A_K)[m]$ is the m-torsion subgroup of the Tate Shafarevich group $Ш(A_K)$. Assuming that $A_K[m](K)$ is a finite R-module for some commutative finite ring R, we can obtain the upper bound of the rank of A_K as

$$\mathrm{rank}_{\mathbb{Z}} A_K(K) + \mathrm{rank}_R A_K[m](K) \leq \mathrm{rank}_R \mathrm{Sel}_m(A_K) \tag{1.23}$$

where the notation $\mathrm{rank}_R M$ for a finitely generated R-module M denotes

$$\mathrm{rank}_R M := \max_{\mathfrak{p} \subset R \text{ prime}} \left[\dim_{R/\mathfrak{p}} (M \otimes_R R/\mathfrak{p}) \right]. \tag{1.24}$$

Using the structure of the endomorphism ring of cyclic twists of elliptic curves, we can now define the following Selmer groups of cyclic prime twists of elliptic curves.

Definition 1.3.7. Let E be any elliptic curve over K which contains a primitive ℓ-th root of unity μ_ℓ. Fix an ℓ-th power free element $f \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^\ell$. Using Definition 1.3.6, we can define the following two types of prime Selmer groups of abelian varieties $\mathcal{I}_{f,\ell} \otimes E$.

1. The p-Selmer group of $\mathcal{I}_{f,\ell} \otimes E$ is a finite dimensional $\mathbb{F}_p$-vector space

$$\mathrm{Sel}_p(\mathcal{I}_{f,\ell} \otimes E) \subset H^1_{\text{ét}}(K, (\mathcal{I}_{f,\ell} \otimes E)[p]). \tag{1.25}$$

2. Recall that $\sigma_{\ell,f}$ is a generator of the multiplicative group $\mathrm{Gal}(K(\sqrt[l]{f})/K)^\times$. The $1 - \sigma_{\ell,f}$ Selmer group of $\mathcal{I}_{f,\ell} \otimes E$ is a finite dimensional $\mathbb{F}_l$-vector space

$$\mathrm{Sel}_{1-\sigma_{l,f}}(\mathcal{I}_{f,l} \otimes E) \subset H^1_{\text{ét}}(K, (\mathcal{I}_{f,l} \otimes E)[1 - \sigma_{l,f}]) \cong H^1_{\text{ét}}(K, E[l]) \tag{1.26}$$

where the last isomorphism follows from the canonical $\mathrm{Gal}(\overline{K}/K)$-module isomorphism

$$(\mathcal{I}_{f,l} \otimes E)[1 - \sigma_{l,f}] \cong E[l]. \tag{1.27}$$

(See Mazur and Rubin 2007[Proposition 4.1] for a complete proof of this fact).

Using the notations introduced in Definition 1.3.5, Klagsbrun, Mazur, and Rubin Klagsbrun, Mazur, and Rubin 2014 carefully analyzes the variations of Selmer groups of A_f over number fields using Galois cohomology groups and Poitou-Tate duality theorem. Analogous results on the variation of prime Selmer ranks of A_f under local quadratic twists of E over $\mathbb{F}_q(t)$ can also be proven using the identical argument, see for instance Chapter 1 of Milne 2006 for a rigorous treatment of Poitou-Tate duality theorems for global function fields.

Suppose that ℓ is any prime number that is coprime to the characteristic of the global function field $K = \mathbb{F}_q(t)$ of characteristic coprime to 2 and 3. Throughout this section, we assume that the following properties hold, where $F(x) \in K[x]$ is a cubic polynomial.

$$\begin{aligned}
&\bullet\ E : y^2 = F(x) \text{ is a non-isotrivial elliptic curve over } K.\\
&\bullet\ E \text{ contains a place } \infty \text{ of split multiplicative reduction.}\\
&\bullet\ \text{The constant field } \mathbb{F}_q, \text{ of characteristic coprime to } 2, 3, \ell, \text{ and contains } \mu_p.\\
&\bullet\ \text{The image of } Gal(\overline{K}/K) \to \mathrm{Aut}(E[\ell]) \text{ contains } \mathrm{SL}_2(\mathbb{F}_\ell).
\end{aligned} \tag{1.28}$$

By Igusa's theorem, for any non-isotrivial elliptic curve E, there exists a prime ℓ and a finite separable extension of $K = \mathbb{F}_q(t)$ such that E satisfies all the four conditions Igusa 1959; Bandini, Longhi, and Vigni 2009.

Definition 1.3.8. We introduce the following notations continuing from Definition 1.3.5, as stated in Klagsbrun, Mazur, and Rubin 2014, Sections 5, 7, and 9.

- Given a cyclic order-ℓ character χ, the endomorphism ring of E^χ, denoted as $\mathrm{End}(E^\chi)$, contains the group ring $\mathbb{Z}[\mathrm{Gal}(F^\chi/K)] \cong \mathbb{Z}[\zeta_\ell]$. We denote by π the unique prime

ideal of $\mathbb{Z}[\zeta_\ell]$ lying above the ideal $(\ell) \subset \mathbb{Z}$. Note that π defines an isogeny over the twist E^χ.

- Given a local character $\chi \in \Omega_\sigma$, the π-Selmer group (or $1-\sigma_\ell$ Selmer group) of the twist E^χ is given by

$$\mathrm{Sel}_\pi(E^\chi) := \mathrm{Ker}\left(H^1_{\text{ét}}(K, E[\ell]) \to \oplus_v H^1_{\text{ét}}(K_v, E[\ell])/\mathrm{im}\delta_v^\chi\right), \tag{1.29}$$

where $\delta_v^\chi : E^{\chi_v}(K_v)/\pi E^{\chi_v}(K_v) \to H^1_{\text{ét}}(K_v, E[\ell])$ is the local Kummer map at v. Under all but the third assumption stated in (1.28), we use the isomorphism

$$H^1_{\text{ét}}(K, E[\ell]) \cong H^1_{\text{ét}}(K, E^\chi[\pi]),$$
$$H^1_{\text{ét}}(K_v, E[\ell]) \cong H^1_{\text{ét}}(K_v, E_v^\chi[\pi])$$

to define the Selmer group $\mathrm{Sel}_\pi(E^\chi)$, see in particular Mazur and Rubin 2007, Proposition 4.1, Definition 4.3. Even though the reference particularly states about elliptic curves over number fields, the ideas of the proofs of relevant results are extendable to global function fields. Note that if $\ell = 2$, the π-Selmer groups of E^χ correspond to 2-Selmer groups of E twisted by a quadratic character χ.

- For $1 \leq i \leq 2$, define the set

$$\mathcal{P}_i := \{v \mid v \notin \Sigma, \mu_\ell \subset K_v, \text{and}\, \dim_{\mathbb{F}_\ell} E(K_v)[\ell] = i\}$$

We also define the set

$$\mathcal{P}_0 := \{v \mid v \notin \Sigma \cup \mathcal{P}_1 \cup \mathcal{P}_2\}.$$

The set $\mathcal{P}$ is the set

$$\mathcal{P} := \{v \mid v \notin \Sigma\} = \mathcal{P}_0 \cup \mathcal{P}_1 \cup \mathcal{P}_2.$$

- Given a positive number $d \in \mathbb{N}$, the set $\mathcal{P}_i(d)$ is defined as

$$\mathcal{P}_i(d) := \{v \in \mathcal{P}_i \mid \deg v = d\}.$$

  Likewise, the set $\mathcal{P}(d)$ is defined as

$$\mathcal{P}(d) := \{v \in \mathcal{P} \mid \deg v = d\}.$$

- Given a local character $\chi \in \Omega_\sigma$, we denote by $\mathrm{rk}(\chi)$ the dimension of $\mathrm{Sel}_\pi(E^\chi)$ as an $\mathbb{F}_\ell$-vector space.

Using the assumption (1.28), we recall the following statement from Klagsbrun, Mazur, and Rubin 2013, Lemma 4.3 that the Frobenius elements of certain primes lying above a place v over K determines which classes of $\mathcal{P}_i$ the place v lives in. Again, the original statement of the lemma is shown for arbitrary number fields, which can be extended to the case for global function fields.

Lemma 1.3.9. *Klagsbrun, Mazur, and Rubin 2013, Lemma 4.3 Fix an elliptic curve E/K satisfying the conditions stated in (1.28). Let v be a place over K such that $v \notin \Sigma$. Denote by $\mathrm{Frob}_v \in \mathrm{Gal}(K(E[\ell])/K)$ the Frobenius element associated to v. Then*

1. $v \in \mathcal{P}_2 \iff \mathrm{Frob}_v = 1$
2. $v \in \mathcal{P}_1 \iff \mathrm{Frob}_v$ *has order exactly* ℓ
3. $v \in \mathcal{P}_0 \iff \mathrm{Frob}_v^\ell \neq 1$

Remark 1.3.10. Igusa's theorem implies that any non-isotrivial elliptic curve satisfying conditions (1.28) satisfies the condition that $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{SL}_2(\mathbb{F}_\ell) \rtimes T$, where T is a cyclic subgroup of order prime to ℓ corresponding to the Galois group of the constant field extension of $K(E[\ell])/K$. With the condition that $\mu_\ell \subset K$, one may assume without loss of generality that $|T| = 1$. Nevertheless, the proofs of the results outlined in the manuscript are shown for any such finite cyclic group T.

Computing the conjugacy classes of $\mathrm{SL}_2(\mathbb{F}_\ell)$ and Theorem 2.2.1 show that there exists a constant $C > 0$ such that for sufficiently large d,

$$\max\left\{\left|\frac{\#\mathcal{P}_0(d)}{\#\mathcal{P}(d)} - \left(1 - \frac{\ell}{|T|(\ell^2-1)}\right)\right|, \left|\frac{\#\mathcal{P}_1(d)}{\#\mathcal{P}(d)} - \frac{1}{|T|\ell}\right|, \left|\frac{\#\mathcal{P}_2(d)}{\#\mathcal{P}(d)} - \frac{1}{|T|(\ell^3-\ell)}\right|\right\} < Cq^{-\frac{d}{2}}. \tag{1.30}$$

Suppose in particular that $\ell = 2$. Given a Weierstrass equation of an elliptic curve $E : y^2 = F(x)$ satisfying the conditions from Theorem 2.1.2, denote by L the cubic field extension $L = K[x]/(F(x))$. Note that the constant field of L is equal to $\mathbb{F}_q$. The sets $\mathcal{P}_0, \mathcal{P}_1$, and $\mathcal{P}_2$ correspond to set of unramified places over K not in Σ which are inert, split into two places, or totally split in L. Theorem 2.2.1 shows that there exists a constant $C > 0$ such that for sufficiently large d,

$$\max\left\{\left|\frac{\#\mathcal{P}_0(d)}{\#\mathcal{P}(d)} - \frac{1}{3}\right|, \left|\frac{\#\mathcal{P}_1(d)}{\#\mathcal{P}(d)} - \frac{1}{2}\right|, \left|\frac{\#\mathcal{P}_2(d)}{\#\mathcal{P}(d)} - \frac{1}{6}\right|\right\} < Cq^{-\frac{d}{2}} \tag{1.31}$$

Note that (1.31) immediately follows from (1.30) by setting $\ell = 2$ and $|T| = 1$.

Definition 1.3.11. Fix a square-free product of places σ coprime to elements in Σ.

Fix a local character $\chi \in \Omega_\sigma$. Given a single place $\mathfrak{v}$ over K such that $\mathfrak{v} \nmid \sigma$ and $\mathfrak{v} \notin \Sigma$, let $\chi' \in \Omega_{\sigma\mathfrak{v}}$ be a local character such that

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

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

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

1.3.3 Relevant works

This subsection closely follows Section 2 of Park 2022.

The validity of the Bhargava-Kane-Lenstra-Poonen-Rains conjecture is 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 Bhargava and Shankar 2015.

- 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 $\mathbb{Q}$ Heath-Brown 1994; Swinnerton-Dyer 2008; D. Kane 2013.

- Klagsbrun, Mazur, and Rubin generalized the construction of Markov chains suggested by Swinnerton-Dyer Swinnerton-Dyer 2008 to compute the probability distribution of 2-Selmer groups over the quadratic twist families of elliptic curves with $\mathrm{Gal}(K(E[2])/K) = S_3$. 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-ℓ twist families of elliptic curves with $\mathrm{Gal}(K(E[\ell])/K) = SL_2(\mathbb{F}_\ell)$ as well Klagsbrun, Mazur, and Rubin 2014.

- 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 $E[2](\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. As the upper bound on the height H grows to infinity, the error bounds of the probability distribution is given by an order of $O(e^{-c(\log\log\log H)^{\frac{1}{4}}})$ for some constant $c > 0$. Smith utilizes Markov chains which govern the variations of kernel ranks of alternating square matrices comprised induced from Cassels-Tate pairings. Note that the Markov chains Smith utilzied are different from those constructed by Swinnterton-Dyer and Klagsbrun, Mazur, and Rubin Alexander Smith 2017; Alexander Smith 2020; Alexander Smith 2022a; Alexander Smith 2022b.

- The Markov chains suggested by Smith can be utilized to prove the Cohen-Lenstra heuristics on l^∞-torsion subgroups of class groups of cyclic l-extensions of $\mathbb{Q}$ (assuming

the generalized Riemann hypothesis) Koymans and Pagano 2021, and Stevenhagen's conjecture on the asymptotic behavior of the solubility of negative Pell equations Koymans and Pagano 2022.

Consider the case where $K = \mathbb{F}_q(t)$ of characteristic coprime to 2 and 3. Previous studies computed the probability distribution of ℓ-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 2-Selmer groups is computed.)

Given a non-negative integer j, denote by $\mathbb{P}\left[\dim_{\mathbb{F}_2} \mathrm{Sel}_\ell(E) = j \mid E \in \mathcal{M}_n(\mathbb{F}_q)\right]$ the probability that the dimensions of 2-Selmer groups of finitely many elliptic curves of fixed height n are equal to j. Below we list three probability distributions of 2-Selmer groups of elliptic curves that can be computed over global function fields:

$$\lim_{n\to\infty} \mathbb{P}\left[\dim_{\mathbb{F}_2} \mathrm{Sel}_\ell(E) = j \mid E \in \mathcal{M}_n(\mathbb{F}_q)\right] \tag{1.32}$$

$$\lim_{q\to\infty} \lim_{n\to\infty} \mathbb{P}\left[\dim_{\mathbb{F}_2} \mathrm{Sel}_\ell(E) = j \mid E \in \mathcal{M}_n(\mathbb{F}_q)\right] \tag{1.33}$$

$$\lim_{n\to\infty} \lim_{q\to\infty} \mathbb{P}\left[\dim_{\mathbb{F}_2} \mathrm{Sel}_\ell(E) = j \mid E \in \mathcal{M}_n(\mathbb{F}_q)\right] \tag{1.34}$$

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 Q.P. Ho 2014 compute the average size of 2-Selmer groups over the universal family of elliptic curves, whereas de Jong Jong 2002 computes that of 3-Selmer groups over the same family.

- For the third limit (large-q limit, then large-height), Feng, Landesman, and Rains Tony Feng, Landesman, and Rains 2023 prove that for any composite number m, 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 proposes a Markov chain constructed from random kernel models, which governs the variation of n-Selmer groups over global function fields $\mathbb{F}_q(t)$. Using this Markov chain, they successfully prove the Poonen-Rains conjecture for n-Selmer groups of universal families of elliptic curves under the large q-limit.

- For any composite number m, the average size of m-Selmer groups of universal families of elliptic curves under the third limit were computed by Landesman 2021 over universal families of elliptic curves.

- The average size of ℓ-Selmer groups of quadratic twist families of non-isotrivial elliptic curves under the third limit were computed by the author of this paper and Wang Park and N. Wang 2023.

- The key ingredient behind computing these distributions is a careful and rigorous determination of images of monodromy over algebraic spaces whose geometric fibers parametrize ℓ-Selmer groups over a prescribed family of elliptic curves, see for instance Jong and Friedman 2011; Hall 2006; Ellenberg, Venkatesh, and Westerland 2016.

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. For example, Klagsbrun and Lemke Oliver showed that more than half the quadratic twists of elliptic curves over number fields K with partial K-rational 2-torsion points (i.e. $E[2](K) = \mathbb{Z}/2\mathbb{Z}$) and without any cyclic 4-isogeny over K have arbitrarily large 2-Selmer ranks Klagsbrun and Lemke Oliver 2015. 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 $\mathbb{F}_q$ N. Wang 2021 .

Chapter 2

A probabilistic approach

This section is based on Park 2022, which develops upon the mathematical insights for coputing probablity distribution of Selmer groups of twist families of elliptic curves with respect to fan structures, as presented in Swinnerton-Dyer 2008 and Klagsbrun, Mazur, and Rubin 2014.

2.1 Main result

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

Given a polynomial $f \in F_n(\mathbb{F}_q)$, there is a cyclic order-ℓ Galois extension $L^f := K(\sqrt[\ell]{f})$ over K. Let $\sigma_f \in \mathrm{Gal}(K(\sqrt[\ell]{f})/K)$ be a generator of the cyclic Galois group. We may associate the field L_f with a cyclic order-ℓ character $\chi_f \in \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_\ell)$ defined via the quotient map

$$\chi_f : \mathrm{Gal}(\overline{K}/K) \twoheadrightarrow \mathrm{Gal}(L^f/K) \to \mu_\ell$$

that maps σ_f to $\zeta_\ell \in \mu_\ell$.

Fix a non-isotrivial elliptic curve E over K. The goal of this manuscript focuses on

understanding the following question.

Question 2.1.1. 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 understanding the K-rational points of the $\ell - 1$ dimensional abelian variety E^{χ_f} over K defined as

$$E^{\chi_f} := \text{Ker}\left(\text{Nm}_K^{L_f} : \text{Res}_K^{L_f} E \to E\right) \tag{2.1}$$

where $\text{Nm}_K^{L_f}$ is the field norm map, and $\text{Res}_K^{L_f} E$ is the Weil restriction of scalars of E with respect to the Galois extension L_f/K. It follows that

$$\text{rank}_{\mathbb{Z}} E^{\chi_f}(K) = \text{rank}_{\mathbb{Z}} E(L^f) - \text{rank}_{\mathbb{Z}} E(K). \tag{2.2}$$

For the rest of the manuscript we use the abbreviation $\pi := 1 - \sigma_f$, as stated in Klagsbrun, Mazur, and Rubin 2014, Chapter 6. In particular, if $\ell = 2$, then $\pi = 2$, and E^{χ_f} is the quadratic twist of E by the quadratic character χ_f.

In this section, we focus on computing the dimension of the following family of π-Selmer groups of E^{χ_f}, defined as

$$\text{Sel}_\pi(E^{\chi_f}) := \text{Ker}\left(H^1_{\text{ét}}(K, E[\ell]) \to \prod_v H^1_{\text{ét}}(K_v, E^{\chi_f})[\pi]\right), \tag{2.3}$$

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

$$\mathbb{P}\left[\dim_{\mathbb{F}_\ell} \text{Sel}_\pi(E^{\chi_f}) = j \mid f \in F_n(\mathbb{F}_q)\right] := \frac{\#\{f \in F_n(\mathbb{F}_q) \mid \dim_{\mathbb{F}_\ell} \text{Sel}_\pi(E^{\chi_f}) = j\}}{\#F_n(\mathbb{F}_q)} \tag{2.4}$$

Theorem 2.1.2 (Main Theorem)**.** *Fix a prime number ℓ. Let $K = \mathbb{F}_q(t)$ be a global function field whose characteristic is coprime to* 2,3*, and $q \equiv 1$ mod ℓ. 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* $\mathrm{Gal}(K(E[\ell]/K))$ *is isomorphic to* $\mathrm{SL}_2(\mathbb{F}_\ell)$.

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

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

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

$$\left| \mathbb{P}\left[\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = j \mid f \in F_n(\mathbb{F}_q) \right] - \left(\prod_{m \geq 0} \frac{1}{1 + \ell^{-m}} \right) \left(\prod_{m=1}^{j} \frac{\ell}{\ell^m - 1} \right) \right| < \frac{A_{E,\ell,q}}{(n \log q)^{\alpha(\ell) - \epsilon}}$$

The distribution of 2-Selmer ranks of quadratic twist families of some non-isotrivial elliptic curves E over any global function field $K = \mathbb{F}_q(t)$ under certain mild conditions. The values of α for some values of $\ell = 2, 3, 5, 7$ 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 2.1.3. The condition that E is non-isotrivial further implies that conditions (ii) and (iii) in the statement of Theorem 2.1.2 are obtainable after taking finite separable extension of any global function field $K = \mathbb{F}_q(t)$ Bandini, Longhi, and Vigni 2009, Proposition 3.4.

As a corollary, we are able to obtain a partial answer to Question 2.1.1.

Corollary 2.1.4. *Assume the conditions and notations as in Theorem 2.1.2. We denote by*

$$\mathbb{P}\left[rank_{\mathbb{Z}}E(L^f) - rank_{\mathbb{Z}}E(K) = j \mid f \in F_n(\mathbb{F}_q)\right] := \frac{\#\{f \in F_n(\mathbb{F}_q) \mid rank_{\mathbb{Z}}E(L^f) - rank_{\mathbb{Z}}E(K) = j\}}{\#F_n(\mathbb{F}_q)}$$

Then we have

$$\lim_{n\to\infty} \mathbb{P}\left[rank_{\mathbb{Z}}E(L^f) - rank_{\mathbb{Z}}E(K) \leq j \mid f \in F_n(\mathbb{F}_q)\right] \leq \sum_{J=0}^{j} \left(\prod_{m\geq 0} \frac{1}{1+\ell^{-m}}\right)\left(\prod_{m=1}^{J} \frac{\ell}{\ell^m - 1}\right)$$

In particular, for sufficiently large ℓ, the rank of $E(L^f)$ increases by at most 1 from the rank of $E(K)$ for almost all $f \in \mathbb{F}_q[t]$.

Remark 2.1.5. We warn the readers, however, that the given upper bound is not binding for any values of $\ell \geq 3$ unlike the case for quadratic twist families of elliptic curves, as the ℓ-torsion subgroup of the Tate-Shafarevich group of the abelian variety E^{χ_f} is not of an even dimensional $\mathbb{F}_\ell$-vector space, as explicitly constructed by William Stein Stein 2002 and discussed in detail by Howe Howe 2001. Specific conditions which can guarantee the Tate-shafarevich groups to be of even dimension are provided in Mazur and Rubin 2007, Chapter 6. Indeed, there are conjectural statements by David, Fearnley, and Kisilevsky David, Fearnley, and Kisilevsky 2007 and Mazur and Rubin Mazur and Rubin 2019 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-ℓ extensions over $\mathbb{Q}$. The function field analogue was carefully studied in a recent work by Comeau-Lapointe, David, Lalin, and Li Comeau-Lapointe et al. 2022, 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.

2.1.1 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 determines the rate of convergence of

the desired probability distribution to the Poonen-Rains distribution.

1. **Effective Chebotarev Density Theorem**

   - **Relevant results**: Theorem 2.2.1, Corollary 2.2.2, Proposition 2.4.3, Corollary 2.3.12
   - **Error term**: $-\rho \log\left(1 - \frac{\ell}{\ell^2-1}\right)$, arising from the density that the Frobenius element of an irreducible polynomial has order prime to ℓ inside $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$.

2. **Effective Erdös-Kac Theorem**

   - **Relevant results**: Theorem 2.2.6, Proposition 2.3.9, Proposition 2.3.10
   - **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 2.5.7
   - **Error term**: $-\rho\left(\frac{\ell}{\ell^2-1}\right)$, arising from geometric rate of convergence of the constructed Markov chain to the stationary distribution.

2.1.2 Outline of the proof

We provide the outline of the proof of the main theorem along with the organization of this manuscript. We let ρ to be a parameter whose value is between 0 and 1. The motivation for the proof originates from the previous work by Swinnerton-Dyer Swinnerton-Dyer 2008 and Klagsbrun, Mazur and Rubin Klagsbrun, Mazur, and Rubin 2014 who studied Lagrangian Markov operators over $\mathbb{Z}_{\geq 0}$ which govern the distribution of dimensions of π-Selmer groups over number fields.

1. **Effective theorems**: In Section 2.2, we discuss the effective versions of Chebotarev density theorem and Erdös-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 $f = f_* f^*$, where f^* is a product of irreducible factors of f (including multiplicities) of degree greater than $\frac{4(\log n)^2}{\log q}$. In Section 2.3.1, we define the notion of splitting partitions and show using Merten's theorem and the effective Erdös-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^* is at least $(1-\epsilon)\rho(\log n + \log\log q)$ for small enough $\epsilon > 0$.
    - There is an irreducible factor of f^* whose Frobenius element in $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$ has order prime to ℓ.

3. **Equidistribution**: In Section 2.3.2, 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 2.4.1, we recall the definition of local Selmer groups of E associated to cyclic order ℓ local characters as shown in Klagsbrun, Mazur, and Rubin 2014. We use the ideas from Klagsbrun, Mazur, and Rubin 2014, Proposition 9.4 and the effective Chebotarev theorem to identify Chebotarev conditions that govern the image of the global cohomology group $H^1_{\text{ét}}(K, E[\ell])$ with respect to the localization map at a place v of K.

5. **Auxiliary Place**: In Section 2.4.2, 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 $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$ has order prime to ℓ. Using the equidistribution results from Section 2.3.2 and the Chebotarev conditions from Section 2.4.1, 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 ℓ characters. This proves the effective version of the construction

of governing Markov operators, as stated in Klagsbrun, Mazur, and Rubin 2014, Theorem 4.3, Theorem 9.5 and Swinnerton-Dyer 2008, Theorem 1.

6. **Lagrangian Markov operators**: In Section 2.5.1, 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 2.5.2, 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 2.3. Combined with the rate of convergence of the governing Markov oeprator from Section 2.5.1, we prove that the three key ingredients each give rise to the rate of convergence of the desired probability distribution to the Poonen-Rains distribution.

2.2 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 Frob_v the Frobenius element at v. Denote by g_L the genus of a finite separable field extension L/K.

2.2.1 Effective Chebotarev density theorem

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

Theorem 2.2.1 (Effective Chebotarev density theorem)**.** *Fried and Jarden 2008, Proposition 6.4.8*

Let L/K be a Galois extension of global function fields over $\mathbb{F}_q(t)$. Pick a conjugacy

class $C \subset G = \mathrm{Gal}(L/K)$. If the constant fields of L and K are both equal to $\mathbb{F}_q$, then

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

The constraint that the constant fields of L and K are identical allows one to reconstruct the counterpart of the Chebotarev density theorem with explicit error bounds for function fields. Suppose the constant field of L, say $\mathbb{F}_{q^l}$, is a non-trivial extension of the constant field $\mathbb{F}_q$ of K. Then to compute the equation stated in Theorem 2.2.1, one is required to compare whether the restriction of the conjugacy class C to $\mathrm{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q)$ agrees with the n-th power of the arithmetic Frobenius $\tau : x \mapsto x^q$ as a cyclic generator of $\mathrm{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q)$. 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 Lagarias and Odlyzko 1975. We note that Galois extensions of global function fields with non-trivial constant field extensions also satisfy the following equation:

$$\lim_{s \to 1^+} \frac{\sum_{\substack{v \text{ a place over } K \\ \mathrm{Frob}_v \in C}} |\{\mathcal{O}_K/v\}|^{-s}}{\sum_{v \text{ a place over } K} |\{\mathcal{O}_K/v\}|^{-s}} = \frac{|C|}{|G|} \tag{2.5}$$

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 2.2.2. *Let L/K be a Galois extension of global function fields over $\mathbb{F}_q(t)$. Pick two non-empty subsets $S, S' \subset G = \mathrm{Gal}(L/K)$ 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

$$q^{\frac{n}{2}} - q^{\frac{n}{4}} > 2(|G| + g_L + 2g_K)$$

Then the following inequality holds.

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

In particular, if $n \geq 2\frac{\log 8 + \log(|G| + g_L + 2g_K)}{\log q}$, then

$$\left| \frac{\{v,\ a\ place\ over\ K \mid \mathrm{Frob}_v \in S,\ \dim_{\mathbb{F}_q}(K/v) = n\}}{\{v,\ a\ place\ over\ K \mid \mathrm{Frob}_v \in S',\ \dim_{\mathbb{F}_q}(K/v) = n\}} - \frac{|S|}{|S'|} \right| < 16\frac{|S|}{|S'|}(|G| + g_L + 2g_K)q^{-\frac{n}{2}}$$

Remark 2.2.3. We note that Deligne's proof of the Weil conjectures determine the error bounds of the effective Chebotarev density theorem. We refer to Rosen 2002, Theorem 9.13B for further discussions.

2.2.2 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 2.2.4. From this section and onwards, given two positive integers n and $q \geq 5$, we denote by $m_{n,q}$ the quantity

$$m_{n,q} := \log n + \log\log q \tag{2.6}$$

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

Theorem 2.2.5 (Erdös-Kac Theorem for Function Fields)**.** *Liu 2004, 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 $a \in \mathbb{R}$,

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

Fix positive integers α, β. We denote by

$$\mathbb{P}\left[\alpha < w(f) < \beta \;\mid\; f \in F_n(\mathbb{F}_q)\right]$$

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

$$\mathbb{P}\left[\alpha \leq w(f) \leq \beta \;\mid\; f \in F_n(\mathbb{F}_q)\right] := \frac{\#\{f \in F_n(\mathbb{F}_q) \mid \alpha \leq w(f) \leq \beta\}}{\#\{f \in F_n(\mathbb{F}_q)\}} \tag{2.7}$$

Let ρ 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 $F_n(\mathbb{F}_q)$ which does not satisfy the condition above can be obtained as follows.

Theorem 2.2.6 (Effective Erdös-Kac)**.** *For sufficiently large n, there exists a fixed constant $0 < C_{EK} < 4$ such that*

$$\mathbb{P}\left[w(f) < \rho m_{n,q} \text{ or } w(f) > 2m_{n,q} \mid f \in F_n(\mathbb{F}_q)\right] < C_{EK}(n \log q)^{\rho \log \rho + 1 - \rho}. \tag{2.8}$$

Proof. From Tingting Feng, S. Wang, and Yang 2020, Theorem 1, we obtain that there exists a constant $0 < C_1 < 2$ such that

$$\mathbb{P}[w(f) > 2m_{n,q} \mid f \in F_n(\mathbb{F}_q)] < C_1(n \log q)^{-2\log 2 - 1} \tag{2.9}$$

From Tingting Feng, S. Wang, and Yang 2020, Theorem 1 and Liu 2004, Theorem 1, we also obtain that there exists a constant $0 < C_2 < 2$ such that

$$\mathbb{P}[w(f) < \rho m_{n,q} \mid f \in F_n(\mathbb{F}_q)] < C_2(n \log q)^{-\rho \log \rho + \rho - 1} \tag{2.10}$$

Combine 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

$$\mathbb{P}[w(f) < \rho m_{n,q} \text{ or } w(f) > 2m_{n,q} \mid f \in F_n(\mathbb{F}_q)] < C_{EK}(n \log q)^{-\rho \log \rho + \rho - 1}. \tag{2.11}$$

□

Remark 2.2.7. We note that Theorem 2.2.6 can be also obtained from using the results by Cohen, see for instance S. D. Cohen 1969, Theorem 6 and Cheong et al. 2022, Theorem 1.1.

2.3 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 $\mathrm{Sel}_\pi(E^{\chi_f})$ 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 $\rho m_{n,q}$ and $2m_{n,q}$.
- The number of distinct irreducible factors of f^* is at least $(1-\epsilon)\rho m_{n,q}$ for some small enough $\epsilon > 0$.
- There is an irreducible factor of f^* whose Frobenius element in $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$ has order prime to ℓ.

2.3.1 Splitting partition of polynomials over finite fields

In this subsection, we define the splitting partition with respect to a tuple of integers (n, w), which will help us organize conditions that we wish to impose on irreducible factors of $f \in F_n(\mathbb{F}_q)$.

Definition 2.3.1. Let $m < n$ be two positive integers. We denote by

$$\lambda_{[m,n]} := \{(\lambda_{i,j,k}, i, j, k)\}_{m \leq i \leq n, 1 \leq j \leq n, 0 \leq k \leq 2} \tag{2.12}$$

to denote a set of $3n(m - n + 1)$ many 4-tuples. We also use the abbreviation $\lambda_n := \lambda_{[1,n]}$.

Definition 2.3.2. Throughout the rest of the manuscript, we denote by $\mathfrak{n}$ the positive integer

$$\mathfrak{n} := \lfloor \frac{4(m_{n,q})^2}{\log q} \rfloor = \lfloor \frac{4(\log n + \log\log q)^2}{\log q} \rfloor. \tag{2.13}$$

Definition 2.3.3. Fix two positive integers n and w. We say that λ_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

$$\lambda_{i,j,k} = \begin{cases} 2 & \text{if } i = 2, j = 1, k = 2 \\ 1 & \text{if } i = 1, j = 2, k = 1 \\ 0 & \text{otherwise} \end{cases} \tag{2.14}$$

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

Definition 2.3.4. Let λ_n be a splitting partition with respect to (n, w).

1. We say that λ_n is ℓ-th power free if

$$\lambda_{i,j,k} = 0 \text{ whenever } j \geq \ell \tag{2.15}$$

   In other words, any polynomial $f \in F_n(\mathbb{F}_q)$ admitting the splitting partition λ_n is a ℓ-th power free polynomial over $\mathbb{F}_q$.

2. We say that λ_n is admissible if it satisfies

$$\lambda_{i,j,k} = 0 \text{ whenever } i \leq \mathfrak{n} \tag{2.16}$$

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

3. We say that λ_n is forgettable if

$$\lambda_{i,j,k} = 0 \text{ whenever } i > \mathfrak{n} \tag{2.17}$$

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

4. We say that an admissible partition λ_n is locally arrangeable if

$$\lambda_{i,j,0} \neq 0 \text{ for some } i > N \text{ and } j \not\equiv 0 \bmod \ell \tag{2.18}$$

   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 $\mathfrak{n}$ and of multiplicity coprime to ℓ.

Definition 2.3.5. We define the following set of splitting partitions with respect to a tuple of positive integers (n, w).

- $\Lambda_{n,w} := \{\lambda_n \mid \lambda_n \text{ is a splitting partition with respect to } (n, w)\}$

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

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

Definition 2.3.6. 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

$$f^* := \prod_{\substack{g|f \\ g\in\cup_{i=N+1}^{n}\mathcal{P}(d)}} g^{v_g(f)}, \quad f_* := \prod_{\substack{g|f \\ g\in\cup_{i=1}^{N}\mathcal{P}(d)}} g^{v_g(f)} \tag{2.19}$$

We note that $f = f^* f_*$, where the irreducible factors of f^* are all of degree greater than N (and likewise for f_*).

Definition 2.3.7. 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

$$F_{n,(w,w')}(\mathbb{F}_q) := \{f \in F_n(\mathbb{F}_q) \mid w(f) = w \text{ and } w(f^*) = w'\} \tag{2.20}$$

2. Given a positive integer $N < n$, we denote by

$$F_{(n,N),(w,w')}(\mathbb{F}_q) := \{f \in F_{n,(w,w')}(\mathbb{F}_q) \mid \deg f^* = N \text{ and } f^* \text{ is } \ell\text{-th power free}\} \tag{2.21}$$

3. Given a locally arrangeable partition $\lambda \in \Lambda_{N,w'}^{la}$ and a forgettable partition $\eta \in \Lambda_{n-N,w-w'}^{for}$, we denote by

$$F_{(n,N),(w,w')}^{(\lambda,\eta)}(\mathbb{F}_q) := \{f \in F_{(n,N),(w,w')}(\mathbb{F}_q) \mid f^* \text{ admits } \lambda \in \Lambda_{N,w'}^{la},\ f_* \text{ admits } \eta \in \Lambda_{n-N,w-w'}^{for}\}. \tag{2.22}$$

4. We denote by $\hat{F}_{(n,N),(w,w')}(\mathbb{F}_q)$ the following subset of $F_{(n,N),(w,w')}(\mathbb{F}_q)$:

$$\hat{F}_{(n,N),(w,w')}(\mathbb{F}_q) := \bigsqcup_{\lambda \in \Lambda^{la}_{N,w'}} \bigsqcup_{\eta \in \Lambda^{for}_{n-N,w-w'}} F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q). \tag{2.23}$$

Remark 2.3.8. The construction of $F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$ is closely related to the construction of fan structure from Klagsbrun, Mazur, and Rubin 2014, Chapter 2, 3, 4. Given two sets B and C, denote by

$$B * C := \{\{\delta\} \cup \{q\} \mid \delta \in B, q \in C \setminus \{q\}\}, \tag{2.24}$$

as stated in Klagsbrun, Mazur, and Rubin 2014, Chapter 4, Page 1085. Note that if $B \cap C = \emptyset$, then $B * C = B \times C$. For any positive integer $m > 0$, inductively define

$$\begin{aligned} \mathcal{P}_k(i)^{*1} &= \mathcal{P}_k(i) \\ \mathcal{P}_k(i)^{*m} &= \mathcal{P}_k(i)^{*(m-1)} * \mathcal{P}_k(i) \end{aligned} \tag{2.25}$$

Then one has

$$F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) = \left[\prod_{i,j,k} \mathcal{P}_k(i)^{*\lambda_{i,j,k}}\right] \times \left[\prod_{\hat{i},\hat{j},\hat{k}} \mathcal{P}_k(i)^{*\eta_{\hat{i},\hat{j},\hat{k}}}\right] \tag{2.26}$$

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 $\mathfrak{n}$.

Proposition 2.3.9. *Suppose $m_{n,q} := \log n + \log\log q$ satisfies the condition that $m_{n,q} > e^{e^e}$. Let $\epsilon = \frac{1}{\log\log m_{n,q}}$. Then*

$$\#\{f \in F_n(\mathbb{F}_q) \mid w(f_*) > \epsilon m_{n,q}\} < q^n \cdot 4 \cdot (n \log q)^{-(\log m_{n,q})^{1-\sqrt{\epsilon}}} \tag{2.27}$$

where f_* is the product of all irreducible factors (with multiplicities) of f of degree at most $\mathfrak{n}$.

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 Merten'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

$$q^n \cdot \frac{1}{r!} \cdot \left(\sum_{g \in \mathcal{Q}} q^{-\deg(g)} \right) \tag{2.28}$$

For our purposes, we let

$$\mathcal{Q} := \cup_{i=1}^{\mathfrak{n}} \mathcal{P}(i) \tag{2.29}$$

where we recall that $m_{n,q} := \log n + \log\log q$ and $\mathfrak{n} := \lfloor \frac{4(\log n + \log\log q)^2}{\log q} \rfloor = \lfloor \frac{4m_{n,q}^2}{\log q} \rfloor$. Then

$$\sum_{g \in \mathcal{Q}} q^{-\deg g} = \sum_{k=1}^{\mathfrak{n}} \#\mathcal{P}(i) \cdot q^{-i} \leq 2 \cdot \sum_{k=1}^{\mathfrak{n}} \frac{1}{i} \leq 2\log(\mathfrak{n}) + 2 \leq 4\log m_{n,q} + 4\log 2 + 2. \tag{2.30}$$

Suppose that $m_{n,q} > e^{e^e}$. We let

$$r := \epsilon m_{n,q}, \;\; \epsilon := \frac{1}{\log\log m_{n,q}} \tag{2.31}$$

Sterling's approximation theorem shows that for such n satisfying $m_{n,q} > e^{e^e}$,

$$\begin{aligned} \frac{1}{r!} &< \frac{1}{\sqrt{2\pi r}\left(\frac{r}{e}\right)^r} \\ &= \frac{1}{\sqrt{2\pi\epsilon m_{n,q}}} \cdot (n\log q)^{-\epsilon\log m_{n,q} - \epsilon\log\epsilon + \epsilon} \end{aligned} \tag{2.32}$$

We note that because $0 < \epsilon < 1$, it follows that $0 < \epsilon - \epsilon\log\epsilon < 1$. Hence, the above equation can be simplified as

$$\frac{1}{r!} < \frac{1}{\sqrt{\pi m_{n,q}}} \cdot (n\log q)^{-\epsilon\log m_{n,q} + 1} \tag{2.33}$$

Combining with equation (2.28), we obtain

$$\begin{aligned}\#\{f \in F_n(\mathbb{F}_q) \mid w(f_*) > \epsilon m_{n,q}\} &< q^n \cdot \frac{4\log m_{n,q} + 4\log 2 + 2}{\sqrt{\pi m_{n,q}}} \cdot (n\log q)^{-\epsilon \log m_{n,q}+1} \\ &< q^n \cdot 4 \cdot (n\log q)^{-\epsilon \log m_{n,q}+1}\end{aligned} \tag{2.34}$$

The statement of the proposition follows from the inequality that whenever $m_{n,q} > e^{e^e}$, we have $\epsilon \log m_{n,q} - 1 > (\log m_{n,q})^{1-\sqrt{\epsilon}}$. □

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

Proposition 2.3.10. *Let $\rho \in (0,1)$ be a positive number. Suppose n is a positive integer such that $m_{n,q} > e^{e^e}$. Let $\epsilon = \frac{1}{\log\log m_{n,q}}$. Then*

$$\begin{aligned}&\#F_n(\mathbb{F}_q) - \sum_{w=\rho m_{n,q}}^{2m_{n,q}} \sum_{w'=(1-\epsilon)w}^{w} \sum_{N=w'\mathfrak{n}}^{n} \hat{F}_{(n,N),(w,w')}(\mathbb{F}_q) \\ &\leq 4 \cdot q^n \cdot \max\left(n^{-\rho\log\rho+1-\rho}, m_{n,q}^2 \cdot \left(\frac{\ell}{\ell^2-1}\right)^{(1-\epsilon)\rho m_{n,q}}\right)\end{aligned} \tag{2.35}$$

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

Proof. By Theorem 2.2.6 and Proposition 2.3.9, for any small enough $\epsilon > 0$,

$$\#F_n(\mathbb{F}_q) - \sum_{w=\rho m_{n,q}}^{2m_{n,q}} \sum_{w'=(1-\epsilon)w}^{w} \#F_{n,(w,w')}(\mathbb{F}_q) \leq 4 \cdot q^n \cdot n^{-\rho \log \rho + 1 - \rho} \tag{2.36}$$

Using the definition of f^*, it follows that if f^* is not ℓ-th power free, then the degree of the ℓ-th power free part of f^* is at most $n - \ell\mathfrak{n}$. Therefore, one obtains that

$$\#F_{n,(w,w')}(\mathbb{F}_q) - \sum_{N=w'\mathfrak{n}}^{n} \#F_{(n,N),(w,w')}(\mathbb{F}_q) \leq q^n \cdot n^{-4(\ell-1)(\log n)^2} \tag{2.37}$$

Using the definition of $\Lambda_{n,w}$ it follows that for any four integers $n > N$ and $w > w'$,

$$F_{(n,N),(w,w')} = \bigsqcup_{\lambda \in \Lambda^{ad}_{N,w'}} \bigsqcup_{\eta \in \Lambda^{for}_{n-N,w-w'}} F^{(\lambda,\eta)}_{(n,N),(w,w')} \tag{2.38}$$

Applying Theorem 2.2.1 with respect to the field $K(E[\ell])/K$, we obtain that

$$\sum_{N=w'\mathfrak{n}}^{n} \left(\#F_{(n,N),(w,w')}(\mathbb{F}_q) - \sum_{\lambda \in \Lambda^{la}_{N,w}} \sum_{\eta \in \Lambda^{for}_{n-N,w-w'}} \#F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) \right) \leq q^n \cdot \left(\frac{\ell}{\ell^2 - 1} \right)^{w'} \tag{2.39}$$

where the quantity $\left(\frac{\ell}{\ell^2-1}\right)^{w'}$ is the leading term of the probability that none of the irreducible factors of f^* are in $\mathcal{P}_0$. Combining equations (2.36), (2.37), and (2.39), we obtain the statement of the proposition. □

2.3.2 Equidistribution of local characters

In this subsection, we prove that for sufficiently large n, the probability distribution that the set of global cyclic order-ℓ characters induced from the set of irreducible polynomials of degree n forms a uniform distribution when restricted to the set of finite Cartesian products of local unramified cyclic order-ℓ characters at finitely many places of degree strictly less than n. The probabilistic behavior of the restrictions of global characters over global function fields are well-studied, for instance as seen from the following Theorem

from Hsu 1998.

Theorem 2.3.11 (Theorem 2.1, Hsu 1998)**.** *Let h be any square-free polynomial over $\mathbb{F}_q$. Let χ_h be a non-trivial character $\chi : (\mathbb{F}_q[t]/h)^\times \to \mathbb{C}^\times$. Then*

$$\sum_{v \in \mathcal{P}(i)} \chi(v) \leq (\deg h + 1)\frac{q^{\frac{i}{2}}}{i}. \tag{2.40}$$

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-ℓ 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 $q^{-\frac{n}{2}}$.

Corollary 2.3.12. *Let $K = \mathbb{F}_q(t)$ be a global function field such that $\mu_\ell \subset \mathbb{F}_q$. Let $h_1, h_2, \cdots, h_w$ be irreducible polynomials over $\mathbb{F}_q$. Given a place v of degree i, denote by $\left(\frac{v}{h_k}\right)_\ell \in \mu_\ell$ the ℓ-th power residue symbol. Then for any $a \in \mu_\ell^{\oplus w}$,*

$$\left| \frac{\#\{v \in \mathcal{P}(i) \mid \left(\left(\frac{v}{h_k}\right)_\ell\right)_{k=1}^{w} = a \in \mu_\ell^{\oplus w}\}}{\#\mathcal{P}(i)} - \frac{1}{p^w} \right| < \left(\sum_{k=1}^{w} \deg h_k + 1\right) \cdot q^{-i/2}/i. \tag{2.41}$$

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

$$\sum_{\chi \in \Omega} \frac{\chi(g_1)}{\chi(g_2)} = \begin{cases} |H| & \text{if } g_1 = g_2 \\ 0 & \text{otherwise .} \end{cases} \tag{2.42}$$

We let H to be the abelian group isomorphic to $\mu_\ell^{\oplus w}$ generated by the Legendre symbols

$$\left\{ \left(\frac{\cdot}{h_1}\right)_\ell, \left(\frac{\cdot}{h_2}\right)_\ell, \cdots, \left(\frac{\cdot}{h_w}\right)_\ell \right\} \tag{2.43}$$

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

$$\sum_{v\in\mathcal{P}(i)}\sum_{\chi\in\Omega}\frac{\chi\left(\left(\frac{v}{h_1}\right)_\ell,\left(\frac{v}{h_2}\right)_\ell,\cdots,\left(\frac{v}{h_w}\right)_\ell\right)}{\chi(a)} = \#\left\{v\in\mathcal{P}(i)\mid \left(\left(\frac{v}{h_k}\right)_\ell\right)_{k=1}^{w} = a\right\}\cdot\ell^w \quad (2.44)$$

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

$$= \#\mathcal{P}(i) + \sum_{\substack{\chi\in\Omega\\ \chi\neq id}}\sum_{v\in\mathcal{P}(i)}\frac{\chi\left(\left(\frac{v}{h_1}\right)_\ell,\left(\frac{v}{h_2}\right)_\ell,\cdots,\left(\frac{v}{h_w}\right)_\ell\right)}{\chi(a)} \quad (2.45)$$

Using Theorem 2.3.11, 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

$$\left|\frac{\#\{v\in\mathcal{P}(i)\mid \left(\left(\frac{v}{h_k}\right)_\ell\right)_{k=1}^{w} = a\in\mu_\ell^{\oplus w}\}}{\#\mathcal{P}(i)} - \frac{1}{p^w}\right| < (\sum_{k=1}^{w}\deg(h_i)+1)\cdot\frac{q^{-i/2}}{i}. \quad (2.46)$$

□

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 2.3.13. *Let E be an elliptic curve over K satisfying conditions in (1.28). Suppose that $h_1, h_2, \cdots, h_w$ are irreducible polynomials over $\mathbb{F}_q$ such that $K(\sqrt[\ell]{h_k})\cap K(E[\ell]) = K$ for all $1\le k\le w$. Let n be an integer such that $\sum_{k=1}^{w}\deg h_k \le n$ and $w\le 2m_{n,q}$. Then for sufficiently large n, for any element $a\in\mu_\ell^{\oplus w}$, and $i>\mathfrak{n}$, there exists a constant $C_{E,\ell,q}>0$ depending only on E, ℓ, q such that*

$$\left|\frac{\#\{v\in\mathcal{P}_k(i)\mid \left(\left(\frac{v}{h_k}\right)_\ell\right)_{k=1}^{w} = a\in\mu_\ell^{\oplus w}\}}{\#\mathcal{P}_k(i)} - \frac{1}{p^w}\right| < (n\log q)^{-2m_{n,q}+1}. \quad (2.47)$$

Proof. Given an irreducible polynomial h over $\mathbb{F}_q$, consider the cyclic order-ℓ abelian extension $K(\sqrt[\ell]{h})/K$. Then if v is coprime to h, then the ℓ-th power residue symbol $\left(\frac{v}{h}\right)_\ell$

defines the action of the Frobenius element Frob_v on $\sqrt[\ell]{h}$ via

$$\mathrm{Frob}_v(\sqrt[\ell]{h}) = \left(\frac{v}{h}\right)_\ell \sqrt[\ell]{h}$$

which in fact originates from the definition of the Artin reciprocity map, see Rosen 2002, Chapter 3, Chapter 10 for a detailed description.

With the irreducible polynomials $h_1, h_2, \cdots, h_w$ as stated, consider the field extension $L := K(E[\ell], \sqrt[\ell]{h_1}, \cdots, \sqrt[\ell]{h_w})$. Because $K(\sqrt[\ell]{h_k}) \cap K(E[\ell]) = K$ for all k, it follows that

$$\mathrm{Gal}(L/K) \cong \mathrm{SL}_2(\mathbb{F}_\ell) \times \mu_\ell^{\oplus k} \tag{2.48}$$

and its conjugacy classes are of form $C \times \{a\}$, where $C \subset \mathrm{SL}_2(\mathbb{F}_\ell)$ is a conjugacy class and $a \in \mu_\ell^{\oplus k}$ is an element. Recall that

$$\#\mathrm{Gal}(L/K) = \ell^w \cdot (\ell^3 - \ell). \tag{2.49}$$

By Riemann-Hurwitz theorem,

$$g_L \leq \ell^w \cdot (2g_{K(E[\ell])} - 2 + \ell^3). \tag{2.50}$$

Applying Corollary 2.2.2 and Corollary 2.3.12 proves the statement of the theorem. □

2.4 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 ℓ local character, and understanding their dimensions over the subset of polynomials $F(n, N), (w, w')^{(\lambda,\eta)}(\mathbb{F}_q)$. These results will be of relevant use in Section 2.5, where we will understand the dimensions of $\mathrm{Sel}_\pi(E^{\chi_f})$ as f ranges over $F_n(\mathbb{F}_q)$.

2.4.1 Local twists

The constructions and properties of the local Selmer groups, as explored in Mazur and Rubin 2007; Klagsbrun, Mazur, and Rubin 2013; Klagsbrun, Mazur, and Rubin 2014, 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 $\mathbb{F}_q(t)$, see for example Chapter 1 of Milne 2006 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 $\mathbb{F}_q(t)$ explored from Section 2.2 which are not necessarily proven for number fields.

Definition 2.4.1. We introduce the following notations regarding local Selmer groups of E associated to cyclic order ℓ characters $\chi \in \mathrm{Hom}(\mathrm{Gal}(\overline{K_v}/K_v, \mu_\ell)$, some of which are as stated in Klagsbrun, Mazur, and Rubin 2014, Sections 5, 7, 9.

- Given a local character $\chi \in \Omega_\sigma$, the local Selmer group of E associated to the cyclic order-ℓ character χ is denoted as

$$\mathrm{Sel}(E[\ell], \chi) := \mathrm{Ker}\left(H^1_{\text{ét}}(K, E[\ell]) \to \oplus_v H^1_{\text{ét}}(K_v, E[\ell])/\mathcal{H}_v^\chi\right), \tag{2.51}$$

  where

$$\mathcal{H}_v^\chi := \begin{cases} \mathrm{im}\delta_v^\chi & \text{if } v \in \Sigma(\sigma) \\ H^1(\mathcal{O}_{K_v}, E[\ell]) & \text{if } v \notin \Sigma(\sigma) \end{cases} \tag{2.52}$$

  Under all but the third assumption stated in (1.28), we use the isomorphism

$$H^1_{\text{ét}}(K, E[\ell]) \cong H^1_{\text{ét}}(K, E^\chi[\pi]),$$
$$H^1_{\text{ét}}(K_v, E[\ell]) \cong H^1_{\text{ét}}(K_v, E_v^\chi[\pi])$$

  to define the local Selmer group $\mathrm{Sel}(E[\ell], \chi)$, see in particular Mazur and Rubin 2007, 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 $\mathcal{H}_v^\chi$ is trivial. If $v \in \mathcal{P}_1 \cap \Sigma(\sigma)$, then there is a unique 1-dimensional ramified subspace $\mathcal{H}_v^\chi$. If $v \in \mathcal{P}_2 \cap \Sigma(\sigma)$, then there are ℓ distinct 2-dimensional ramified subspaces $\mathcal{H}_v^\chi$, each corresponding to a tamely totally ramified cyclic ℓ extension over K_v.

- Given a local character $\chi \in \Omega_\sigma$, we denote by $\mathrm{rk}(\chi)$ the dimension of $\mathrm{Sel}(E[\ell], \chi)$ as an $\mathbb{F}_\ell$-vector space.

- Denote by $t_\chi(\mathfrak{v})$ the dimension of the image of the local Selmer group $\mathrm{Sel}(E[\ell], \chi)$ with respect to the localization map at $\mathfrak{v}$, i.e.

$$t_\chi(\mathfrak{v}) := \dim_{\mathbb{F}_\ell} \mathrm{im}\left(\mathrm{loc}_\mathfrak{v} : \mathrm{Sel}(E[\ell], \chi) \to H^1(\mathcal{O}_{K_\mathfrak{v}}, E[\ell])\right) \tag{2.53}$$

  We note that if $\mathfrak{v} \in \mathcal{P}_i$, then $0 \leq t_\chi(\mathfrak{v}) \leq i$.

The relation between $t_\chi(\mathfrak{v})$ and the differences between ranks of local Selmer groups associated to characters $\chi \in \Omega_\sigma$ and $\chi' \in \Omega_{\chi,\mathfrak{v}}$ is stated in Klagsbrun, Mazur, and Rubin 2014, Proposition 7.2.

Proposition 2.4.2. *Let E be a non-isotrivial elliptic curve over K satisfying the conditions from equation (1.28). Fix a square-free product of places σ coprime to elements in Σ, and let $\mathfrak{v}$ be a place of K such that $\mathfrak{v} \notin \Sigma(\sigma)$. Fix a character $\chi \in \Omega_\sigma$. Then for any $\chi' \in \Omega_{\chi,\mathfrak{v}}$,*

$$rk(\chi') - rk(\chi) = \begin{cases} 2 & \text{if } \mathfrak{v} \in \mathcal{P}_2 \text{ and } t_\chi(\mathfrak{v}) = 0 \text{ for exactly } \ell - 1 \text{ many } \chi' \in \Omega_{\chi,\mathfrak{v}} \\ 1 & \text{if } \mathfrak{v} \in \mathcal{P}_1 \text{ and } t_\chi(\mathfrak{v}) = 0 \\ -1 & \text{if } \mathfrak{v} \in \mathcal{P}_1 \text{ and } t_\chi(\mathfrak{v}) = 1 \\ -2 & \text{if } \mathfrak{v} \in \mathcal{P}_2 \text{ and } t_\chi(\mathfrak{v}) = 2 \\ 0 & \text{otherwise} \end{cases} \tag{2.54}$$

Proof. The proof follows from adapting the proof of Klagsbrun, Mazur, and Rubin 2014,

Proposition 7.2. The two conditions required in the statement of Klagsbrun, Mazur, and Rubin 2014, Proposition 7.2, which are

1. $\mathrm{Pic}(\mathcal{O}_{K,\Sigma}) = 0$
2. The map $\mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^{\ell} \to \prod_{v\in\Sigma} K_v^{\times}/(K_v^{\times})^{\ell}$ is injective

hold regardless of the choice of Σ because $\mathcal{O}_K = \mathbb{F}_q[t]$ is a Euclidean domain. □

The probability that $t_\chi(\mathfrak{v})$ achieves a certain value can be obtained from a Chebotarev condition over K obtained from $\mathrm{Sel}(E[\ell], \chi)$, as shown in Klagsbrun, Mazur, and Rubin 2014, Proposition 9.4.

Proposition 2.4.3 (Local twists of π-Selmer groups)**.** *Let E be a non-isotrivial elliptic curve over K satisfying the conditions from equation (1.28). Fix a square-free product of places σ coprime to elements in Σ. Fix a local character $\chi \in \Omega_\sigma$.*

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

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

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

$$D_{E,\ell,q} := \ell^{max_{\chi\in\Omega_E}(rk(\chi))} \tag{2.55}$$

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

$$\left|\frac{\#\{\mathfrak{v}\in\mathcal{P}_i(d) \mid \mathfrak{v}\notin\Sigma(\sigma) \text{ and } t_\chi(\mathfrak{v}) = j\}}{\#\{\mathfrak{v}\in\mathcal{P}_i(d) \mid \mathfrak{v}\notin\Sigma(\sigma)\}} - d_{i,j}\right| < C_{E,\ell,q}\cdot\ell^{3\#\Sigma(\sigma)}\cdot q^{-\frac{d}{2}}. \tag{2.56}$$

Proof. The theorem can be proved in an analogous way to how Klagsbrun, Mazur, and Rubin 2014, 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 $t_\chi(\mathfrak{v})$

We first review the ideas presented in Klagsbrun, Mazur, and Rubin 2014, Proposition 9.4. Denote by *Res* the restriction morphism of cohomology groups:

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

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

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

The field $F_{\sigma,\chi}$ satisfies the following properties, as shown in Klagsbrun, Mazur, and Rubin 2014, Proposition 9.3:

1. $F_{\sigma,\chi}$ is Galois over K.
2. There is a $\text{Gal}(K(E[\ell])/K)$-module isomorphism $\text{Gal}(F_{\sigma,\chi}/K(E[\ell])) \cong (E[\ell])^{\text{rk}(\chi)}$.
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 $c \in \text{Sel}(E[\ell], \chi)$ maps the arithmetic Frobenius $\tau \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ to the identity element of $E[\ell]$. Consider the local Kummer map $im\delta_v^\chi$ 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 $\overline{K_v}$-rational points of E is given by

$$E(\overline{K_v}) \cong \overline{K_v}^\times / \langle q \rangle,$$

which implies for any positive number n,

$$E[n](\overline{K_v}) \cong \langle q^{\frac{1}{n}}, \mu_n \rangle / \langle q \rangle,$$

see for example [Section 3.3]Bandini, Longhi, and Vigni 2009 for a detailed discussion on these results. To analyze the condition that the basis element $c \in \mathrm{Sel}(E[\ell], \chi)$ maps the arithmetic Frobenius $\tau \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ to the identity element of $E[\ell]$, it suffices to verify that $Q^\tau - Q = O$ for $Q \in E[\ell](\overline{K_v})$, which follows from the assumption that the constant field of K_v contains the primitive ℓth-root of unity.

Frobenius conjugacy class

Using the techniques of the proof from Klagsbrun, Mazur, and Rubin 2014, 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 $S_{i,j}, S_i' \subset \mathrm{Gal}(F_{\sigma,\chi}/K)$ stable under conjugation, i.e. $d_{i,j} = \frac{\#S_{i,j}}{\#S_i'}$. These subsets satisfy the condition that

$$\begin{cases} \mathfrak{v} \in \mathcal{P}_i(d) & \iff \mathrm{Frob}_\mathfrak{v} \in S_i' \\ \dim_{\mathbb{F}_\ell} \mathrm{im}\delta_\mathfrak{v}^\chi = j \text{ and } \mathfrak{v} \in \mathcal{P}_i(d) & \iff \mathrm{Frob}_\mathfrak{v} \in S_{i,j} \end{cases} \tag{2.57}$$

We refer to Klagsbrun, Mazur, and Rubin 2014, Proposition 9.4 for a detailed description of what these subsets are in $\mathrm{Gal}(F_{\sigma,\chi}/K)$.

Effective error bounds

Because the constant field of $F_{\sigma,\chi}$ is $\mathbb{F}_q$, we can use Theorem 2.2.1 to bound the error terms of the following equation:

$$\left| \frac{\#\{\mathfrak{v} \in \mathcal{P}_i(d) \mid \mathfrak{v} \notin \Sigma(\sigma) \text{ and } t_\chi(\mathfrak{v}) = j\}}{\#\{\mathfrak{v} \in \mathcal{P}_i(d) \mid \mathfrak{v} \notin \Sigma(\sigma)\}} - d_{i,j} \right|. \tag{2.58}$$

To apply Theorem 2.2.1, one needs to understand how the groups G as well as the genus $g_{F_{\sigma,\chi}}$ grow in terms of $\deg \sigma$. Proposition 2.4.2 shows that

$$\#\mathrm{Gal}(F_{\sigma,\chi}/K) = [F_{\sigma,\chi} : K(E[\ell])] \leq D_{E,\ell,q} \cdot \ell^{2\#\Sigma(\sigma)} \tag{2.59}$$

is a constant that only depends on the choice of the elliptic curve E, q, and ℓ. Recall that $F_{\sigma,\chi}/K$ is unramified away from $v \in \Sigma(\sigma)$. Hence, the Riemann-Hurwitz theorem implies that

$$g_{F_{\sigma,\chi}} \leq D_{E,\ell,q} \cdot \ell^{2\#\Sigma(\sigma)} \cdot (\ell^3 - \ell) \cdot \#\Sigma(\sigma).$$

Then one obtains that

$$\begin{aligned} \#\mathrm{Gal}(F_{\sigma,\chi}/K) + g_{F_{\sigma,\chi}} &\leq D_{E,\ell,q} \cdot \ell^{2\#\Sigma(\sigma)} \cdot (1 + (\ell^3 - \ell) \cdot \#\Sigma(\sigma)) \\ &\leq D_{E,\ell,q} \cdot \ell^{2\#\Sigma(\sigma)+3} \cdot \#\Sigma(\sigma) \\ &\leq D_{E,\ell,q} \cdot \ell^{3\#\Sigma(\sigma)+3} \end{aligned} \tag{2.60}$$

Corollary 2.2.2 implies that for any d satisfying

$$d > \frac{12 \log \ell + 2 \log D_{E,\ell,q} + (6 \log \ell) \cdot \#\Sigma(\sigma)}{\log q} \tag{2.61}$$

the following inequality holds:

$$\left| \frac{\#\{\mathfrak{v} \in \mathcal{P}_i(d) \ \mid \ \mathfrak{v} \notin \Sigma(\sigma) \text{ and } t_\chi(\mathfrak{v}) = j\}}{\#\{\mathfrak{v} \in \mathcal{P}_i(d) \ \mid \ \mathfrak{v} \notin \Sigma(\sigma)\}} - d_{i,j} \right| < 16 \cdot D_{E,\ell,q} \cdot \ell^{3\#\Sigma(\sigma)+3} \cdot q^{-\frac{d}{2}}.$$

Letting $C_{E,\ell,q} = 16 \cdot D_{E,\ell,q} \cdot \ell^3$ proves the statement of the theorem. □

Remark 2.4.4. The technical condition on the degree of the place $\mathfrak{v}$ will be used in the upcoming sections when we compute the probability distribution of local Selmer ranks of elliptic curves twisted by cyclic order-ℓ characters associated to ℓ-th power free polynomials f of large enough degree n. We will show that for almost all $f \in F_n(\mathbb{F}_q)$, the cardinality of the associated set $\Sigma(\sigma)$ is bounded above by $2m_{n,q} := 2(\log n + \log\log q)$ by Theorem

2.2.5. This in turn will allow us to compute the probability distribution of π-Selmer rank of the cyclic order-ℓ twists of E from local Selmer ranks $\mathrm{Sel}(E[\ell], \chi)$.

Remark 2.4.5. Proposition 2.4.3 states that if $\mathrm{Gal}(K(E[\ell])/K) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$, then the Chebotarev density theorem completely determines the variations of π-Selmer groups of elliptic curves twisted by local cyclic order-ℓ characters. This is not the case if the Galois group $\mathrm{Gal}(K(E[\ell])/K)$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, as carefully studied in Friedlander et al. 2013 and Alexander Smith 2022a. For example, suppose that $p = 2$ and $\mathrm{Gal}(K(E[\ell])/K) = \mathbb{Z}/3\mathbb{Z}$. Friedlander, Iwaniec, Mazur, and Rubin showed that the variation of 2-Selmer groups of certain subfamilies of quadratic twists of elliptic curves are governed by the spin of odd principal prime ideals defined over totally real cyclic Galois extensions Friedlander et al. 2013, Chapter 3, Chapter 10. Smith uses a generalized notion of spin of prime ideals called “symbols of prime ideals" Alexander Smith 2022a, Definition 3.11, Proposition 3.14 to classify which classes of prime ideals equivalently varies the Selmer groups of twistable modules, a generalized notion of quadratic twist families of abelian varieties Alexander Smith 2022a, Chapter 4. Thankfully, Proposition 2.4.3 demonstrates that one does not require to use the spin of prime ideals to determine the variations of the dimensions of $\mathrm{Sel}(E[\ell], \chi)$ as χ varies over the set of Cartesian product of local characters.

2.4.2 Auxiliary places

Given a polynomial $f \in F_n(\mathbb{F}_q)$, recall from the introduction that we can identify a cyclic order-ℓ character $\chi_f \in \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_\ell)$ via the quotient map

$$\chi_f : \mathrm{Gal}(\overline{K}/K) \twoheadrightarrow \mathrm{Gal}(L^f/K) \to \mu_\ell$$

that maps the generator $\sigma_f \in \mathrm{Gal}(L^f/K)$ to ζ_ℓ. Given a place v of K, denote by $\chi_{f,v} \in \mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell)$ the restriction of the global character χ_f to K_v.

The goal of this subsection is to understand the distribution of $\mathrm{rk}((\chi_{f,v})_v)$ as f ranges over the set $F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$ for some $\lambda \in \Lambda^{la}_{N,w'}$ and $\eta \in \Lambda^{for}_{n-N,w-w'}$. To do so, we introduce the notion of an auxiliary place of a polynomial $f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$.

Definition 2.4.6. 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

$$\overline{f} := \prod_{\substack{g|f \\ g\in\mathcal{P}_1\cup\mathcal{P}_2}} g, \quad \overline{f}_* := \prod_{\substack{g|f_* \\ g\in\mathcal{P}_1\cup\mathcal{P}_2}} g, \quad \overline{f}^* := \prod_{\substack{g|f^* \\ g\in\mathcal{P}_1\cup\mathcal{P}_2}} g \tag{2.62}$$

i.e. they are products of irreducible factors of f (and f_* and f^*, respectively) of degree greater than $\mathfrak{n}$ which lies in $\mathcal{P}_1$ or $\mathcal{P}_2$.

Definition 2.4.7 (Auxiliary place)**.** Given positive integers $n > N$ and $w > w'$, let $\lambda \in \Lambda^{la}_{N,w'}$ and $\eta \in \Lambda^{for}_{n-N,w-w'}$ be splitting partitions.

- Given a degree n polynomial $f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$, an auxiliary place of f is an irreducible polynomial $g \in \mathcal{P}_0$ of maximal degree dividing f, i.e. it is an irreducible polynomial which satisfies the condition that $\lambda_{i,j,0} = 0$ whenever $i > \deg(f_a)$.

- We denote by d_a the degree of an auxiliary place f_a of any $f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$. By definition, the degree is invariant with respect to choices of f.

- We denote by f_a the auxiliary factor of f defined as

$$f_a := \prod_{\substack{g|f \\ g\in\mathcal{P}_0(d_a)}} g^{v_g(f)}. \tag{2.63}$$

- We denote by d_{a^*} the degree of the auxiliary factor of f, which can be written as

$$d_{a^*} := d_a \cdot \left(\sum_{j=1}^{\ell-1} \lambda_{d_a,j,0} \right). \tag{2.64}$$

- Fix a polynomial $h \in F_{n-d_{a^*}}(\mathbb{F}_q)$. We define the following subset of $F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$:

$$F^{(\lambda,\eta),h}_{(n,N),(w,w')}(\mathbb{F}_q) := \left\{ f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \frac{f}{f_a} = h \right\} \tag{2.65}$$

  The above subset is empty if h does not divide any polynomial in $F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$.

By definition, the following relation holds:

$$F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) = \bigsqcup_{h\in F_{n-d_{a^*}}(\mathbb{F}_q)} F^{(\lambda,\eta),h}_{(n,N),(w,w')}(\mathbb{F}_q) \tag{2.66}$$

Definition 2.4.8. Let $f \in F_n(\mathbb{F}_q)$. We denote by Σ_f the set of places

$$\Sigma_f := \Sigma_E \cup \{v \in \mathcal{P} \mid v \text{ divides } f_*\} \tag{2.67}$$

We note that if $f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}$, then $\#\Sigma_f = \#\Sigma_E + w'$.

Definition 2.4.9. Given a polynomial $f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$, we use the abbreviation $\Omega_{\overline{f}^*}$ to denote the set of finite Cartesian products of local characters

$$\begin{aligned} \Omega_1 &= \prod_{v\in\Sigma_f} \mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell) \\ \Omega_{\overline{f}^*} &= \prod_{v\in\Sigma_f} \mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell) \times \prod_{\substack{v\mid f^* \\ v\nmid f_a}} \mathrm{Hom}_{ram}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell) \end{aligned} \tag{2.68}$$

such that the component χ_v is ramified if $v \mid f^*$, and we ignore the local characters at any places v dividing the auxiliary factor f_a of f. In particular, we enlarge the set Σ from Definition 1.3.8 to include places $v \mid f_*$ 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 $F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$ given partitions $\lambda := \{(\lambda_{i,j,k}, i, j, k)\} \in \Lambda^{ad}_{N,w'}$ and $\eta := \{(\eta_{\hat{i},\hat{j},\hat{k}}, \hat{i}, \hat{j}, \hat{k})\} \in \Lambda^{for}_{n-N,w-w'}$. Given a set X, we denote by

$$\mathrm{PConf}_n(X) := \{(x_1, \cdots, x_n) \in X^{\oplus n} \mid x_i \neq x_j \text{ for all } 1 \leq i < j \leq n\} \tag{2.69}$$

the set-theoretic ordered configuration set of n elements in X. There is a transitive action

of the symmetric group S_n on $\mathrm{PConf}_n(X)$, which prompts us to define

$$\mathrm{Conf}_n(X) := \mathrm{PConf}_n(X)/S_n \tag{2.70}$$

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

$$F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) := \left[\prod_{i,j,k} \mathrm{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i))\right] \times \left[\prod_{\hat{i},\hat{j},\hat{k}} \mathrm{Conf}_{\eta_{\hat{i},\hat{j},\hat{k}}}(\mathcal{P}_{\hat{k}}(\hat{i}))\right] \tag{2.71}$$

where we regard $\mathrm{Conf}_0(X) = \{0\}$. In particular, if a polynomial $f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$ admits an irreducible factorization via

$$\begin{aligned} f^* &:= \prod_{i,j,k} \prod_{m=1}^{\lambda_{i,j,k}} g^j_{i,j,k,m} \\ f_* &:= \prod_{\hat{i},\hat{j},\hat{k}} \prod_{m=1}^{\eta_{\hat{i},\hat{j},\hat{k}}} h^{\hat{j}}_{\hat{i},\hat{j},\hat{k},m} \end{aligned} \tag{2.72}$$

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

$$\left(\prod_{i,j,k} \{g_{i,j,k,m}\}_{m=1}^{\lambda_{i,j,k}}\right) \times \left(\prod_{\hat{i},\hat{j},\hat{k}} \{h_{\hat{i},\hat{j},\hat{k},m}\}_{m=1}^{\eta_{i,j,k}}\right) \tag{2.73}$$

Using this identification, we can reformulate Definition 2.4.7 as follows. There is a natural projection map

$$\begin{aligned} \phi_{d_a} : &\left[\prod_{i,j,k} \mathrm{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i))\right] \times \left[\prod_{\hat{i},\hat{j},\hat{k}} \mathrm{Conf}_{\eta_{\hat{i},\hat{j},\hat{k}}}(\mathcal{P}_{\hat{k}}(\hat{i}))\right] \\ &\to \left[\prod_{\substack{i,j,k \\ (i,k)\neq(d_a,0)}} \mathrm{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i))\right] \times \left[\prod_{\hat{i},\hat{j},\hat{k}} \mathrm{Conf}_{\eta_{\hat{i},\hat{j},\hat{k}}}(\mathcal{P}_{\hat{k}}(\hat{i}))\right] \end{aligned}$$

which forgets all the irreducible factors of $f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$ lying in $\prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a))$. Then

$$F^{(\lambda,\eta),h}_{(n,N),(w,w')}(\mathbb{F}_q) := \phi_{d_a}^{-1}(h). \tag{2.74}$$

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

Using the notations introduced in this subsection, an immediate result of Corollary 2.3.13 can be stated as follows.

Corollary 2.4.10. *Fix a locally arrangeable partition $\lambda \in \Lambda^{la}_{N,w'}$ and a forgettable partition $\eta \in \Lambda^{for}_{n-N,w-w'}$. Recall that d_a is the auxiliary degree, and d_{a^*} is the degree of the auxiliary factor of any polynomial $f \in F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$.*

Fix a polynomial $h \in F_{n-d_{a^*}}(\mathbb{F}_q)$. If the set $F^{(\lambda,\eta),h}_{(n,N),(w,w')}$ is non-empty and $w \le 2m_{n,q}$, then for any character $\chi \in \Omega_{\overline{f}^*}$,

$$\left| \frac{\#\{f \in F^{(\lambda,\eta),h}_{(n,N),(w,w')}(\mathbb{F}_q) \mid (\chi_{f,v})_{v\in\Sigma(\overline{f})} = \chi\}}{\#F^{(\lambda,\eta),h}_{(n,N),(w,w')}(\mathbb{F}_q)} - \frac{1}{\ell^{\#\Sigma_E(\overline{f})}} \right| < (n\log q)^{-2m_{n,q}+1}$$

Equivalently, we have

$$\left| \frac{\#\{f \in \phi_{d_a}^{-1}(h) \mid (\chi_{f,v})_{v\in\Sigma(\overline{f})} = \chi\}}{\#\phi_{d_a}^{-1}(h)} - \frac{1}{\ell^{\#\Sigma_E(\overline{f})}} \right| < (n\log q)^{-2m_{n,q}+1}$$

Proof. We note that there exists a bijection between the following sets:

$$\begin{aligned} F^{(\lambda,\eta),h}_{(n,N),(w,w')}(\mathbb{F}_q) &\to \prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a)) \\ f = hf_a &\mapsto f_a \end{aligned} \tag{2.75}$$

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

$$F : \prod_{j=1}^{\ell-1} \mathrm{PConf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a)) \to \prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a)) \tag{2.76}$$

where for any fixed f_a, every element in $F^{-1}(f_a)$ restricts to an identical character in $\Omega_{\overline{f}^*}$.

It hence suffices to compute the desired probability over the ordered configuration set $\mathrm{PConf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a))$. Iteratively applying Corollary 2.3.13 by at most $w-1$ many times gives the result. □

Definition 2.4.11. Given a locally arrangeable partition $\lambda \in \Lambda^{la}_{N,w'}$ and a forgettable partition $\eta \in \Lambda^{for}_{n-N,w-w'}$, consider the set of polynomials $F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$.

Fix $1 \leq j^* \leq \ell - 1$ 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 ϕ_{d,j^*,k^*} the canonical projection map

$$\phi_{d,j^*,k^*} : F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) \to \left[\prod_{\substack{i,j,k \\ (i,k)\neq(d_a,0) \\ (i,j,k)\neq(d,j^*,k^*)}} \mathrm{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i))\right] \times \left[\prod_{\hat{i},\hat{j},\hat{k}} \mathrm{Conf}_{\eta_{\hat{i},\hat{j},\hat{k}}}(\mathcal{P}_{\hat{k}}(\hat{i}))\right]$$

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

$$\mathrm{Conf}_{\lambda_{d,j^*,k^*}}(\mathcal{P}_{k^*}(d)) \times \prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a)).$$

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 $\phi^{-1}_{d,j^*,k^*}(h) \subset F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$ the set of fibers of ϕ_{d,j^*,k^*} at h. This set admits the following bijection:

$$\phi^{-1}_{d,j^*,k^*}(h) \cong \mathrm{Conf}_{\lambda_{d,j^*,k^*}}(\mathcal{P}_{k^*}(d)) \times \prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a))$$

We can now combine the equidistribution of characters from Corollary 2.4.10 and the Chebotarev conditions from Proposition 2.4.2 and Proposition 2.4.3. 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 2.4.12. *Assume the notations and conditions as stated in Definition 2.4.11. Let E/K be an elliptic curve satisfying conditions in (1.28).*

Given $f \in \phi^{-1}_{d,j^*,k^*}(h)$, let ω_f and ω'_f be defined as

$$\omega_f := (\chi_{f,v})_{v\in\Sigma_f(\overline{h})} \in \Omega_{\overline{h}^*}, \quad \omega'_f := (\chi_{f,v})_{v\in\Sigma_f(\overline{f})} \in \Omega_{\overline{f}^*} \tag{2.77}$$

Denote by $\delta_h : \mathbb{Z}_{\geq 0} \to [0,1]$ the probability distribution

$$\delta_h(J) := \frac{\#\{\omega \in \Omega_{\overline{h}^*} \mid rk(\omega) = J\}}{\#\Omega_{\overline{h}^*}}. \tag{2.78}$$

Let $\tilde{k} := \lambda_{d,j^*,k^*} \cdot k^*$. Then for any n such that $m_{n,q} > \deg \Delta_E$, there exists a fixed constant $C'_{E,\ell,q}$ dependent only on E, p, q such that

$$\left| \frac{\#\{f \in \phi^{-1}_{d,j^*,k^*}(h) \mid rk(\omega'_f) = J\}}{\#\phi^{-1}_{d,j^*,k^*}(h)} - (M_L^{\tilde{k}}\delta)(J) \right| < \lambda_{d,j^*,k^*} C'_{E,\ell,q} \cdot ((n\log q)^{-2m_{n,q}+6\log \ell+1}). \tag{2.79}$$

where $M_L := [\ell_{r,s}]$ is the Markov operator over $\mathbb{Z}_{\geq 0}$ given by

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

Proof. We prove by induction on the values of λ_{d,j^*,k^*}. The induction step becomes straightforward once one shows the base cases, where $\lambda_{d,j^*,k^*} = 1$. Definition 2.4.11 implies that

$$\phi^{-1}_{d,j^*,k^*}(h) = \mathcal{P}_{k^*}(d) \times \prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a))$$

By Corollary 2.4.10, and the condition that $w < 2m_{n,q}$, for any fixed $g \in \mathcal{P}_{k^*}(d)$ and

$\omega' \in \Omega_{\overline{f}^*}$,

$$\left| \frac{\#\{f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \frac{f}{f_a \cdot h} = g,\ \omega'_f = \omega'\}}{\#\phi_{d_a}^{-1}(h)} - \frac{1}{\ell^{\#\Sigma_f(\overline{f})}} \right| < (n \log q)^{-2m_{n,q}+1}. \tag{2.80}$$

Fix a non-negative integer J_0. Let $\omega \in \Omega_{\overline{h}^*}$ be any character such that $\mathrm{rk}(\omega) = J_0$. Equation (2.80) implies that for any J_0,

$$\left| \frac{\#\{f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \frac{f}{f_a \cdot h} = g, \omega_f = \omega\}}{\#\phi_{d_a}^{-1}(h)} - \frac{1}{\ell^{\#\Sigma_f(\overline{h})}} \right| < (n \log q)^{-2m_{n,q}+1}. \tag{2.81}$$

Here we are using the equidistribution of global characters over $\Omega_{\overline{h}^*}$ using the equidistribution of global characters over $\Omega_{\overline{f}^*}$. Take summation over all characters $\omega \in \Omega_{\overline{h}^*}$ with $\mathrm{rk}(\omega) = J_0$ to obain

$$\left| \frac{\#\{f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \frac{f}{f_a \cdot h} = g, \mathrm{rk}(\omega_f) = J_0\}}{\#\phi_{d_a}^{-1}(h)} - \delta_h(J_0) \right| < (n \log q)^{-2m_{n,q}+1}. \tag{2.82}$$

We note that

$$\begin{aligned} &\#\{f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \mathrm{rk}(\omega'_f) = J_1, \mathrm{rk}(\omega_f) = J_0\} \\ &= \sum_{g \in \mathcal{P}_{k^*}(d)} \#\{f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \frac{f}{f_a \cdot h} = g, \mathrm{rk}(\omega'_f) = J_1, \mathrm{rk}(\omega_f) = J_0\} \end{aligned} \tag{2.83}$$

By equation (2.81), we have that the set

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

can be evaluated as

$$= \begin{cases} \#\phi_{d_a}^{-1}(h) \cdot \left(\delta_h(J_0) + O((n \log q)^{-2m_{n,q}+1})\right) & \text{if } \mathrm{rk}(\omega'_f) - \mathrm{rk}(\omega_f) = J_1 - J_0 \\ 0 & \text{otherwise} \end{cases} \tag{2.84}$$

where the secondary error term has explicit constant term of absolute value at most 1.

Summing over all $g \in \mathcal{P}_{k^*}(d)$ and using equation (2.80), we obtain

$$\left| (2.83) - \left(\sum_{g \in \mathcal{P}_{k^*}(d)} \frac{\#\{\omega' \in \Omega_{\omega,g} \mid \mathrm{rk}(\omega') = J_1 - J_0\}}{\#\Omega_{\omega,g}} \right) \cdot \#\phi_{d_a}^{-1}(h) \cdot \delta_h(J_0) \right| \tag{2.85}$$
$$< \#\phi_{d_a}^{-1}(h) \cdot \#\mathcal{P}_{k^*}(d) \cdot 2 \cdot (n \log q)^{-2m_{n,q}+1}$$

where the notations $\Omega_{\omega,g}$ were introduced in Definition 2.4.1.

Because we assume that $d > \mathfrak{n} = \frac{4m_{n,q}^2}{\log q}$ and $w < 2m_{n,q}$, it follows that as long as $m_{n,q} > \deg \Delta_E$, the conditions for applying Proposition 2.4.3 hold. Proposition 2.4.2 and Proposition 2.4.3 show that there exists a fixed constant $C_{E,\ell,q} > 0$ depending only on the elliptic curve E, q, and ℓ such that

$$\left| \sum_{g \in \mathcal{P}_{k^*}(d)} \frac{\#\{\omega' \in \Omega_{\omega,g} \mid \mathrm{rk}(\omega') = J_1 - J_0\}}{\#\Omega_{\omega,g}} - c_{k^*,J_1-J_0} \cdot \delta_h(J_0) \cdot \#\mathcal{P}_{k^*}(d) \right| \tag{2.86}$$
$$< C_{E,\ell,q} \cdot \#\mathcal{P}_{k^*}(d) \cdot ((n \log q)^{-2m_{n,q}+6\log \ell+1}).$$

The constants c_{k^*,J_1-J_0} are probabilities obtained from this table, see for example Klagsbrun, Mazur, and Rubin 2014, Proposition 9.5 on how the table from Proposition 2.4.3 is related to the table provided below.

c_{k^*,J_1-J_0}	$k^* = 0$	$k^* = 1$	$k^* = 2$
$J_1 - J_0 = -2$	$\times$	$\times$	$1 - (\ell+1)\ell^{-J_0} + \ell^{1-2J_0}$
$J_1 - J_0 = -1$	$\times$	$1 - \ell^{-J_0}$	$\times$
$J_1 - J_0 = 0$	1	$\times$	$(\ell+1)\ell^{-J_0} - (\ell + \frac{1}{\ell})\ell^{-2J_0}$
$J_1 - J_0 = 1$	$\times$	ℓ^{-J_0}	$\times$
$J_1 - J_0 = 2$	$\times$	$\times$	ℓ^{-1-2J_0}

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,

$$\begin{aligned} c_{1,-1} &= p_{J_0,J_0-1} \\ c_{1,1} &= p_{J_0,J_0+1} \\ c_{2,-2} &= p_{J_0,J_0-1} \cdot p_{J_0-1,J_0-2} \\ c_{2,0} &= p_{J_0,J_0-1} \cdot p_{J_0-1,J_0} + p_{J_0,J_0+1} \cdot p_{J_0+1,J_0} \\ c_{2,2} &= p_{J_0,J_0+1} \cdot p_{J_0+1,J_0+2}. \end{aligned} \tag{2.87}$$

Combine equations (2.85) and (2.86), and the fact that $\#\phi^{-1}_{d,j^*,k^*}(h) = \#\phi^{-1}_{d_a}(h) \cdot \#\mathcal{P}_{k^*}(d)$ to obtain

$$\left|(2.83) - (M_L^{k^*}\delta_h)(J_1) \cdot \#\phi^{-1}_{d,j^*,k^*}(h)\right| < 2C_{E,\ell,q} \cdot \#\phi^{-1}_{d,j^*,k^*}(h) \cdot ((n\log q)^{-2m_{n,q}+6\log \ell+1}).$$

Therefore, we obtain that

$$\left|\frac{(2.83)}{\#\phi^{-1}_{d,j^*,k^*}(h)} - (M_L^{k^*}\delta_h)(J_1)\right| < C'_{E,\ell,q} \cdot ((n\log q)^{-2m_{n,q}+6\log \ell+1}) \tag{2.88}$$

where $C'_{E,\ell,q} = 6C_{E,\ell,q}$. This proves the base case of the induction step.

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

$$\phi^{-1}_{d,j^*,k^*}(h) = \mathrm{Conf}_{\lambda_{d,j^*,k^*}}(\mathcal{P}(d)) \times \prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a)) \tag{2.89}$$

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

$$F : \mathrm{PConf}_{\lambda_{d,j^*,k^*}}(\mathcal{P}(d)) \times \prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a)) \to \varphi^{-1}_{d,j^*,k^*}(h) \tag{2.90}$$

Note that for any fixed $f \in \phi^{-1}_{d,j^*,k^*}(h)$, every element in $F^{-1}(f)$ restricts to an identical

character in $\Omega_{\overline{f}^*}$. Therefore, it suffices to compute the desired probability over the set

$$\mathrm{PConf}_{\lambda_{d,j^*,k^*}}(\mathcal{P}(d)) \times \prod_{j=1}^{\ell-1} \mathrm{Conf}_{\lambda_{d_a,j,0}}(\mathcal{P}_0(d_a)).$$

By definition, we have the equation

$$\#\mathrm{PConf}_{\lambda_{d,j^*,k^*}}(\mathcal{P}(d)) = \prod_{m=1}^{\lambda_{d,j^*,k^*}} (\mathcal{P}_{k^*}(d) - m + 1) \tag{2.91}$$

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

$$\begin{aligned} &\left| \frac{\#\{f \in \phi_{d,j^*,k^*}^{-1}(h) \mid \mathrm{rk}(\omega'_f) = J_1, \mathrm{rk}(\omega_f) = J_0\}}{\#\phi_{d,j^*,k^*}^{-1}(h)} - (M_L^{\tilde{k}}\delta_h)(J_1) \right| \\ &< \lambda_{d,j^*,k^*} C'_{E,\ell,q} \cdot ((n \log q)^{-2m_{n,q}+6\log \ell+1}). \end{aligned} \tag{2.92}$$

□

Remark 2.4.13. One may regard Proposition 2.4.12 as an effective version of Klagsbrun, Mazur, and Rubin 2014, Theorem 4.3, Theorem 9.5. Instead of using fan structures, we consider a subset of polynomials over $\phi_{d,j^*,k^*}^{-1}(h)$ to show that the Markov chain M_L governs the probability distribution of ranks of local Selmer groups with explicitly computable rate of convergence.

2.5 Global Selmer groups

The goal of this section is to use the probability distribution of $\mathrm{rk}((\chi_{f,v})_v)$ ranging over $F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q)$ (Proposition 2.4.12) to prove the statement of the main theorem.

2.5.1 Governing Markov operator

We will use the Markov operator constructed from Klagsbrun, Mazur, and Rubin 2014, known as the mod ℓ Lagrangian operator, to analyze variations of π-Selmer ranks of a subfamily of global quadratic twists of elliptic curves over K satisfying the conditions from

Theorem 2.1.2.

Definition 2.5.1. Let $M_L = [\ell_{r,s}]$ be the operator over the state space of non-negative integers $\mathbb{Z}_{\geq 0}$ given by

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

Remark 2.5.2. The construction of the mod ℓ Lagrangian Markov operator dates back to previous works by Swinnerton-Dyer 2008 and Klagsbrun, Mazur, and Rubin 2014. Other references such as Alexander Smith 2017, Alexander Smith 2020, and Tony Feng, Landesman, and Rains 2023 also use Markov chains to obtain the probability distribution of l-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 Klagsbrun, Mazur, and Rubin 2014, Section 2.

Definition 2.5.3. 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 μ is the sum of probabilities at odd state spaces, i.e.

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

Proposition 2.5.4. *Klagsbrun, Mazur, and Rubin 2014, Proposition 2.4*

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

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

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

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

$$\lim_{k\to\infty} M_L^k(\mu)(n) = \prod_{j\geq 0}^{\infty}(1+\ell^{-j})^{-1}\prod_{j=1}^{n}\frac{\ell}{\ell^j - 1} \tag{2.93}$$

Remark 2.5.5. 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 2.5.6 (Geometric ergodic theorem for Markov chains)**.** *Meyn and Tweedie 1993, 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 $X_1, X_2, \cdots, X_n, \cdots : \mathcal{X} \to [0,1]$ be a sequence of random variables which satisfies

$$X_{n+1} = M(X_n) \tag{2.94}$$

for all n. Let π 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 $x_n \in \mathcal{X}$,

$$\mathbb{E}[V(M(X_n)) \mid X_n = x_k] - V(x_k) \leq -\rho V(x_k) + \kappa \tag{2.95}$$

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

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

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

Given a cyclic finite group T, Proposition 2.4.3 implies that the Markov chain

$$\left(1 - \frac{\ell}{\ell^2 - 1}\right) + \frac{1}{\ell} M_L + \frac{1}{\ell^3 - \ell} M_L^2 \tag{2.96}$$

over the state space $\mathbb{Z}_{\geq 0}$ governs the variation of π-Selmer ranks of families of elliptic curves twisted by local cyclic order-ℓ characters. To elaborate, the sequence of random variables X_n corresponds to the empirical probability distribution of dimensions of π-Selmer groups of a non-isotrivial elliptic curve E consecutively twisted by n local characters at places v satisfying the conditions from Proposition 2.4.3. The markov chain M_L provides a mechanism on how the empirical probability distribution of dimensions of π-Selmer groups of E consecutively twisted by $n+1$ local characters can be obtained from that computed over families of E consecutively twisted by n local characters.

Proposition 2.5.4 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 (2.96) is given by the Poonen-Rains distribution as stated in (2.93). One can also show that given a fixed prime number ℓ, 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 $\ell = 2$).

Corollary 2.5.7. *Let* $\mu : \mathbb{Z}_{\geq 0} \to [0, 1]$ *be a probability distribution over the state space* $\mathbb{Z}_{\geq 0}$. *Denote by* π *the stationary probability distribution of the Markov operator given by*

$$M := \left(1 - \frac{\ell}{\ell^2 - 1}\right) + \frac{1}{\ell} M_L + \frac{1}{\ell^3 - \ell} M_L^2. \tag{2.97}$$

for some fixed prime number ℓ 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

$$\sup_{z \in X} \left| \left(\left(1 - \frac{\ell}{\ell^2 - 1} \right) + \frac{1}{\ell} M_L + \frac{1}{\ell^3 - \ell} M_L^2 \right)^n (\mu) - \pi \right| < c\gamma^n (\beta^\mu + 1) \tag{2.98}$$

where the term β^μ is the expected value of the function $V(x) = \beta^x$ under the probability distribution μ, i.e. $\beta^\mu := \mathbb{E}[\beta^x \mid x \in \mu]$. Explicitly, the rate of convergence γ satisfies

$$1 - \frac{\ell}{\ell^2 - 1} < \gamma < 1 \tag{2.99}$$

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 $x \in \mathbb{Z}_{\geq 0}$,

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

Setting $\gamma = 1 - \frac{\ell}{\ell^2 - 1} + \frac{1}{\ell\beta} + \frac{1}{(\ell^3 - \ell)\beta^2}$, the corollary follows from Theorem 2.5.6. □

In particular, the above corollary implies that the rate of convergence of the Markov chain M from (2.96) is given by $1 - \frac{\ell}{\ell^2 - 1} + \epsilon$ for some positive number $\epsilon > 0$.

It now remains to show that the stationary distribution of the desired Markov chain (2.96) is the probability distribution conjectured by Poonen-Rains Bhargava, D. M. Kane, et al. 2015.

Lemma 2.5.8. *Let ℓ be any fixed value of prime, and let T be a finite cyclic group. Then the probability distribution*

$$PR(j) := \prod_{j \geq 0}^{\infty} (1 + \ell^{-j})^{-1} \prod_{j=1}^{n} \frac{\ell}{\ell^j - 1} \tag{2.100}$$

is the unique stationary distribution of the Markov chain

$$M := \left(1 - \frac{\ell}{\ell^2 - 1} \right) \cdot I + \frac{1}{\ell} M_L + \frac{1}{\ell^3 - \ell} M_L^2. \tag{2.101}$$

where I denotes the identity operator over the countable state space $\mathbb{Z}_{\geq 0}$.

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

$$\rho(\pi) = \left(1 - \frac{1}{\ell}\right)\rho(\pi) + \frac{1}{\ell}\left(1 - \rho(\pi)\right) = \left(1 - \frac{2}{\ell}\right)\rho(\pi) + \frac{1}{\ell}. \tag{2.102}$$

Therefore, we obtain that $\rho(\pi) = \frac{1}{2}$. Using Proposition 2.5.4 and the fact that the Markov chain M is aperiodic and irreducible, we immediately obtain the statement of the lemma. □

Remark 2.5.9. One crucial result from using Corollary 2.5.7 and Lemma 2.5.8 is that the stationary distribution of applying the Markov chain from (2.96) 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 2.5.10. We note that the Markov chain constructed from Smith's work is different from the Markov chain presented in this manuscript Alexander Smith 2022a; Alexander Smith 2022b. The sequence of random variables X_n Smith considers correspond to the empirical probability distribution of the subspace

$$\dim_{\mathbb{F}_\ell} \pi^{n-1}\mathrm{Sel}_{\pi^n}(E^\chi) \subset \mathrm{Sel}_\pi(E) \tag{2.103}$$

where χ ranges over grids of twists Alexander Smith 2022a, 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 Alexander Smith 2022a, 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 π^n-Selmer groups which also lie inside the π-Selmer group of E.

2.5.2 Relating global and local Selmer groups

We now obtain the desired probability distribution of dimensions of $\mathrm{Sel}_\pi(E^{\chi_f})$ 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 χ_f, as stated in Proposition 2.4.12.

Proposition 2.5.11. *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

$$m_{n,q} > max\left(e^{e^e}, \deg \Delta_E, \sqrt{3\log \ell + 1}\right) \tag{2.104}$$

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

$$\begin{aligned}&\left|\frac{\#\{f \in \hat{F}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\}}{\#\hat{F}_{(n,N),(w,w')}(\mathbb{F}_q)} - PR(J)\right| \\ &< \tilde{C}_{E,\ell,q,\beta} \cdot (n\log q)^{4\epsilon\log\beta} \cdot \left((n\log q)^{-m_{n,q}} + \left(1 - \frac{\ell}{\ell^2-1} + \frac{1}{\ell\beta} + \frac{1}{(\ell^3-\ell)\beta^2}\right)^{w'-1}\right)\end{aligned} \tag{2.105}$$

where $\hat{F}_{(n,N),(w,w')}(\mathbb{F}_q)$ is a subset of $F_n(\mathbb{F}_q)$ as stated in Definition 2.3.7.

Proof. There exists a $\mathrm{Gal}(\overline{K}/K)$-equivariant isomorphism

$$E^{\chi_f}[\pi] \cong E[\ell] \tag{2.106}$$

see Mazur and Rubin 2007, Proposition 4.1 for the proof. This implies that the π-Selmer

group of E^{χ_f} satisfies

$$\mathrm{Sel}_\pi(E^{\chi_f}) \subset H^1_{\text{ét}}(K, E[\ell]) \tag{2.107}$$

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

$$\mathrm{Sel}_\pi(E^{\chi_f}) = \mathrm{Sel}(E[\ell], (\chi_{f,v})_{v\in\Sigma_f(\overline{f}^*)}) \in \Omega_{\overline{f}^*}. \tag{2.108}$$

The relation between π-Selmer groups and local Selmer groups also holds over number fields as well, see for example Klagsbrun, Mazur, and Rubin 2014, Chapter 10.

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

$$\mathfrak{d}_z := \min\{d > \mathfrak{n} \mid \sum_{i=\mathfrak{n}+1}^{d} \sum_{j=1}^{\ell-1} \sum_{k=0}^{2} \lambda_{i,j,k} < z\} \tag{2.109}$$

In other words, it is the z-th lowest degree of distinct irreducible factors of f^*. We define polynomials $f_{\mathfrak{d}_z}$ as follows:

$$f_{\mathfrak{d}_z} := \prod_{\substack{g|f^* \\ g\in\cup_{i=\mathfrak{n}+1}^{\mathfrak{d}_z}\mathcal{P}_1(i)\cup\mathcal{P}_2(i)}} g^{v_g(f)} \tag{2.110}$$

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

$$\chi_{f,0} := (\chi_{f,v})_{v\in\Sigma_f}, \quad \chi_{f,z} := (\chi_{f,v})_{v\in\Sigma_f\cup(\overline{f_{\mathfrak{d}_z}})} \tag{2.111}$$

In other words, $\chi_{f,z}$ is the Cartesian product of restriction of the global character χ_f over places in Σ_f and places of degree at most the z-th lowest degree of distinct irreducible

factors of f^*. Using these notations, we have

$$\mathrm{Sel}_\pi(E^{\chi_f}) = \mathrm{Sel}(E[\ell], \chi_{f,w'}). \tag{2.112}$$

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

$$\Phi : F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) = \left[\prod_{i,j,k} \mathrm{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i))\right] \times \left[\prod_{\hat{i},\hat{j},\hat{k}} \mathrm{Conf}_{\eta_{\hat{i},\hat{j},\hat{k}}}(\mathcal{P}_{\hat{k}}(\hat{i}))\right] \to \left[\prod_{\hat{i},\hat{j},\hat{k}} \mathrm{Conf}_{\eta_{\hat{i},\hat{j},\hat{k}}}(\mathcal{P}_{\hat{k}}(\hat{i}))\right]$$

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

$$\begin{aligned}
&\#\{f \in \Phi^{-1}(h_*) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\} \\
&= \#\{f \in \Phi^{-1}(h_*) \mid \mathrm{rk}(\chi_{f,w'}) = J\} \\
&= \sum_{J_0=0}^{\infty} \# \left\{ f \in \Phi^{-1}(h_*) \mid \mathrm{rk}(\chi_{f,0}) = J_0, \sum_{z=1}^{w'} \mathrm{rk}(\chi_{f,z}) - \mathrm{rk}(\chi_{f,z-1}) = J \right\}
\end{aligned} \tag{2.113}$$

Denote by $\Omega_{\overline{h_*}}$ the following set of Cartesian product of local characters

$$\Omega_{\overline{h_*}} := \prod_{v \in \Sigma_E} \mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell) \times \prod_{v \mid h_*} \mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), \mu_\ell) \subset \Omega_1 \tag{2.114}$$

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

$$\delta(J) := \frac{\#\{\omega \in \Omega_{\overline{h_*}} \mid \mathrm{rk}(\omega) = J\}}{\#\Omega_{\overline{h_*}}} \tag{2.115}$$

Let d_λ be an integer associated to a choice of a splitting partition λ defined as

$$d_\lambda := \sum_{i,j} (\lambda_{i,j,1} + 2 \cdot \lambda_{i,j,2}). \tag{2.116}$$

Note that there exists a bijection

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

Inductively applying Proposition 2.4.12 to each term $\mathrm{Conf}_{\lambda_{i,j,k}}(\mathcal{P}_k(i))$, we obtain that there exists an explicit constant $C_{E,\ell,q} > 0$ such that

$$\begin{aligned} &\left| \frac{\#\{f \in \Phi^{-1}(h_*) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\}}{\#\Phi^{-1}(h_*)} - (M_L^{d_\lambda}\delta_{h_*})(J) \right| \\ &< C_{E,\ell,q} \cdot n \cdot ((n\log q)^{-2m_{n,q}+6\log\ell+1}) \\ &< C_{E,\ell,q} \cdot ((n\log q)^{-2m_{n,q}+6\log\ell+2}). \end{aligned} \tag{2.117}$$

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

$$\begin{aligned} F^{h_*}_{(n,N),(w,w')}(\mathbb{F}_q) &:= \bigsqcup_{\lambda \in \Lambda^{la}_{N,w'}} \Phi^{-1}(h_*) \\ F^{\eta}_{(n,N),(w,w')}(\mathbb{F}_q) &:= \bigsqcup_{\substack{h_* \in F_{n-N}(\mathbb{F}_q) \\ h_* \text{ admits } \eta}} F^{h_*}_{(n,N),(w,w')}(\mathbb{F}_q) \end{aligned} \tag{2.118}$$

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

$$M := \left(1 - \frac{\ell}{\ell^2-1}\right) \cdot I + \frac{1}{\ell} M_L + \frac{1}{\ell^3-\ell} M_L^2 \tag{2.119}$$

where I denotes the identity operator over the countable state space $\mathbb{Z}_{\geq 0}$. Using Theorem 2.2.1 with respect to the field extension $K(E[\ell])/K$ and $d = \mathfrak{n}$, we obtain that there exists a fixed constant $B_{E,\ell,q} > 0$ such that

$$\begin{aligned} &\left| \frac{\#\{f \in F^{h_*}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\}}{\#F^{h_*}_{(n,N),(w,w')}(\mathbb{F}_q)} - (M^{w'-1}\delta_{h_*})(J) \right| \\ &< B_{E,\ell,q} \cdot (n\log q)^{-2m_{n,q}+6\log\ell+2} \\ &< B_{E,\ell,q} \cdot (n\log q)^{-m_{n,q}} \end{aligned} \tag{2.120}$$

where I denotes the identity operator over the countable state space $\mathbb{Z}_{\geq 0}$. 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 $\Omega_{\Sigma_f(\overline{f}^*)}$, hence allowing us to apply Proposition 2.4.12.

Recall the Poonen-Rains distribution

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

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

$$\max_{J \in \mathbb{Z}_{\geq 0}} \{J \mid \delta_{h_*}(J) \neq 0\} \leq \max_{\chi \in \Omega_E} \mathrm{rk}(\chi) + 2\epsilon w. \tag{2.121}$$

By Corollary 2.5.7, we obtain that there exists a fixed constant $c > 0$ such that

$$\sup_{J \in \mathbb{Z}_{\geq 0}} \left| (M^{w'-1}\delta_{h_*})(J) - PR(J) \right| < c \cdot \left(1 - \frac{\ell}{\ell^2 - 1} + \frac{1}{\ell\beta} + \frac{1}{(\ell^3 - \ell)\beta^2}\right)^{w'-1} \cdot \mathbb{E}[\beta^x \mid x \in \delta] \tag{2.122}$$

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

$$\mathbb{E}[\beta^x \mid x \in \delta] \leq \beta^{\max_{\chi \in \Omega_E} \mathrm{rk}(\chi)} \cdot (n \log q)^{4\epsilon \log \beta} \tag{2.123}$$

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

$$(2.122) < c_\beta \cdot \left(1 - \frac{\ell}{\ell^2 - 1} + \frac{1}{\ell\beta} + \frac{1}{(\ell^3 - \ell)\beta^2}\right)^{w'-1} \cdot (n \log q)^{4\epsilon \log \beta} \tag{2.124}$$

Using triangle inequality with equation (2.117), we obtain for all $J \geq 0$ and for any small

enough $0 < \epsilon < 1$, there exists an explicit constant $\tilde{C}_{E,\ell,q,\beta} := B_{E,\ell,q} + c_\beta$ such that

$$\begin{aligned}&\left|\frac{\#\{f \in F^{h_*}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\}}{\#F^{h_*}_{(n,N),(w,w')}(\mathbb{F}_q)} - PR(J)\right| \\ &< \tilde{C}_{E,\ell,q,\beta} \cdot (n\log q)^{4\epsilon\log\beta} \cdot \left((n\log q)^{-m_{n,q}} + \left(1 - \frac{\ell}{\ell^2-1} + \frac{1}{\ell\beta} + \frac{1}{(\ell^3-\ell)\beta^2}\right)^{w'-1}\right)\end{aligned} \tag{2.125}$$

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

$$\begin{aligned}&\left|\frac{\#\{f \in F^{\eta}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\}}{\#F^{\eta}_{(n,N),(w,w')}(\mathbb{F}_q)} - PR(J)\right| \\ &< \tilde{C}_{E,\ell,q,\beta} \cdot (n\log q)^{4\epsilon\log\beta} \cdot \left((n\log q)^{-m_{n,q}} + \left(1 - \frac{\ell}{\ell^2-1} + \frac{1}{\ell\beta} + \frac{1}{(\ell^3-\ell)\beta^2}\right)^{w'-1}\right)\end{aligned} \tag{2.126}$$

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

$$\hat{F}_{(n,N),(w,w')}(\mathbb{F}_q) := \bigsqcup_{\lambda \in \Lambda^{la}_{N,w'}} \bigsqcup_{\eta \in \Lambda^{for}_{n-N,w-w'}} F^{(\lambda,\eta)}_{(n,N),(w,w')}(\mathbb{F}_q) = \bigsqcup_{\eta \in \Lambda^{for}_{n-N,w-w'}} F^{\eta}_{(n,N),(w,w')}(\mathbb{F}_q) \tag{2.127}$$

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

We now prove the main theorem of this manuscript.

Proof of Theorem 2.1.2. From Proposition 2.3.10, we obtain that

$$\begin{aligned}&\#F_n(\mathbb{F}_q) - \sum_{w=\rho m_{n,q}}^{2m_{n,q}} \sum_{w'=(1-\epsilon)w}^{w} \sum_{N=w'\mathfrak{n}}^{n} \hat{F}_{(n,N),(w,w')}(\mathbb{F}_q) \\ &\leq 4 \cdot q^n \cdot \max\left((n\log q)^{-\rho\log\rho+1-\rho}, m^2_{n,q} \cdot \left(\frac{\ell}{\ell^2-1}\right)^{(1-\epsilon)\rho m_{n,q}}\right) \\ &\leq 4 \cdot q^n \cdot \max\left((n\log q)^{-\rho\log\rho+1-\rho}, m^2_{n,q} \cdot (n\log q)^{(1-\epsilon)\rho\log\left(\frac{\ell}{\ell^2-1}\right)}\right)\end{aligned} \tag{2.128}$$

where $\epsilon = \frac{1}{\log\log m_{n,q}}$. Letting w to satisfy $\rho m_{n,q} \leq w < 2m_{n,q}$, and $(1-\epsilon)w \leq w' \leq w$, we obtain from Proposition 2.5.11 that

$$\begin{aligned}
&\left| \frac{\#\{f \in \hat{F}_{(n,N),(w,w')}(\mathbb{F}_q) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\}}{\#\hat{F}_{(n,N),(w,w')}(\mathbb{F}_q)} - PR(J) \right| \\
&< \tilde{C}_{E,\ell,q,\beta} \cdot (n\log q)^{4\epsilon\log\beta} \cdot \left((n\log q)^{-m_{n,q}} + 3 \cdot (n\log q)^{(1-\epsilon)\rho\log\left(1-\frac{\ell}{\ell^2-1}+\frac{1}{\ell\beta}+\frac{1}{(\ell^3-\ell)\beta^2}\right)} \right) \\
&< 6 \cdot \tilde{C}_{E,\ell,q,\beta} \cdot (n\log q)^{(1-\epsilon)\rho\log\left(1-\frac{\ell}{\ell^2-1}+\frac{1}{\ell\beta}+\frac{1}{(\ell^3-\ell)\beta^2}\right)+4\epsilon\log\beta}
\end{aligned} \tag{2.129}$$

Combine two equations to obtain

$$\begin{aligned}
&\left| \frac{\#\{f \in F_n(\mathbb{F}_q) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\}}{\#F_n(\mathbb{F}_q)} - PR(J) \right| \\
&< 6 \cdot m_{n,q}^2 \cdot \tilde{C}_{E,\ell,q,\beta} \cdot (n\log q)^{\alpha(\rho,\beta,\epsilon)}
\end{aligned} \tag{2.130}$$

where

$$\alpha(\rho,\beta,\epsilon) := \max \begin{cases} -\rho\log\rho + 1 - \rho \\ (1-\epsilon)\rho\log\left(\frac{\ell}{\ell^2-1}\right) \\ (1-\epsilon)\rho\log\left(1-\frac{\ell}{\ell^2-1}+\frac{1}{\ell\beta}+\frac{1}{(\ell^3-\ell)\beta^2}\right) + 4\epsilon\log\beta \end{cases} \tag{2.131}$$

We now choose $\beta = \frac{1}{\epsilon} = \log\log m_{n,q} > e$. Then we have

$$\tilde{C}_{E,\ell,q,\beta} \leq (B_{E,\ell,q} + c) \cdot (\log\log\log m_{n,q})^{\max_{\chi\in\Omega_E} \mathrm{rk}(\chi)}, \tag{2.132}$$

$$\alpha(\rho,\beta,\epsilon) = \max \begin{cases} -\rho\log\rho + 1 - \rho \\ \rho\log\left(\frac{\ell}{\ell^2-1}\right) + O(\frac{1}{\log\log m_{n,q}}) \\ \rho\log\left(1-\frac{\ell}{\ell^2-1}\right) + O(\frac{1}{\log\log\log m_{n,q}}) \end{cases} \tag{2.133}$$

We let

$$\alpha(\rho) := \max \begin{cases} -\rho \log \rho + 1 - \rho \\ \rho \log \left(\frac{\ell}{\ell^2 - 1} \right) \\ \rho \log \left(1 - \frac{\ell}{\ell^2 - 1} \right) \end{cases} \tag{2.134}$$

Then for small enough $\delta > 0$, there exists sufficiently large n and an explicit constant $A_{E,\ell,q} = 6 \cdot (B_{E,\ell,q} + c)$ such that

$$\left| \frac{\#\{f \in F_n(\mathbb{F}_q) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\pi(E^{\chi_f}) = J\}}{\#F_n(\mathbb{F}_q)} - PR(J) \right| < A_{E,\ell,q} \cdot (n \log q)^{\alpha(\rho)+\epsilon}. \tag{2.135}$$

□

Chapter 3

A geometric approach

This section is based on the following work in progress Park 2024a, the intellectual origins of which come from using middle convolution sheaves to understand vanishing of twisted L functions of elliptic curves over global function fields, as presented in N. Katz 1998 and Hall 2008.

3.1 Main result

Let $K = \mathbb{F}_q(t)$ be the global function field over the finite field $\mathbb{F}_q$ of characteristic coprime to 2 and 3. Fix a prime number $\ell > 0$ that is coprime to $2, 3$, and $\mathrm{Char}(K)$. Let E be an elliptic curve over K. Throughout this manuscript, we will assume the following five conditions.

Condition 3.1.1. Assume the following conditions on K, ℓ, and E.

1. The primitive ℓ-th roots of unity is contained in K, i.e. $\mu_\ell \subset K$.
2. The elliptic curve E/K is non-isotrivial.
3. The elliptic curve E/K admits a place of split multiplicative reduction.
4. The prime ℓ is coprime to any local Tamagawa factors of E/K.

5. The Galois group $\mathrm{Gal}(K(E[\ell])/K)$ obtained from adjoining ℓ-torsion points of E/K contains the special linear group $\mathrm{SL}_2(\mathbb{F}_\ell)$.

In this chapter, we improve the convergence rate of the probability distribution of $\{\mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K)\}$ twisted by the set of degree n polynomials f over $\mathbb{F}_q$ Park 2022. This theorem verifies that the probability distribution of $\mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K)$ twisted by the set of degree n polynomials f over $\mathbb{F}_q$ converges to the Bhargava-Kane-Lenstra-Poonen-Rains distribution Bhargava, D. M. Kane, et al. 2015; Poonen and Rains 2012 for sufficiently large n and sufficiently large q.

Theorem 3.1.2 (A geometric approach)**.** *Assume Condition 3.1.1. Then there exist integers $M_1, M_2 > 0$ and a fixed constant $C(\ell, E) > 0$ independent of n and q such that for every $n > M_1$ and $q > M_2$,*

$$\left| \frac{\#\{f \in \mathbb{F}_q[t] \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K) = r,\ \deg f = n\}}{\#\{f \in \mathbb{F}_q[t] \mid \deg f = n\}} - \prod_{i=0}^{\infty} \frac{1}{1+\ell^{-i}} \prod_{i=1}^{r} \frac{\ell}{\ell^i - 1} \right| < C(\ell, E) \cdot \frac{1}{\sqrt{q}}. \tag{3.1}$$

Other than obtaining the improved error bounds, the significance of Theorem 3.1.2 lies in the idea of the proof that the statistics of these Selmer groups can be obtained from counting $\mathbb{F}_q$ rational points of a scheme over $\overline{\mathbb{F}}_q$ which parametrize the Selmer groups of these abelian varieties. Unlike the stochastic approach taken from Park 2022, we obtain the statistics of the desired Selmer groups by applying the Grothendieck-Lefschetz trace formula to the space $\tau_{n,\sigma_{\ell,f},E}$ over $\overline{\mathbb{F}}_q$ (which will be constructed in Section 3.2) whose $\mathbb{F}_q$-rational points parametrize the elements of the Selmer groups $\mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K)$ for degree n polynomials f over $\mathbb{F}_q$.

The significance of Theorem 3.1.2 hence lies in obtaining a correspondence between the sequences of étale cohomology groups of $\{\tau_{n,\sigma_{\ell,f},E}\}_{n\geq 1}$ and stochastic properties of Markov chains over $\mathbb{Z}_{\geq 0}$ defined as $M_L := \left(1 - \frac{\ell}{\ell^2-1}\right) + \frac{1}{\ell}M + \frac{1}{\ell^3-\ell}M^2$ Klagsbrun, Mazur,

and Rubin 2014; Park 2022, where M is the Markov chain over $\mathbb{Z}_{\geq 0}$ defined as

$$M(r,s) := \begin{cases} 1 - \frac{1}{\ell^r} & \text{if } s = r-1 \\ \frac{1}{\ell^r} & \text{if } s = r+1 \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

As an application of Theorem 3.1.2, we demonstrate that a polynomial upper bound on the dimensions, homological stability, and bounds on absolute values of Frobenius eigenvalues of these étale cohomology groups $H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v)$ imply the triviality of any fixed i-th étale cohomology groups $\{\tau_{n,\sigma_{\ell,f},E}\}_{n\geq 1}$ for sufficiently large $n > N(i)$. We refer to Theorem 3.3.1 for the complete rigorous statement of the theorem.

We present the main result of the chapter as follows. Section 3.2 proves Theorem 3.1.2 by utilizing Grothendieck-Lefschetz trace formula applied to a generalization of Katz's and Hall's constructions of representable étale lisse $\mathbb{F}_\ell$ sheaves N. Katz 1998; Hall 2008 and incorporating probabilistic results obtained from the previous chapter Park 2022. Section 3.3 proves Theorem 3.3.1, along with a discussion on how one may incorporate probabilistic models, arithmetic results, and homological stability Ellenberg, Venkatesh, and Westerland 2016; Ellenberg, TriThang Tran, and Westerland 2023; Ellenberg and Landesman 2023 to obtain new results on the vanishing of twisted cohomology groups of the configuration space of unordered n points over a complex plane with k punctures.

3.2 Geometric model

In this section, we verify the Bhargava-Kane-Lenstra-Poonen-Rains heuristics for cyclic twist families of elliptic curves over $\mathbb{F}_q(t)$ by using the Grothendieck-Lefschetz trace formula to a geometric space over $\overline{\mathbb{F}_q}$ whose $\mathbb{F}_q$-rational points parametrize $1 - \sigma_{\ell,f}$ Selmer groups of cyclic twists of elliptic curves.

3.2.1 Geometric space

There are a number of recent research which utilizes the notion of colored configuration spaces, see for example Kupers, Miller, and Trithang Tran 2016; Palmer 2018. For the sake of making the paper self-contained, we introduce the notations used in this paper denoting colored configuration spaces as provided below.

Definition 3.2.1. Let $F_{n,\ell}$ be the set of ℓ-th power free polynomials f over $\overline{\mathbb{F}}_q$ of degree n which is coprime to the discriminant Δ_E of the elliptic curve E:

$$F_{n,\ell} := \left\{ f \in \overline{\mathbb{F}}_q[t] \mid \deg f = n, v_p(f) \leq \ell - 1 \text{ for all irreducible } p \in \overline{\mathbb{F}}_q[t], (f, \Delta_E) = 1 \right\}. \tag{3.3}$$

We note that $F_{n,\ell}$ can be identified with the open subscheme of the unordered configuration space of n points of $\mathbb{A}^1$ over $\overline{\mathbb{F}}_q$ with $\ell - 1$ colors $X = \{1, 2, \cdots, \ell - 1\}$, denoted as $\mathrm{Conf}_n(\mathbb{A}^1, X)$, whose elements are coprime to Δ_E. Each color corresponds to determining the valuation of the polynomial $f \in \overline{\mathbb{F}}_q[t]$ with respect to a choice of a linear polynomial $p = t - c \in \mathbb{F}_q[t]$. The elements of $F_{n,\ell}$ can be written as the set of n-many unordered tuples in $\mathbb{A}^1_{\overline{\mathbb{F}}_q} \times X$, i.e. as $\{(c_1, x_1), (c_2, x_2), \cdots, (c_n, x_n)\}$ where $c_i \in \mathbb{A}^1_{\overline{\mathbb{F}}_q}$ and $x_i \in X$.

Definition 3.2.2. A weighted partition of n into $\ell - 1$ components is an array of $\ell - 1$ integers $\eta^{[n,\ell]} := [\eta_1, \eta_2, \cdots, \eta_{\ell-1}]$ which satisfies $\eta_1 + 2\eta_2 + \cdots + (\ell - 1)\eta_{\ell-1} = n$.

Definition 3.2.3. Let $\eta^{[n,\ell]} := [\eta_1, \eta_2, \cdots, \eta_{\ell-1}]$ be a weighted partition of n into $\ell - 1$ components. Given such a partition $\eta^{[n,\ell]}$, we denote by $F_{\eta^{[n,\ell]}}$ the subset of ℓ-th power free polynomials over $\overline{\mathbb{F}_q}$ of degree n defined as

$$F_{\eta^{[n,\ell]}} := \left\{ f \in \overline{\mathbb{F}_q}[t] \mid f = g_1 g_2^2 \cdots g_{\ell-1}^{\ell-1},\ \deg g_i = \eta_i,\ g_i \text{ square-free over } \overline{\mathbb{F}_q}, (f, \Delta_E) = 1 \right\} \tag{3.4}$$

Likewise, $F_{\eta^{[n,\ell]}}$ is an open connected subscheme of the unordered configuration space of n points of $\mathbb{A}^1$ over $\overline{\mathbb{F}_q}$ with $\ell - 1$ colors $X = \{1, 2, \cdots, \ell - 1\}$, where each color i has η_i many distinct points, denoted as $\mathrm{Conf}_{\eta^{[n,\ell]}}(\mathbb{A}^1, X)$. In particular, if we denote by

$\mathrm{Conf}_n(\mathbb{A}^1)$ the unordered configuration space of n points in $\mathbb{A}^1$ without labels, then we have the inclusion

$$\begin{aligned} \mathrm{Conf}_{\eta^{[n,\ell]}}(\mathbb{A}^1, X) &\to \mathrm{Conf}_{\eta_1}(\mathbb{A}^1) \times \mathrm{Conf}_{\eta_2}(\mathbb{A}^1) \times \cdots \times \mathrm{Conf}_{\eta_{\ell-1}}(\mathbb{A}^1) \\ g_1 g_2^2 \cdots g_{\ell-1}^{\ell-1} &\mapsto (g_1, g_2, \cdots, g_{\ell-1}). \end{aligned} \tag{3.5}$$

Note that if $\Phi_{n,\ell}$ denotes the set of all partitions of n into $\ell - 1$ components, then one obtains that

$$F_{n,\ell} = \sqcup_{\eta^{[n,\ell]} \in \Phi_{n,\ell}} F_{\eta^{[n,\ell]}}. \tag{3.6}$$

Lastly, we denote by $F_{n,\ell}(\mathbb{F}_q)$ and $F_{\eta^{[n,\ell]}}(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points of $F_{n,\ell}$ and $F_{\eta^{[n,\ell]}}$. Concretely, these sets can be written as

$$F_{n,\ell}(\mathbb{F}_q) := \{ f \in \mathbb{F}_q[t] \mid \deg f = n, v_p(f) \leq \ell - 1 \text{ for all irreducible } p \in \mathbb{F}_q[t], (f, \Delta_E) = 1 \}, \tag{3.7}$$

$$F_{\eta^{[n,\ell]}}(\mathbb{F}_q) := \left\{ f \in \mathbb{F}_q[t] \mid f = g_1 g_2^2 \cdots g_{\ell-1}^{\ell-1},\ \deg g_i = \eta_i,\ g_i \text{ square-free over } \mathbb{F}_q, (f, \Delta_E) = 1 \right\}. \tag{3.8}$$

Likewise, we obtain that

$$F_{n,\ell}(\mathbb{F}_q) = \sqcup_{\eta^{[n,\ell]} \in \Phi_{n,\ell}} F_{\eta^{[n,\ell]}}(\mathbb{F}_q). \tag{3.9}$$

Because the order of the isogeny $1 - \sigma_{\ell,f}$ and the order of the cyclic character χ_f associated to the cyclic twist $\mathcal{I}_{f,\ell} \otimes E$ are identical, we cannot directly use the construction of the étale lisse-sheaves provided by Katz N. Katz 1998, Chapter 6 or Hall Hall 2008, Chapter 5. Nevertheless, the above constructions can be extended to obtain the geometric space of our interest, as we provide below. The construction of the representable sheaf is outlined analogously to Park and N. Wang 2023, Section 3.2.

Definition 3.2.4. We construct the representable étale $\mathbb{F}_\ell$-lisse sheaf $\tau_{n,\sigma_{\ell,f},E} \to F_{n,\ell}$ over $\overline{\mathbb{F}}_q$ as provided below. It is suffice to specify the construction of the étale $\mathbb{F}_\ell$-lisse sheaf

$\tau_{n,\sigma_{\ell,f},E} \to F_{\eta^{[n,\ell]}}$ given a choice of a partition $\eta^{[n,\ell]} \in \Phi_{n,\ell}$ (Here we abuse the notation and abbreviate $\tau_{n,\sigma_{\ell,f},E}|_{F_{\eta^{[n,\ell]}}} \to F_{\eta^{[n,\ell]}}$ as $\tau_{n,\sigma_{\ell,f},E} \to F_{\eta^{[n,\ell]}}$).

Let $\mathcal{E}$ be the Neron model of the elliptic curve E defined over $K\overline{\mathbb{F}_q}$. The multiplication by ℓ map $\times\ell : E \to E$ induces the multiplication by ℓ map over the Néron models $\times\ell : \mathcal{E} \to \mathcal{E}$. We denote by $\mathcal{E}[\ell]$ the kernel with respect to $\times\ell$ map.

Given any $f \in F_{\eta^{[n,\ell]}}$, denote by $\mathcal{A}_f$ the Néron model of the $(\ell-1)$ dimensional abelian variety A_f over $K\overline{\mathbb{F}_q}$. The degree ℓ isogeny $1-\sigma_{\ell,f} : A_f \to A_f$ extends to the endomorphism $1-\sigma_{\ell,f} : \mathcal{A}_f \to \mathcal{A}_f$.

Given any $f \in F_{\eta^{[n,\ell]}}$, we can write the factorization of f as $f = g_1 g_2^2 \cdots g_{\ell-1}^{\ell-1}$, where each polynomial g_i's are square-free polynomials over $\overline{\mathbb{F}_q}$ and $\deg g_k = \eta_k$ for $1 \le k \le \ell-1$. Consider the $2\ell-2$ open subsets of $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$ defined for each $1 \le k \le \ell-1$:

$$\begin{aligned} U_{g_k} &:= \mathbb{P}^1_{\overline{\mathbb{F}_q}} \setminus (g_k^{-1}(0) \cup \{0,\infty\}) \\ U_{g_k,E} &:= \mathbb{P}^1_{\overline{\mathbb{F}_q}} \setminus (g_k^{-1}(0) \cup \{0,\infty\} \cup \{v \in \mathbb{P}^1_{\overline{\mathbb{F}_q}} : v \mid \Delta_E\}). \end{aligned} \tag{3.10}$$

We also consider the corresponding inclusion maps $i_k : U_{g_k} \to \mathbb{P}^1_{\overline{\mathbb{F}_q}}$, $\tilde{i}_k : U_{g_k} \to \mathbb{P}^1_{\overline{\mathbb{F}_q}} \setminus \{0,\infty\}$, and $j_k : U_{g_k,E} \to \mathbb{P}^1_{\overline{\mathbb{F}_q}}$.

We denote by $L_\chi \to \mathbb{P}^1_{\overline{\mathbb{F}_q}} \setminus \{0,\infty\}$ the Kummer sheaf obtained from the order ℓ character $\chi : \pi_1^{\text{tame}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}} \setminus \{0,\infty\}) \to \mathbb{F}_\ell$ of the tame fundamental group of $\mathbb{P}^1_{\overline{\mathbb{F}_q}} \setminus \{0,\infty\}$. (Note that this is where we use the condition that $q \equiv 1 \bmod l$).

For each factor g_k of f, we inductively construct étale $\mathbb{F}_\ell$-lisse sheaves over $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$. For $k=1$, we denote by $\mathcal{F}^{[1]}_{n,\sigma_{\ell,f},E}$ the étale $\mathbb{F}_\ell$-lisse sheaf over $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$ defined as

$$\mathcal{F}^{[1]}_{n,\sigma_{\ell,f},E} := (j_1)_* \left(j_1^* \mathcal{E}[\ell] \otimes j_1^* (i_1)_* \tilde{i}_1^* L_\chi \right) \to \mathbb{P}^1_{\overline{\mathbb{F}_q}} \tag{3.11}$$

For $2 \le k \le \ell-1$, we iteratively define the étale $\mathbb{F}_\ell$-lisse sheaf over $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$ as

$$\mathcal{F}^{[k]}_{n,\sigma_{\ell,f},E} := (j_k)_* \left(j_k^* \mathcal{F}^{[k-1]}_{n,\sigma_{\ell,f},E} \otimes j_k^* (i_k)_* \tilde{i}_k^* L_{\chi^k} \right) \to \mathbb{P}^1_{\overline{\mathbb{F}_q}} \tag{3.12}$$

Let $\pi^{[1]} : \mathbb{P}^1_{\overline{\mathbb{F}_q}} \times_{\overline{\mathbb{F}_q}} F_{\eta^{[n,\ell]}} \to \mathbb{P}^1_{\overline{\mathbb{F}_q}}$ and $\pi^{[2]} : \mathbb{P}^1_{\overline{\mathbb{F}_q}} \times_{\overline{\mathbb{F}_q}} F_{\eta^{[n,\ell]}} \to F_{\eta^{[n,\ell]}}$ be the projection maps. Then the étale $\mathbb{F}_\ell$-lisse sheaf $\tau_{n,\sigma_{\ell,f},E}|_{F_{\eta^{[n,\ell]}}} \to F_{\eta^{[n,\ell]}}$ is defined to be the image of the higher direct images which forgets support:

$$R^1\pi^{[2]}_! \left((\pi^{[1]})^* \mathcal{F}^{[k]}_{n,\sigma_{\ell,f},E} \right) \to R^1\pi^{[2]}_* \left((\pi^{[1]})^* \mathcal{F}^{[k]}_{n,\sigma_{\ell,f},E} \right). \tag{3.13}$$

Remark 3.2.5. Given any $f \in F_{n,\ell}(\mathbb{F}_q)$, the geometric fiber of f is the étale cohomology group $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])$. Furthermore, there is an inclusion of étale cohomology groups

$$H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}]) \subset H^1_{\text{ét}}(K\overline{\mathbb{F}}_q, A_f[1-\sigma_{\ell,f}]) \cong H^1_{\text{ét}}(K\overline{\mathbb{F}}_q, E[\ell]). \tag{3.14}$$

The Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$ induces a symmetric pairing over $H^1_{\text{ét}}(K\overline{\mathbb{F}}_q, \mathcal{E}[\ell])$ via cup product and Poincaré duality. In particular, the symmetric pairing on $H^1_{\text{ét}}(K\overline{\mathbb{F}}_q, \mathcal{E}[\ell])$ descends to the symmetric pairing on $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])$, regardless of the choice of the polynomial $f \in F_{n,\ell}(\mathbb{F}_q)$.

The dimensions of the étale cohomology groups $H^i_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])$ can be computed as follows.

Lemma 3.2.6. *Given a weighted partition $\eta^{[n,\ell]} \in \Phi_{n,\ell}$, let $f \in F_{\eta^{[n,\ell]}}(\mathbb{F}_q)$. The étale cohomology groups of $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$ with coefficients in $\mathcal{A}_f[1-\sigma_{\ell,f}]$ satisfy*

$$\dim_{\mathbb{F}_\ell} H^i_{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}]) = \begin{cases} \deg(M_E) + 2\deg(A_E) - 2 + 2\sum_{i=1}^k \eta_k & \text{if } i = 1,\ \ell \nmid \deg(f) \\ \deg(M_E) + 2\deg(A_E) - 4 + 2\sum_{i=1}^k \eta_k & \text{if } i = 1,\ \ell \mid \deg(f) \\ 0 & \text{otherwise} \end{cases} \tag{3.15}$$

where M_E and A_E are divisors of multiplicative and additive reductions of the elliptic curve E/K.

Proof. The proof follows from adapting the arguments of N. Katz 1998, Section 5.1 and Hall 2008, Lemma 6.2. It suffices to compute the dimensions of cohomology groups

when $i = 0, 1, 2$. Because the function field K is of characteristic coprime to $6l$, and the Galois group $\mathrm{Gal}(K(E[\ell])/K)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, the group scheme $\mathcal{A}_f[1-\sigma_{\ell,f}]$ is lisse and irreducible of rank 2 over the open subscheme $U_{f,E}$ of $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$, where

$$U_{f,E} := \mathbb{P}^1_{\overline{\mathbb{F}_q}} \setminus (f^{-1}(0) \cup \{0, \infty\} \cup \{v \in \mathbb{P}^1_{\overline{\mathbb{F}_q}} : v \mid \Delta_E\}) \tag{3.16}$$

Because H^0 and H^2 are $\pi_1^{\text{ét}}(U_{f,E})$- invariants and $\pi_1^{\text{ét}}(U_{f,E})$-coinvariants of $A_f[1-\sigma_{\ell,f}]$, we obtain that both cohomology groups are equal to 0. Note that the same line of reasoning shows that $H^0_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{E}[\ell])$ and $H^0_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[\ell])$ are also trivial. Note that $(1-\sigma_{\ell,f})^{\ell-1} = \ell \circ \varphi$ for some $\varphi \in \mathrm{End}(A_f/K)$. Hence, the short exact sequence induced from multiplication by $1 - \sigma_{\ell,f}$

$$0 \to \mathcal{A}_f[1-\sigma_{\ell,f}] \to \mathcal{A}_f[\ell] \to \mathcal{A}_f[\ell] \to 0$$

induces a short exact sequence of étale cohomology groups

$$0 \to H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}]) \to H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[\ell]) \to H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[\ell]) \to 0.$$

. Hence, we obtain the isomorphism

$$H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}]) \cong H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[\ell])[1-\sigma_{\ell,f}].$$

On the other hand, the short exact sequence of group schemes

$$0 \to \mathcal{A}_f[\ell] \to (\mathrm{Res}_K^{K(\sqrt[\ell]{f})}\mathcal{E})[\ell] \to \mathcal{E}[\ell] \to 0 \tag{3.17}$$

implies that one obtains using Shapiro's lemma,

$$\dim_{\mathbb{F}_\ell} H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[\ell]) = \dim_{\mathbb{F}_\ell} H^1_{\text{ét}}(C_f, \mathcal{E}[\ell]) - \dim_{\mathbb{F}_\ell} H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{E}[\ell]), \tag{3.18}$$

where C_f is a smooth projective curve over $\overline{\mathbb{F}_q}$ with $K\overline{\mathbb{F}_q}(C_f) = K\overline{\mathbb{F}_q}(\sqrt[l]{f})$. We then use the Ogg-Shafarevich formula to the ℓ-primary part of the abelian variety A_f Ogg 1962,

Theorem 2 to obtain

$$\dim_{\mathbb{F}_\ell} H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[\ell]) = (\ell-1)\deg(M_E) + 2(\ell-1)\deg(A_E) + 4\text{genus}(C_f)$$

Using the Riemann-Hurwitz formula, depending on the difference of ramification behavior at the place ∞ when $\ell \mid \deg(f)$, we obtain that

$$\dim_{\mathbb{F}_\ell} H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[\ell]) = \begin{cases} (\ell-1)(\deg(M_E) + 2\deg(A_E) - 2 + 2\sum_{k=1}^{\ell-1}\eta_k) & \text{if } \ell \nmid \deg(f) \\ (\ell-1)(\deg(M_E) + 2\deg(A_E) - 4 + 2\sum_{k=1}^{\ell-1}\eta_k) & \text{if } \ell \mid \deg(f) \end{cases}$$

The lemma hence can be obtained from taking the $(1-\sigma_{\ell,f})$-torsion submodule of $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[\ell])$ with respect to coordinate-wise cyclic permutation action of $\sigma_{\ell,f}$. □

Using the Leray spectral sequence as in Park and N. Wang 2023, Lemma 3.9, we obtain that

$$H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])^{\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)} \cong H^1_{\text{ét}}(\mathbb{P}^1_{\mathbb{F}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]). \tag{3.19}$$

Because the $(\ell-1)$ dimensional abelian variety A_f is a subscheme of the Weil restriction of scalars of E, under Condition 3.1.1, Cesnavicius 2016, Proposition 5.4 implies

$$H^1_{\text{ét}}(\mathbb{P}^1_{\mathbb{F}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]) \cong \text{Sel}_{1-\sigma_{\ell,f}}(A_f/K). \tag{3.20}$$

Hence, the first moment of the size of $\text{Sel}_{1-\sigma_{\ell,f}}(A_f/K)$ over $f \in F_{n,\ell}(\mathbb{F}_q)$ is equivalent to counting $\mathbb{F}_q$-rational points of $\tau_{n,\sigma_{\ell,f},E}$, which can be obtained from utilizing the Grothendieck-Lefschetz trace formula:

$$\frac{\sum_{f\in F_{n,\ell}(\mathbb{F}_q)} \#\text{Sel}_{1-\sigma_{\ell,f}}(A_f/K)}{\#F_{n,\ell}(\mathbb{F}_q)} = \sum_{i=0}^{2n}(-1)^i q^{\frac{i}{2}-n}\text{TrFrob}_q | H^i_{\text{ét},c}(\tau_{n,\sigma_{\ell,f},E}, \mathbb{Q}_v). \tag{3.21}$$

Remark 3.2.7. The k-th moment of the size of $\text{Sel}_{1-\sigma_{\ell,f}}(A_f/K)$ over $f \in F_{n,\ell}(\mathbb{F}_q)$ can be computed from counting $\mathbb{F}_q$-rational points of the étale $\mathbb{F}_\ell$-lisse sheaf $\tau^{\oplus k}_{n,\sigma_{\ell,f},E} \to F_{\eta^{[n,\ell]}}$ where the geometric fiber at $f \in F_{\eta^{[n,\ell]}}(\mathbb{F}_q)$ is given by the direct sum $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])^{\oplus k}$.

The action of the étale fundamental group $\pi_1(F_{\eta^{[n,\ell]}}, f)$ is given by the coordinate-wise diagonal action of $\pi_1(F_{\eta^{[n,\ell]}}, f)$ acting on each of the component $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])$.

3.2.2 Big monodromy

We now demonstrate that the representable étale $\mathbb{F}_\ell$-lisse sheaf $\tau_{n,\sigma_{\ell,f},E} \to F_{n,\ell}$ satisfies the big monodromy result that the geometric and the arithmetic étale fundamental group contains index 2 subgroup of the orthogonal group of $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])$ with respect to the symmetric pairing induced from the Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$.

Theorem 3.2.8. *Given a weighted partition $\eta^{[n,\ell]} \in \Phi_{n,\ell}$, let $\tau_{n,\sigma_{\ell,f},E} \to F_{\eta^{[n,\ell]}}$ be the étale $\mathbb{F}_\ell$-lisse sheaf constructed from Definition 3.2.4.*

1. *Both the geometric monodromy group and the arithmetic monodromy group of $\tau_{n,\sigma_{\ell,f},E} \to F_{\eta^{[n,\ell]}}$ is isomorphic to a subgroup of the orthogonal group $O(H^1_{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])$ of index at most 2, but not isomorphic to $SO(H^1_{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{F}_q}}, \mathcal{A}_f[1-\sigma_{\ell,f}])$.*
2. *The trace of the Frobenius acting on $H^{2n}_{\acute{e}t,c}(\tau_{n,\sigma_{\ell,f},E}, \mathbb{Q}_v)$ is equal to $\ell+1$.*
3. *The trace of the Frobenius acting on $H^{2n}_{\acute{e}t,c}(\tau^{\oplus k}_{n,\sigma_{\ell,f},E}, \mathbb{Q}_v)$ is equal to $\prod_{m=1}^k(\ell^m+1)$.*

Proof. **Setup**

The first part of the theorem follows from adapting the big monodromy group results outlined in Hall 2008, Section 6 and N. Katz 1998, Theorem 4.1.10. Fix an integer m and a tuple of integers $(m_1, m_2, \cdots, m_{\ell-1})$ such that $m = \sum_{i=1}^{\ell-1} i m_i$. Denote by $\eta^{[n-m,\ell]}$ the partition obtained from $\eta^{[n,\ell]}$ which satisfies

$$\eta^{[n-m,\ell]} = [\eta_1 - m_1, \eta_2 - m_2, \cdots, \eta_k - m_k, \cdots, \eta_{\ell-1} - m_{\ell-1}].$$

We may choose an ℓ-th power free polynomial $g \in F_{\eta^{[n-m,\ell]}}$, and denote by U_g an open subscheme of $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$ excluding $g^{-1}(0)$ and $\{0,\infty\}$. Let g' be an ℓ-th power free polynomial $g' \in F_{m,\ell}$ such that $gg' \in F_{\eta^{[n,\ell]}}$. For shorthand notation, we denote by $\mathcal{A}_g$ the $\ell-1$ dimensional abelian variety over $K\overline{\mathbb{F}_q}$ defined as $\mathcal{A}_g := \text{Ker}\left(\text{Res}^{K\overline{\mathbb{F}_q}(\sqrt[\ell]{gg'})}_{K\overline{\mathbb{F}_q}} E \to E\right)$.

Given $c \in U_g$, fix a topological generator σ_c of the inertia subgroup $I(c)$ of the tame fundamental group $\pi_1^t((F_{\eta^{[n,\ell]}})_{\overline{\mathbb{F}}_q}, f)$. Then any choice of two topological generators σ_{c_1} and σ_{c_2} associated to $c_1, c_2 \in U_g$ such that $\mathcal{E} \to U_g$ has multiplicative reduction at c_1 and $\mathcal{A}_g \to U_g$ has additive reduction at c_2 that is not a place of bad reduction of $\mathcal{E}$ with $\dim_{\mathbb{F}_\ell} \mathcal{A}_g[1-\sigma_{\ell,g}]/\mathcal{A}_g[1-\sigma_{\ell,g}]^{I(c_i)} = 2$ are generators of the index 2 subgroup of the orthogonal group $O(H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]))$ which does not contain the special orthogonal group $SO(H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]))$. The choice of a place c_1 originates from one of the weaker requirements from Condition 3.1.1. Using the Chebotarev density theorem over K with respect to the Galois extension $K(E[\ell])/K$, such a choice of c_2 can always be made.

We first note that both the geometric and the arithmetic monodromy groups of $\tau_{n,\sigma_{\ell,f},E}$ is contained in the orthogonal group $O(H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}])$. In particular, the cup product and Poincarè duality show the existence of the symmetric pairing over $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}])$ and $H^1_{\text{ét}}(\mathbb{P}^1_{\mathbb{F}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}])$:

$$\begin{aligned} H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]) \times H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]) \to H^2_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mu_\ell) \cong \mathbb{F}_\ell \\ H^1_{\text{ét}}(\mathbb{P}^1_{\mathbb{F}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]) \times H^1_{\text{ét}}(\mathbb{P}^1_{\mathbb{F}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]) \to H^3_{\text{ét}}(\mathbb{P}^1_{\mathbb{F}_q}, \mu_\ell) \cong \mathbb{F}_\ell \end{aligned} \tag{3.22}$$

We note that the Galois-equivariance of the Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$ implies that the symmetric pairing is equivariant under the Frobenius action.

Consider an involution $\tau_c : \mathbb{P}^1_{\overline{\mathbb{F}}_q} \to \mathbb{P}^1_{\overline{\mathbb{F}}_q}$ defined as $t \mapsto c - t$. Given a choice of an order-ℓ character $\chi : I(c) \to \mathbb{F}_\ell$ of the inertia group $I(c)$, let $\mathcal{L}_\chi \to \mathbb{P}^1_{\overline{\mathbb{F}}_q} \setminus \{0, \infty\}$ be the Kummer sheaf associated to χ. Let $i : U_g \to \mathbb{P}^1_{\overline{\mathbb{F}}_q}$ be the inclusion map. Then the restriction of the étale sheaf $\tau_{n,\sigma_{\ell,f},E} \to F_{\eta^{[n,\ell]}}$ to U_g is an étale $\mathbb{F}_\ell$-lisse sheaf whose geometric fiber at $c \in \mathbb{P}^1_{\overline{\mathbb{F}}_q}$ is given by $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, i_* i^*(\mathcal{A}_g[1-\sigma_{\ell,g}] \otimes \tau_c^* \mathcal{L}_{\chi^m}))$. In particular, there exists an isomorphism of $\mathbb{F}_\ell$-lisse sheaves $\tau_{n,\sigma_{\ell,f},E} \cong MC_{\chi^m}(\mathcal{A}_g)$ over U_g, where MC_{χ^m} is the middle convolution functor with the choice of a character χ. We refer to Hall 2008, Section 4 and N. Katz 1998, Section 4 for further detailed description of the middle convolution functor.

From here and onwards, for each $c \in U_g$, we use the abbreviation $V_c := H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, i_* i^*(\mathcal{A}_g[1-\sigma_{\ell,g}] \otimes \tau_c^* \mathcal{L}_{\chi^m}))$ to denote the desired vector space.

Monodromy at a place of multiplicative reduction

Let c be a place of multiplicative reduction of $\mathcal{E} \to U_g$. Then $\mathcal{A}_g[1-\sigma_{\ell,g}]/\mathcal{A}_g[1-\sigma_{\ell,g}]^{I(c)}$, as $I(c)$-representation, is isomorphic to the trivial representation $\mathbb{F}_\ell$. To see this, we note that one obtains the following commutative diagram of group schemes,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{A}_g[1-\sigma_{\ell,g}]^{I(c)} & \longrightarrow & \mathcal{A}_g[\ell]^{I(c)} & \longrightarrow & \mathcal{M}_c & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{A}_g[1-\sigma_{\ell,g}] & \longrightarrow & \mathcal{A}_g[\ell] & \longrightarrow & \mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}] & \longrightarrow & 0 \end{array} \tag{3.23}$$

where $\mathcal{M}_c$ is kernel of the connecting morphism $\mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}]^{I(c)} \to H^1(I(c), \mathcal{A}_g[1-\sigma_{\ell,g}])$. By Snake lemma, we have the identification that

$$\mathcal{A}_g[1-\sigma_{\ell,g}]/\mathcal{A}_g[1-\sigma_{\ell,g}]^{I(c)} \cong \mathrm{Ker}\left((1-\sigma_{\ell,g}) : \mathcal{A}_g[\ell]/\mathcal{A}_g[\ell]^{I(c)} \to \mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}]/\mathcal{M}_c\right).$$

Using the identification that as $\mathrm{Gal}(\overline{K}/K\overline{\mathbb{F}_q})$-representations,

$$\mathrm{Res}^{K\overline{\mathbb{F}_q}(\sqrt[l]{gg'})}_{K\overline{\mathbb{F}_q}} E[\ell] \cong Ind^{\mathrm{Gal}(\overline{K}/K\overline{\mathbb{F}_q})}_{\mathrm{Gal}(\overline{K}/K\overline{\mathbb{F}_q}(\sqrt[l]{gg'}))} E[\ell], \tag{3.24}$$

it follows that the monodromy of $\mathcal{A}_g[\ell]$ at $t=c$ is an element of direct sums of $(\ell-1)$ trivial representations $\oplus_{i=1}^{\ell-1}\mathbb{F}_\ell$, with each of the summands indexed by elements $\sigma^i_{\ell,g}$ for $1 \le i \le \ell-1$. Without loss of generality, we can choose a multiplicative map sending $\sigma_{\ell,g} \mapsto \sigma^2_{\ell,g}$ which induces the action of $\sigma_{\ell,g}$ on $\oplus_{i=1}^{\ell-1}\mathbb{F}_\ell$ as a cyclic permutation of the coordinates. This implies that the representation $\mathcal{A}_g[1-\sigma_{\ell,g}]/\mathcal{A}_g[1-\sigma_{\ell,g}]^{I(c)}$ is isomorphic to $\mathbb{F}_\ell$.

We now verify that $V_c/V_c^{I(c)} \cong \mathbb{F}_\ell \otimes (-1)$. The identification that $\tau_{n,\sigma_{\ell,f},E} \to U_g$ is a middle convolution allows us to utilize N. Katz 1998, Theorem 4.1.10 to understand the action of $I(c)$ on the co-invariants $V_c/V_c^{I(c)}$. Because $\tau_{n,\sigma_{\ell,f},E} \to U_g$ is tamely ramified, we obtain as $I(c)$-representations,

$$V_c/V_c^{I(c)} \cong \mathrm{Ker}\left(1-\sigma_{\ell,g} : \mathcal{A}_g[\ell]/\mathcal{A}_g[\ell]^{I(c)} \otimes \chi^m \to \mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}]/M_c \otimes \chi^m\right)$$

for any $1 \leq m \leq \ell - 1$. The action of χ^m is given by multiplying each i-th component of the $\ell - 1$ dimensional representation by the character $\sigma_{\ell,g}^{im}$ for each $1 \leq i \leq \ell - 1$. Hence, we obtain that $\mathcal{A}_g[\ell]/\mathcal{A}_g[\ell]^{I(c)} \otimes \chi^m \cong \oplus_{i=1}^{l-1}(\mathbb{F}_\ell \otimes \sigma_{\ell,g}^{im}$. With respect to equivalent choice of the multiplicative map $\sigma_{\ell,g} \mapsto \sigma_{\ell,g}^2$, it follows that the representation $V_c/V_c^{I(c)}$ is isomorphic to $\mathbb{F}_\ell \otimes (\sigma_{\ell,g}^m + \sigma_{\ell,g}^{2m} + \cdots + \sigma_{\ell,g}^{(l-1)m}) \cong \mathbb{F}_\ell \otimes (-1)$. This proves that the topological generator σ_c of $I(c)$ acts as a reflection over V_c.

Monodromy at a place of additive reduction

Suppose that c is a place of additive reduction of $\mathcal{A}_g \to U_g$ such that c is not a place of bad reduction of $\mathcal{E} \to U_g$ and $\dim_{\mathbb{F}_\ell} \mathcal{A}_g[1-\sigma_{\ell,g}]/\mathcal{A}_g[1-\sigma_{\ell,g}]^{I(c)} = 2$. Then the monodromy of $\mathcal{A}_g[\ell]$ at $t = c$ is an element of $2(\ell-1)$ dimensional representation $\oplus_{i=1}^{\ell-1}(\mathbb{F}_\ell \otimes \sigma_{\ell,g}^i)$. Because c is a place of good reduction of E, one obtains the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{A}_g[1-\sigma_{\ell,g}]^{I(c)} & \longrightarrow & \mathcal{A}_g[\ell]^{I(c)} & \longrightarrow & \mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}]^{I(c)} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{A}_g[1-\sigma_{\ell,g}] & \longrightarrow & \mathcal{A}_g[\ell] & \longrightarrow & \mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}] & \longrightarrow & 0 \end{array} \tag{3.25}$$

By Snake lemma, we have the identification that

$$\mathcal{A}_g[1-\sigma_{\ell,g}]/\mathcal{A}_g[1-\sigma_{\ell,g}]^{I(c)} \cong \mathrm{Ker}\left((1-\sigma_{\ell,g}) : \mathcal{A}_g[\ell]/\mathcal{A}_g[\ell]^{I(c)} \to \mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}]/\mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}]^{I(c)}\right).$$

The monodromy of $\mathcal{A}_g[\ell]$ at $t = c$ is an element of a $2(\ell-1)$ dimensional representation $\oplus_{i=1}^{\ell-1}(\mathbb{F}_\ell \oplus \mathbb{F}_\ell) \otimes \sigma_{\ell,g}^i$. The identification that $\tau_{n,\sigma_{\ell,f},E} \to U_g$ is a middle convolution allows us to utilize N. Katz 1998, Theorem 4.1.10 to understand the action of $I(c)$ on the co-invariants $V_c/V_c^{I(c)}$. Because $\tau_{n,\sigma_{\ell,f},E} \to U_g$ is tamely ramified, we obtain as $I(c)$-representations,

$$V_c/V_c^{I(c)} \cong \mathrm{Ker}\left(1-\sigma_{\ell,g} : \mathcal{A}_g[\ell]/\mathcal{A}_g[\ell]^{I(c)} \otimes \chi^m \to \mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}]/\mathcal{A}_g[(1-\sigma_{\ell,g})^{\ell-2}]^{I(c)} \otimes \chi^m\right)$$

for any $1 \leq m \leq \ell - 1$. The action of χ^m is given by multiplying each i-th component of the $\ell - 1$ dimensional representation by the character $\sigma_{\ell,g}^{im}$ for each $1 \leq i \leq \ell - 1$.

Let σ_c be the topoolgical generator of $I(c) \subset \pi_1^t(U_g)$. To understand the representation

$V_c/V_c^{I(c)}$, we divide into 2 cases depending on whether $m = \ell - 1$ or $m \neq \ell - 1$. In the first case, we obtain that $\mathcal{A}_g[\ell]/\mathcal{A}_g[\ell]^{I(c)} \otimes \chi^{\ell-1} \cong \oplus_{i=1}^{\ell-1}(\mathbb{F}_\ell \oplus \mathbb{F}_\ell)$. Hence, we obtain $V_c/V_c^{I(c)} \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell$, implying that σ_c acts as an isotropic shear over V_c. In the second case, we obtain that $\mathcal{A}_g[\ell]/\mathcal{A}_g[\ell]^{I(c)} \otimes \chi^m \cong \oplus_{i=1}^{\ell-1}(\mathbb{F}_\ell \oplus \mathbb{F}_\ell) \otimes \sigma_{\ell,g}^{i(m+1)}$. Because $m \neq \ell - 1$, we obtain $V_c/V_c^{I(c)} \cong (\mathbb{F}_\ell \oplus \mathbb{F}_\ell) \otimes (\sigma_{\ell,g}^m + \cdots + \sigma_{\ell,g}^{m(\ell-1)}) \cong (\mathbb{F}_\ell \oplus \mathbb{F}_\ell) \otimes (-1)$. Assuming Condition 3.1.1, because the topological generator $\sigma_{c'}$ of $I(c')$ where $\mathcal{E} \to U_g$ has multiplicative reduction acts as a reflection over V_c, we obtain that the element $\sigma_c \sigma c' \in \pi_1^t(U_g)$ acts as an isotropic shear over V_c.

Big monodromy

By Hall 2008, Theorem 3.1, it follows that the geometric monodromy group of U_g contain an index 2 subgroup of the orthogonal group $O(H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1 - \sigma_{\ell,f}])$ which is not the special orthogonal group $SO(H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1 - \sigma_{\ell,f}])$.

Because the Weil pairing is $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-equivariant, the symmetric pairing is Frob_q -equivariant. Hence, the short exact sequence of étale fundamental groups

$$1 \to \pi_1((F_{n,\ell})_{\overline{\mathbb{F}}_q}, f) \to \pi_1((F_{n,\ell})_{\mathbb{F}_q}, f) \to \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to 1 \tag{3.26}$$

imply that both the geometric and the arithmetic fundamental groups of $F_{n,\ell}$ contain an index 2 subgroup of the orthogonal group $O(H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1-\sigma_{\ell,f}]))$ which is not the special orthogonal group $SO(H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, \mathcal{A}_f[1 - \sigma_{\ell,f}]))$.

Orbits

The second and the third part of the theorem reduces to counting the number of orbits of the geometric (or arithmetic) fundamental group of the space $F_{n,\ell}$ acting on the geometric fibers of $f \in F_{n,\ell}(\mathbb{F}_q)$ that is fixed by the action of the Frobenius Frob_q. Using Tony Feng, Landesman, and Rains 2023, Theorem 4.10 gives the desired results. □

We can now prove Theorem 3.1.2.

Theorem 3.1.2. The Grothendieck-Lefschetz trace formula implies for any $i \geq 0$ and $d \geq 1$,

$$\frac{\sum_{f \in F_{n,\ell}(\mathbb{F}_q)} \left(\#\mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K)\right)^d}{\#F_{n,\ell}(\mathbb{F}_q)} = \sum_{i=0}^{2n} (-1)^i \mathrm{TrFrob}_q | H^i_{\text{ét},c}(\tau^{\oplus d}_{n,\sigma_{\ell,f},E}, \mathbb{Q}_v) \tag{3.27}$$

We recall the identification

$$F_{n,\ell}(\mathbb{F}_q) = \sqcup_{\eta^{[n,\ell]} \in \Phi_{n,\ell}} F_{\eta^{[n,\ell]}}(\mathbb{F}_q). \tag{3.28}$$

and Theorem 3.2.8 that there exists a number $N_1 > 0$ and a fixed constant $B_1(n, \ell, E, d)$ independent of q such that for every $q > \tilde{N}_2$ and $d \geq 1$,

$$\left| \frac{\sum_{f \in F_{n,\ell}(\mathbb{F}_q)} \left(\#\mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K)\right)^d}{\#F_{n,\ell}(\mathbb{F}_q)} - \prod_{m=1}^{d} (\ell^m + 1) \right| < B_1(n, \ell, E, d) \cdot \frac{1}{\sqrt{q}}. \tag{3.29}$$

Using induction on the degree of ℓ-th power free polynomials, there exists a number $N_2 > 0$ and a fixed constant $\tilde{B}_1(n, \ell, E, d)$ independent of q such that for every $q > N_2$ and $d \geq 1$,

$$\left| \frac{\sum_{\substack{f \in \mathbb{F}_q[t] \\ \deg f = n}} (\#\mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K))^d}{\#\{f \in \mathbb{F}_q[t] \mid \deg f = n\}} - \prod_{m=1}^{d} (\ell^m + 1) \right| < \tilde{B}_1(n, \ell, E, d) \cdot \frac{1}{\sqrt{q}}. \tag{3.30}$$

We note that the Poonen-Rains distribution given by

$$BKLPR(\ell, r) := \prod_{j=0}^{\infty} \frac{1}{1 + \ell^{-j}} \cdot \prod_{j=1}^{r} \frac{\ell}{\ell^j - 1} \tag{3.31}$$

is the unique probability distribution whose k-th moments is equal to $\prod_{j=1}^{k}(\ell^j + 1)$, with the condition that the parity conjecture holds, in particular that the probability that the dimension of the $1 - \sigma_{\ell,f}$ Selmer group of A_f is odd is equal to the probability that the dimension of the $1 - \sigma_{\ell,f}$ Selmer group of A_f is even. By Billingsley 1995, Chapter 30 and Sawin and Matchett Wood 2022, Theorem 1.6, 1.7, 1.8, there exists a fixed constant

$C(\ell, E) > 0$ independent of n and q such that for sufficiently large n and q,

$$\left| \frac{\#\{f \in \mathbb{F}_q[t] \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K) = r,\ \deg f = n\}}{\#\{f \in \mathbb{F}_q[t] \mid \deg f = n\}} - \prod_{i=0}^{\infty} \frac{1}{1+\ell^{-i}} \prod_{i=1}^{r} \frac{\ell}{\ell^i - 1} \right| < C(\ell, E) \cdot \frac{1}{\sqrt{q}}. \tag{3.32}$$

□

3.3 Trivial cohomology groups

Recall that we consider the étale $\mathbb{F}_\ell$-lisse sheaf $\tau_{n,\sigma_{\ell,f},E} \to F_{\eta^{[n,\ell]}}$ whose $\mathbb{F}_q$-rational points parametrize $\mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K)$ for each $f \in F_{\eta^{[n,\ell]}}(\mathbb{F}_q)$. We also recall that the open subscheme $F_{\eta^{[n,\ell]}}$ of $\mathrm{Conf}_{\eta^{[n,\ell]}}(\mathbb{A}^1, X)$ has a canonical inclusion map

$$\begin{aligned} \mathrm{Conf}_{\eta^{[n,\ell]}}(\mathbb{A}^1, X) &\to \mathrm{Conf}_{\eta_1}(\mathbb{A}^1) \times \mathrm{Conf}_{\eta_2}(\mathbb{A}^1) \times \cdots \times \mathrm{Conf}_{\eta_{\ell-1}}(\mathbb{A}^1) \\ g_1 g_2^2 \cdots g_{\ell-1}^{\ell-1} &\mapsto (g_1, g_2, \cdots, g_{\ell-1}). \end{aligned} \tag{3.33}$$

For each i such that $1 \leq i \leq \ell-1$, there exists a natural stabilization map $\varphi_i : \mathrm{Conf}_{\eta_i}(\mathbb{A}^1) \to \mathrm{Conf}_{\eta_i+1}(\mathbb{A}^1)$. The stablization map induces the stabilization maps $\varphi_i : \mathrm{Conf}_{\eta^{[n,\ell]}}(\mathbb{A}^1, X) \to \mathrm{Conf}_{\eta_*^{[n+i,\ell]}}(\mathbb{A}^1, X)$ where $\eta_*^{[n+i,\ell]}$ is a weighted partition of $n+i$ into $\ell-1$ many components such that

$$\eta_*^{[n+i,\ell]} = [\eta_1, \eta_2, \cdots, \eta_{i-1}, \eta_i + 1, \eta_{i+1}, \cdots, \eta_{l-1}].$$

It is a nontrivial fact that the stablization maps $\varphi_i : \mathrm{Conf}_{\eta_i}(\mathbb{A}^1) \to \mathrm{Conf}_{\eta_i+1}(\mathbb{A}^1)$ and $\varphi_i : \mathrm{Conf}_{\eta^{[n,\ell]}}(\mathbb{A}^1, X) \to \mathrm{Conf}_{\eta_*^{[n+i,\ell]}}(\mathbb{A}^1, X)$ induces an isomorphism of étale cohomology groups of (colored) configuration spaces, see Palmer 2018 for the full proof of this result.

Using Theorem 3.1.2, we now prove Theorem 3.3.1, which demonstrates that certain geometric conditions on $\tau_{n,\sigma_{\ell,f},E}$ ensures the triviality of their étale cohomology groups.

Theorem 3.3.1. *Let v be a prime which is coprime to $2, 3, \ell$, and Char(K). Given a choice of a number k such that $1 \leq k \leq \ell - 1$, fix two weighted partitions $\eta^{[n,\ell]}, \eta_*^{[n+k,\ell]}$ and a stabilization map $\varphi_k : F_{\eta^{[n,\ell]}} \to F_{\eta_*^{[n+k,\ell]}}$. Suppose the following conditions hold for the étale cohomology groups of $\{\tau_{n,\sigma_{\ell,f},E}\}_{n\geq 1}$:*

1. (***Subexponential Betti Numbers***) *For every n and i, there exists a fixed constant $K > 0$ independent of n and i such that*

$$\dim_{\mathbb{Q}_v} H^i_{\acute{e}t}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v) \leq K^{i+\alpha}. \tag{3.34}$$

for some fixed number $\alpha \in \mathbb{R}$.

2. (***Homological Stability***) *For each fixed $i > 0$, there exists a number $N(i) > 1$ such that for every $n \geq N(i)$, the stabilization map $\varphi_i : F_{\eta^{[n,\ell]}} \to F_{\eta_*^{[n+i,\ell]}}$ induces an isomorphism of étale cohomology groups*

$$\varphi_i : H^i_{\acute{e}t}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}}_q}, \mathbb{Q}_v) \cong H^i_{\acute{e}t}((\tau_{n+1,\sigma_{\ell,f},E})_{\overline{\mathbb{F}}_q}, \mathbb{Q}_v) \tag{3.35}$$

3. (***Frobenius Eigenvalues***) *There exists a strictly increasing function $g : \mathbb{N} \to \mathbb{R}$ such that for all i, there exists a fixed constant $L > 1$ such that all the absolute values of the eigenvalues $\{\lambda_{i,m}\}_m$ of the Frobenius acting on $H^i_{\acute{e}t}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v)$ satisfy*

$$q^{\frac{i}{2}} \leq q^{g(i)} < |\lambda_{i,m}| < q^{g(i+1)} < q^{L\cdot\frac{i}{2}}. \tag{3.36}$$

Then for any fixed $i > 0$, there exists a large number $M(i) > 0$ such that for every $n > M(i)$,

$$H^i_{\acute{e}t}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}}_q}, \mathbb{Q}_v) = 0. \tag{3.37}$$

Proof. Using the Grothendieck-Lefschetz trace formula and Theorem 2.1.2 from Section 2, there exists an integer $N_1 > 0$ and a fixed constant $C(\ell, E)$ such that for any $n \geq N_1$,

$$\left|\mathbb{E}[\#\mathrm{Sel}_{1-\sigma_{\ell,f}}(A_f/K)] - (\ell+1)\right| = \frac{1}{q^n} \cdot \left|\sum_{i=0}^{2n-1} (-1)^i \mathrm{TrFrob}_q | H^i_{\text{ét},c}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v)\right| < C(\ell, E) \cdot \frac{1}{n^\alpha}$$

where v is any prime that is coprime to $2, 3, \ell$. Condition (1) of the statement of the theorem and Deligne bounds on eigenvalues of the Frobenius acting on étale cohomology groups with compact support Deligne 1974 imply that the above series converges for any

$q > K$. Using Poincaré duality and condition (3) of the statement of the theorem that the Frobenius eigenvalues associated to the action on i-th étale cohomology groups of $\tau_{n,\sigma_{\ell,f},E}$ form a strictly increasing function, we can construct a sequence of non-negative numbers $\{C_i\}_{i=0}^{2n-1}$ such that

$$\sum_{i=1}^{2n}(-1)^i \cdot C_i \cdot q^{-g(i)} \cdot \dim_{\mathbb{Q}_v} H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E}), \mathbb{Q}_v)^\vee < C(\ell, E) \cdot \frac{1}{n^{\alpha(\ell)}}. \tag{3.38}$$

where we recall that $g : \mathbb{N} \to \mathbb{R}$ is a strictly increasing function governing the absolute values of eigenvalues of the Frobenius action on i-th étale cohomology groups of $\tau_{n,\sigma_{\ell,f},E}$. Using the upper and lower bounds on Frobenius eigenvalues from condition (3) of the statement of the theorem, for every i such that $1 \leq i < \frac{2\alpha(\ell)}{L} \cdot \frac{\log n}{\log q}$, we obtain that the absolute values of the Frobenius eigenvalues acting on $H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E}), \mathbb{Q}_v)^\vee$ is strictly greater than $\frac{1}{n^{\alpha(\ell)}}$. Hence, we obtain that

$$\sum_{i=1}^{\lfloor \frac{2\alpha(\ell)}{L} \cdot \frac{\log n}{\log q} \rfloor} (-1)^i \cdot C_i \cdot q^{-g(i)} \dim_{\mathbb{Q}_v} H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E}), \mathbb{Q}_v) = 0. \tag{3.39}$$

Because g is a strictly increasing function, we obtain that either $C_i = 0$ or $\dim_{\mathbb{Q}_v} H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v) = 0$ for all such $1 \leq i < \frac{2\alpha(\ell)}{L} \cdot \frac{\log n}{\log q}$. Using condition (1) and (2) of the statement of the theorem, we may permit n to grow arbitrarily large so that for any fixed index i, there exists large enough n such that $i < \frac{2\alpha(\ell)}{L} \cdot \frac{\log n}{\log q}$.

We now demonstrate that $C_i = 0$ also implies that there exists a choice of $n > N(i)$ such that $\dim_{\mathbb{Q}_v} H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v) = 0$. The fact that $C_i = 0$ implies $\text{TrFrob}_{q^k} | H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v) = 0$ for all but finitely many $k \geq 0$. This is because one can always find large enough $n' > N(i)$ (which may be larger than the initial choice of n) such that $i < \frac{2\alpha(\ell)}{L} \cdot \frac{\log n'}{k \log q}$, and condition (2) of the statement of the theorem implies that the action of Frobenius on $H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v)$ is identical to the action of Frobenius on $H^i_{\text{ét}}((\tau_{n',\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v)$. Applying (3.39) to parameters q^k and n' yields

$$\text{TrFrob}_{q^k} H^i_{\text{ét}}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v) = \text{TrFrob}_{q^k} H^i_{\text{ét}}((\tau_{n',\sigma_{\ell,f},E})_{\overline{\mathbb{F}_q}}, \mathbb{Q}_v) = 0. \tag{3.40}$$

By Bombieri and N. M. Katz 2010, Theorem 3.3, it must be the case that for every $k \geq 1$,

$$\mathrm{TrFrob}_{q^k} \mid H^i_{\text{ét},c}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}}_q}, \mathbb{Q}_v) = 0. \tag{3.41}$$

In particular, it must be the case that the eigenvalues of the Frobenius Frob_q acting on i-th étale cohomology groups, denoted as $\{\lambda_{i,m}\}$, are given by

$$\lambda_{i,m} = q^{h(i)} \cdot \zeta^m_{M(i)} \tag{3.42}$$

for some primitive roots of unity $\zeta^m_{M(i)} \in \mu_{M(i)}$ of order M and some strictly increasing function $h : \mathbb{N} \to \mathbb{R}$. But this implies that the action of the Frobenius $\mathrm{Frob}_{q^{M(i)}}$ is given by multiplication by $(q^{(M(i))})^{h(i)}$. Hence, it follows that

$$\mathrm{TrFrob}_{q^{M(i)}} \mid H^i_{\text{ét},c}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}}_q}, \mathbb{Q}_v) = q^{h(i)\cdot M(i)} \cdot \dim_{\mathbb{Q}_v} H^i_{\text{ét},c}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}}_q}, \mathbb{Q}_v) = 0 \tag{3.43}$$

which implies the desired triviality of the i-th étale cohomology groups. □

Remark 3.3.2. The significance of Theorem 3.3.1 lies in the observation that one can obtain non-trivial geometric properties of algebraic spaces by utilizing innate properties of dynamical systems. It would be of great interest to explore whether the two conditions from Theorem 3.3.1 are valid. Even if the two conditions do not hold, Theorem 3.1.2 will construct an example of a sequence of algebraic spaces $\{\tau_{n,\sigma_{\ell,f},E}\}_{n\geq 1}$ whose étale cohomology groups do not satisfy homological stability, but whose alternating weighted sum of the trace of Frobenius acting on their i-th étale cohomology groups with compact support converges to 0 as n grows arbitrarily large. It is also of interest to understand whether one should expect the vanishing of étale cohomology groups of moduli spaces of Selmer groups of different families of abelian varieties to occur, the spaces of which are constructed in Hall 2008; Tony Feng, Landesman, and Rains 2023; Park and N. Wang 2023.

Remark 3.3.3. We note that one can reduce the problem of proving the homological

stability of étale cohomology groups of $\tau_{n,\sigma_{\ell,f},E}$ to proving the homological stability of group cohomology of a braid group with n strands over a punctured plane with twisted coefficients, the dimensions of which grow exponentially in n.

We first note that the colored configuration space $F_{n,\ell}$ can be regarded as an n-dimensional manifold over $\mathbb{C}$ which satisfies

$$H^i(F_{n,\ell}(\mathbb{C}), \mathbb{Z}/v\mathbb{Z}) \cong H^i_{\text{ét},c}((F_{n,\ell})_{\overline{\mathbb{F}}_q}, \mathbb{Z}/v\mathbb{Z}) \tag{3.44}$$

Recall that the symmetric pairing on the geometric fibers of $\tau_{n,\sigma_{\ell,f},E} \to F_{n,\ell}$ is the restriction of a fixed symmetric pairing over $H^1_{\text{ét}}(K\overline{\mathbb{F}}_q, E[\ell])$ induced from the Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$. The complex manifold $\tau_{n,\sigma_{\ell,f},E}(\mathbb{C})$ which satisfies

$$H^i(\tau_{n,\sigma_{\ell,f},E}(\mathbb{C}), \mathbb{Z}/v\mathbb{Z}) \cong H^i_{\text{ét},c}((\tau_{n,\sigma_{\ell,f},E})_{\overline{\mathbb{F}}_q}, \mathbb{Z}/v\mathbb{Z}) \tag{3.45}$$

can be constructed as a finite sheeted covering space over $F_{n,\ell}(\mathbb{C})$ using the following procedure. Fix an infinite dimensional $\mathbb{F}_\ell$-vector space V_∞ with a choice of a quadratic form $q : V_\infty \times V_\infty \to \mathbb{F}_\ell$. For each integer $n \in \mathbb{Z}$, pick a $\deg(M_E) + 2\deg(A_E) - 4 + 2n$-dimensional subspace V_n of V_∞ with the inclusion maps

$$V_1 \subset V_2 \subset V_3 \subset \cdots \subset V_n \subset \cdots \subset V_\infty. \tag{3.46}$$

Take the symmetric pairing on V_n's to be restrictions of the quadratic forms q to each correpsonding subspace of V_∞.

The complex manifold corresponding to $\tau_{n,\sigma_{\ell,f},E}$, denoted as $\tau_{n,\sigma_{\ell,f},E}(\mathbb{C})$ can be constructed from a sequence of orthogonal representations

$$\rho_n : \pi_1(F_{n,\ell}(\mathbb{C})) \to O(V_n) \subset \mathrm{GL}(V_n) \tag{3.47}$$

whose image contains an index 2 subgroup of $O(V_n)$ not isomorphic to the special orthogonal group $SO(V_n)$.

Let $\mathrm{Conf}_n(\mathbb{C} - \{P_1, \cdots, P_k\})$ be the configuration space of unordered n points over a complex plane with k punctures. Denote by $\mathcal{T}$ the twisted coefficient system over $\mathrm{Conf}_n(\mathbb{C}-\{P_1, \cdots, P_k\})$ associated to the covering map $F_{n,\ell}(\mathbb{C}) \to \mathrm{Conf}_n(\mathbb{C}-\{P_1, \cdots, P_k\})$ Palmer 2018, Section 2, Example 4.6. Here, the integer k is the number of distinct irreducible factors of Δ_E over $\overline{\mathbb{F}}_q$. Then the Leray-Serre spectral sequence implies that

$$\begin{aligned} H^*(\tau_{n,\sigma_{\ell,f},E}(\mathbb{C}), \mathbb{Z}/v\mathbb{Z}) &\cong H^*(F_{n,\ell}(\mathbb{C}), \mathbb{Z}/v\mathbb{Z}[V_n]) \\ &\cong H^*(\mathrm{Conf}_n(\mathbb{C} - \{P_1, \cdots, P_k\}), \mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Z}/v\mathbb{Z}[V_n]) \\ &\cong H^*(\pi_1(\mathrm{Conf}_n(\mathbb{C} - \{P_1, \cdots, P_k\})), \mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Z}/v\mathbb{Z}[V_n]) \end{aligned} \tag{3.48}$$

where the notation $\mathbb{Z}/v\mathbb{Z}[V_n]$ in the middle term indicates that the fundamental group $\pi_1(\tau_{n,\sigma_{\ell,f},E})$ acts as elements of the orthogonal group $O(V_n)$, and the notation $\mathbb{Z}/v\mathbb{Z}[V_n]$ indicates that the fundamental group $\pi_1(\mathrm{Conf}_n(\mathbb{C} - \{P_1, \cdots, P_k\}))$ acts as elements of the orthogonal group $O(V_n)$. This allows us to formulate the following naïve conjecture.

Conjecture 3.3.4. *Fix notations as stated in Remark 3.3.3. Then for each $i \geq 1$, there exists an integer $N(i) > 0$ such that for every $n \geq N(i)$,*

$$H^i(\pi_1(\mathrm{Conf}_n(\mathbb{C} - \{P_1, \cdots, P_k\})), \mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Z}/v\mathbb{Z}[V_n]) = 0. \tag{3.49}$$

Remark 3.3.5. The homological stability of group cohomology of braid groups with n strands with twisted coefficients whose dimension grows in accordance to a polynomial in n is carefully explored in a work by Martin Palmer Palmer 2018. As for homological stability of twisted coefficients whose dimension grows in accordance to an exponential function in n, the seminal work by Jordan Ellenberg, Akshay Venkatesh, and Craig Westerland studies the function field analogue of Cohen-Lenstra heuristics by utilizing homological stability of Hurwitz spaces Ellenberg, Venkatesh, and Westerland 2016. A recent work by Jordan Ellenberg, TriThang Tran, and Craig Westerland extends the previous work by proving homological stability of braid groups with twisted coefficients taken from braided vector spaces Ellenberg, TriThang Tran, and Westerland 2023. Another recent groundbreaking

work by Jordan Ellenberg and Aaron Landesman further extends homological stability results to sequences of moduli space of Selmer groups of universal families of hyperelliptic curves Ellenberg and Landesman 2023, the results of which will be of great interest for verifying the conditions of Theorem 3.3.1.

Chapter 4

Non-abelian twist families of elliptic curves

This chapter is based on the following work in progress Park 2024b, the work of which aims to generalize the random matrix model presented in Poonen and Rains 2012 to classes of non principally polarized abelian varieties over global fields. Some of the results presented in this chapter are closely related to the work by Stephanie Chan Chan 2022, the upcoming work by Peter Koymans and Alex Smith Koymans and Alex Smith 2024 and the work in progress with Daniel Keliher Keliher and Park 2024.

4.1 Main result

Fix a prime number ℓ. Let K be a global field whose characteristic is coprime to ℓ. Let L/K be a Galois extension with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ such that $m \mid (\ell - 1)$. We denote by M the Galois subextension of L/K such that $\mathrm{Gal}(M/K) \cong \mathbb{Z}/m\mathbb{Z}$.

Let E be an elliptic curve over K. The overarching question this chapter aims to address is:

Question 4.1.1. Compute the rank growths of the elliptic curve E over L/K:

$$\mathrm{Rank}_{\mathbb{Z}} E(L) - \mathrm{Rank}_{\mathbb{Z}} E(K) \tag{4.1}$$

As shown in previous chapters, there is a wealth of research conducted in the case when L/K is a cyclic Galois extension, i.e. $m = 1$. The case where $\ell = 2$ reduces to understanding the rank of K-rational points of the quadratic twist of E, the problem of which it has been verified for both number fields and global function fields that Goldfeld's conjecture - that approximately half of the quadratic twist families of elliptic curves have ranks 0 or 1, and is of density 0 - is valid assuming the BSD conjecture and some mild conditions on the elliptic curve E Alexander Smith 2022a; Alexander Smith 2022b; Ellenberg and Landesman 2023. The cases for odd primes ℓ can be understood from computing the "cyclic order-ℓ twist" of an elliptic curve E, an $\ell - 1$ dimensional abelian variety obtained from Weil restriction of scalars:

$$\mathrm{Ker}\left(Nm : \mathrm{Res}_K^L E \to E\right) \tag{4.2}$$

The generator σ_ℓ of the Galois group $\mathrm{Gal}(L/K)$ induces an isogeny over the abelian $\ell - 1$ fold, using which one can construct its prime Selmer group, a finite dimensional $\mathbb{F}_\ell$-vector subspace of the first Galois cohomology group $H^1(K, E[\ell])$ Mazur and Rubin 2007. Note that this first Galois cohomology group is invariant to the choice of the cyclic Galois extension L/K, which is obtained from proving that $1 - \sigma_\ell$ torsion subgroup of the abelian $\ell - 1$ fold is Galois-equivariantly isomorphic to ℓ-torsion subgroup of the elliptic curve Mazur and Rubin 2007, Proposition 4.1. The dimension of the prime Selmer group gives an upper bound on the differences of ranks of E as stated in Question 4.1.1 Mazur and Rubin 2007. Assuming a number of mild conditions on the elliptic curve E, the probability distribution of the dimensions of these prime Selmer groups are computed for both number fields (with respect to non-canonically ordered families of field extensions) Klagsbrun, Mazur, and Rubin 2013; Klagsbrun, Mazur, and Rubin 2014 and for global function fields Park 2022. Both of these results rest upon constructing a governing Markov operator over the state space of non-negative integers which govern the changes in dimensions of such prime Selmer groups with respect to consecutively changing local conditions at each place of K.

These probability distributions conform to the probability distribution obtained from a

random matrix model which governs the intersection of two maximal isotropic subspaces of an infinite dimensional $\mathbb{F}_\ell$ vector space, often known as the Poonen-Rains heuristics Poonen and Rains 2012. One of the crucial inputs for formulating the heuristics lies on the existence of the Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$ for ℓ-torsion subgroups of elliptic curves. As will be explored in this chapter, however, we may not expect the identical random matrix model to govern the statistics of prime Selmer groups of a family of abelian varieties, if the given family of abelian varieties of our interest are not equipped with the well-defined symplectic pairing on their torsion subgroups.

The overarching approach to understanding Question 4.1.1, for the case $m = 1$, is to construct a suitable abelian variety over K using Weil restriction of scalars, whose ranks of K-rational points encapsulates the rank growths of an elliptic curve over a Galois extension. Once one can verify that certain torsion subgroups of the desired abelian variety are Galois-equivariantly isomorphic to a fixed Galois module, it remains to construct a discrete stochastic process - whether it be a Markov operator over a countable state space or a random matrix model utilizing maximal isotropic subspaces - whose limiting behavior governs the probability distribution of dimensions of some Selmer groups of the desired families of abelian varieties.

The aim of this chapter focuses on generalizing this overarching philosophy to non-abelian Galois extensions L/K with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ for any $m \mid (\ell-1)$ assuming that the Galois subextension M/K with $\mathrm{Gal}(M/K) \cong \mathbb{Z}/m\mathbb{Z}$ is fixed. Denote by $\mathcal{L}_M(X)$ the set of such Galois extensions L/K with fixed Galois subfield M/K such that the discriminant of L is bounded above by X. The organization of the paper as well as the highlights can be summarized as follows.

- Section 4.2: We construct an $m(\ell-1)$ dimensional abelian variety $B_{L/K}$ governing rank growths of elliptic curves with respect to fields L/K specified in Question 4.1.1.

  Proposition (Proposition 4.2.4)**.** *Given an order ℓ element $\sigma_\ell \in Gal(L/K)$, there exists a $Gal(\overline{K}/K)$-equivariant isomorphism $B_{L/K}[1-\sigma_\ell] \cong (Res_K^M E)[\ell]$.*

- Section 4.3: We construct a random matrix model and a Markov operator governing

the distribution of $1-\sigma_\ell$ Selmer groups of $B_{L/K}$, serving as generalizations of previous works by Poonen-Rains Poonen and Rains 2012 and Klagsbrun-Mazur-Rubin Klagsbrun, Mazur, and Rubin 2014. Assuming some conditions on the local Kummer maps $\delta_v : \frac{B_{L/K}(K_v)}{(1-\sigma_\ell)B_{L/K}(K_v)} \to H^1(K_v, B_{L/K}[1-\sigma_\ell])$ and localization maps $\mathrm{loc}_v : H^1(K, B_{L/K}[1-\sigma_\ell]) \to H^1(K_v, B_{L/K}[1-\sigma_\ell])$, we are able to prove the following result on probability distribution of $1-\sigma_\ell$ Selmer groups of $B_{L/K}$.

Theorem (Theorem 4.3.12)**.** *Denote by $\mathbb{P}_{\mathcal{L}_M(X)}(d)$ the probability that the dimensions of $1-\sigma_\ell$ Selmer groups of families $\{B_{L/K}\}_{L\in\mathcal{L}_M(X)}$ is equal to d, i.e.*

$$\mathbb{P}_{\mathcal{L}_M(X)}(d) := \frac{\#\{L \in \mathcal{L}_M(X) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K) = d\}}{\#\mathcal{L}_M(X)}$$

Then assuming Condition 4.3.9, we obtain

$$\lim_{X\to\infty} \mathbb{P}_{\mathcal{L}_M(X)}(d) = \sum_{\substack{k_0,k_1,\cdots,k_{n-1}\in\mathbb{Z}_{\geq 0} \\ k_1+2k_2+\cdots+(n-1)k_{n-1}=d \\ k_0+k_1+\cdots+k_{n-1}=m}} \binom{k}{k_0,k_1,\cdots,k_{n-1}} \prod_{i=0}^{n-1} \left(\prod_{j\geq 0} \frac{1}{1+\ell^{-j}} \prod_{j=1}^{i} \frac{\ell}{\ell^j-1} \right)^{k_i}.$$

- Section 4.4: We analyze the ranks of $\mathbb{Q}$-rational points of cubic twist families of elliptic curves $E_n : y^2 = x^3 - 432n^2$, and understand how the dimensions of $1-\sigma_3$ Selmer groups of $B_{L/K}$ grow arbitrarily large as n grows arbitrarily large, thereby deviating from the proposed random matrix model from Section 4.3.

  Theorem (Statement (1) of Theorem 4.4.1)**.** *Given an integer n, denote by $w_2(n)$ the number of distinct odd prime factors of n equivalent to 2 modulo 3. Then* $\dim_{\mathbb{F}_3} \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) = 2w_2(n) + \Delta(n)$ *for some integer* $-1 \leq \Delta(n) \leq 3$.

- Section 4.5: We compute global root numbers of cubic twist families of elliptic curves $E_n : y^2 = x^3 - 432n^2$. We also formulate some conjectural statements on probability distribution of coranks of $(1-\sigma_3)^\infty$ Selmer groups of abelian 4-folds $B_{L/K}$ constructed from E_1 with respect to $L = \mathbb{Q}(\zeta_3, \sqrt[3]{n})$, and discuss how these statements are related to the conjecture on the probability that an integer is a sum of two rational cubes

Alpöge, Bhargava, and Shnidman 2022.

4.2 Abelian varieties governing rank growths

Fix a prime number ℓ. Given a global field K of characteristic coprime to ℓ, let L be a Galois extension over K with $\mathrm{Gal}(L/K) = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ such that $m \mid \ell - 1$. Let M/K be the unique subfield of L that is Galois over K and $\mathrm{Gal}(M/K) \cong \mathbb{Z}/m\mathbb{Z}$.

Definition 4.2.1. We denote by $\mathcal{L}_M$ the collection of $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ Galois extensions L/K with a fixed $\mathbb{Z}/m\mathbb{Z}$ Galois subextension M/K. Given any $X > 0$, we denote by $\mathcal{L}_M(X)$ the subcollection of fields $L \in \mathcal{L}_M$ whose absolute value of the discriminant is bounded above by X.

Definition 4.2.2. Denote by $B_{L/K}$ the $m(\ell-1)$ dimensional abelian variety given by

$$B_{L/K} := \mathrm{Ker}\left(\mathrm{Res}_K^L E \to \mathrm{Res}_K^M E\right) \tag{4.3}$$

We obtain that

$$\mathrm{Rank}_{\mathbb{Z}} E(L) = \mathrm{Rank}_{\mathbb{Z}} E(M) + \mathrm{Rank}_{\mathbb{Z}} B_{L/K}(K) \tag{4.4}$$

If one considers the family of $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ Galois extensions $\{L/K\}$ with a fixed degree m Galois extension M/K, then one obtains that

$$\mathrm{Rank}_{\mathbb{Z}} E(L) - \mathrm{Rank}_{\mathbb{Z}} E(M) = \mathrm{Rank}_{\mathbb{Z}} B_{L/K}(K) \tag{4.5}$$

In other words, assuming that one considers the family of Galois extensions $\mathcal{L}_M$, the rank growth of the elliptic curve E with respect to the field extension L/K is controlled by the rank of the abelian variety $B_{L/K}$.

Remark 4.2.3. The abelian variety $B_{L/K}$ is an isotypic component of direct sums of $\frac{\ell-1}{m}$ complex irreducible representations of dimension m of $\mathrm{Gal}(L/K)$ of the Weil restriction

$\mathrm{Res}_K^L E$, each irreducible representation of which originates from inducing direct sums of $\ell-1$ nontrivial 1-dimensional representations of $\mathrm{Gal}(L/M)$. This implies that the algebraic rank of $B_{L/K}$ is a multiple of m, i.e. $\mathrm{Rank}_{\mathbb{Z}} B_{L/K}(K) \equiv 0 \bmod m$. In the special case when $m = \ell - 1$, $B_{L/K}$ is an isotypic component corresponding to the $(\ell-1)$ dimensional irreducible representation of $\mathrm{Gal}(L/K)$, which implies that the algebraic rank of $B_{L/K}$ is a multiple of $\ell - 1$, i.e. $\mathrm{Rank}_{\mathbb{Z}} B_{L/K}(K) \equiv 0 \bmod \ell - 1$.

Pick a cyclic element $\sigma_\ell \in \mathrm{Gal}(L/K)$ of order ℓ. Because there exists a unique normal subgroup $\mathrm{Gal}(L/M)$ of order ℓ inside $\mathrm{Gal}(L/K)$, the element σ_ℓ is an endomorphism of $B_{L/K}$. Similar to Proposition 4.1 of Mazur and Rubin 2007, we have the following description of $1-\sigma_\ell$ torsion subgroup of $B_{L/K}$.

Proposition 4.2.4. *Let L/K be a Galois extension such that $Gal(L/K) = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ with M/K a unique subfield of L that is Galois over K and $Gal(M/K) \cong \mathbb{Z}/m\mathbb{Z}$. Then there exists a $Gal(\overline{K}/K)$-equivariant isomorphism*

$$B_{L/K}[1-\sigma_\ell] \cong (Res_K^M E)[\ell]$$

We note that when $m = 1$, we recover the statement of Proposition 4.1 of Mazur and Rubin 2007. In order to verify this proposition, we first present some definitions which could be of use to re-interpret Weil restriction of scalars of abelian varieties.

Definition 4.2.5. Fix a positive number $k \in \mathbb{N}$. Let $S(k)$ be the kernel of the map $\mathbb{Z}^k \to \mathbb{Z}$ which adds all the components of $\mathbb{Z}^k$:

$$\begin{aligned} 0 \to S(k) \to \mathbb{Z}^k &\to \mathbb{Z} \to 0 \\ (x_i)_{i=1}^k &\mapsto \sum_{i=1}^k x_i \end{aligned} \tag{4.6}$$

Note that $S(k)$ is an integral representation of the cyclic group $\mathbb{Z}/k\mathbb{Z}$ and the symmetric group S_k (In fact, $S(k)$ is the irreducible integral standard representation of S_k).

Definition 4.2.6. Fix an elliptic curve E over a global field K. Let L/K be a Galois extension with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ with $m \mid m-1$ for some prime number ℓ. As before, denote by M/K the unique Galois subextension of L such that $\mathrm{Gal}(L/M) \cong \mathbb{Z}/\ell\mathbb{Z}$. Denote by B_E the $m(\ell-1)$ dimensional abelian variety over K defined as

$$B_E := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell), E) \tag{4.7}$$

We note that B_E is a $\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}]$-module, and $\mathrm{End}_{\mathbb{Z}}(B_E) \supset \mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}]$.

Given a choice of a morphism

$$\psi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(L/K) \cong \mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \subset \mathrm{End}_{\mathbb{Z}}(B_E), \tag{4.8}$$

we denote by B_E^{ψ} the twist of B_E by ψ. Here, given any $\tau \in \mathrm{Gal}(\overline{K}/K)$, the element $\psi(\tau)$ acts on B_E by multiplying the elements of B_E to the left. In explicit terms, we may regard elements of B_E as integral $(\ell-1) \times m$ matrices, and the element $\psi(\tau)$, regarded as a $(\ell-1) \times (\ell-1)$ matrix, acts on the set of integral $(\ell-1) \times m$ matrices via matrix multiplication to the left.

Remark 4.2.7. An equivalent definition of B_E^{ψ} can be formulated as follows. We use the notations for field extensions $L/M/K$ as in Definition 4.2.6. The Weil restriction of an elliptic curve E/K with respect to M/K and L/K admits the following isotypic decomposition of irreducible $\mathbb{Q}$-representations of $\mathrm{Gal}(M/K) \cong \mathbb{Z}/m\mathbb{Z}$ and $\mathrm{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ Mazur and Rubin 2007, Chapter 3:

$$\mathrm{Res}_K^L E \cong \bigoplus_{\substack{\rho \\ \mathbb{Q}-\text{irred. rep. of } \mathrm{Gal}(L/K)}} \mathbb{Q}[\mathrm{Gal}(L/K)]_{\rho} \otimes E \tag{4.9}$$

Let $\rho*$ be the standard representation of S_p, which restricts to a $\mathbb{Z}/\ell\mathbb{Z}$ representation as a direct sum of all non-trivial integral irreducible representations of $\mathbb{Z}/\ell\mathbb{Z}$. Take ρ to be the induced representation $\mathrm{Ind}_{\mathbb{Z}/\ell\mathbb{Z}}^{\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}} \rho*$, which is the $m(\ell-1)$ dimensional representation of the group $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$. We note that there exists an isomorphism of $\mathbb{Q}$-representations

of $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$:

$$\rho \oplus \mathrm{Ind}_{\mathbb{Z}/\ell\mathbb{Z}}^{\mathbb{Z}/m\mathbb{Z}\rtimes\mathbb{Z}/\ell\mathbb{Z}} \mathbb{1} \cong \mathrm{Ind}_{e}^{\mathbb{Z}/m\mathbb{Z}\rtimes\mathbb{Z}/\ell\mathbb{Z}} \mathbb{1}. \tag{4.10}$$

The abelian variety B_E^{ψ} is the ρ-isotypic component of $\mathrm{Res}_K^L E$. In particular, given a choice of a morphism $\psi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(L/K)$, we obtain an isomorphism of Abelian varieties $B_E^{\psi} \cong B_{L/K}$ over K.

With notations stated as above, we prove Proposition 4.2.4.

Proof. Let $\sigma_\ell \in \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ be a choice of an order ℓ element, and $\tau_m \in \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ be an order m element. The integral matrix representation of σ_ℓ and $1 - \sigma_\ell$ acting on $\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell)$, as $(\ell-1) \times (\ell-1)$ matrices over $\mathbb{Z}$, are given by

$$\sigma_\ell = \begin{pmatrix} -1 & -1 & -1 & \cdots & -1 & -1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad 1 - \sigma_\ell = \begin{pmatrix} 2 & 1 & 1 & \cdots & 1 & 1 \\ -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 1 \end{pmatrix}, \tag{4.11}$$

where σ_ℓ and $1-\sigma_\ell$ acts on $\mathbb{Z}[\mathbb{Z}/m\mathbb{Z}\rtimes\mathbb{Z}/\ell\mathbb{Z}]\otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell)$ by matrix multiplication to the left. Likewise, the integral matrix representation of τ_m acting on $\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell)$, as an $m \times m$ matrix over $\mathbb{Z}$, is given by the cyclic column permutation matrix

$$\tau_m = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \tag{4.12}$$

where τ_m acts on $\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell)$ by matrix multiplication to the right.

Let $N_{(\ell-1)\times m}(\mathbb{Z}/\ell\mathbb{Z})$ be the $\mathbb{Z}/\ell\mathbb{Z}[\langle\tau_m\rangle]$-module defined as

$$N_{(\ell-1)\times m}(\mathbb{Z}/\ell\mathbb{Z}) := \left\{ \begin{pmatrix} a_1 & a_2 & \cdots & a_m \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \in M_{(\ell-1)\times m}(\mathbb{Z}/\ell\mathbb{Z}) \right\} \tag{4.13}$$

Then it follows that

$$\frac{\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell)}{(1-\sigma_\ell)\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell)} \cong N_{(\ell-1)\times m}(\mathbb{Z}/\ell\mathbb{Z}). \tag{4.14}$$

Fix a morphism $\psi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$. Let σ_ℓ and τ_m be choices of order ℓ and order m elements of $\mathrm{Gal}(L/K)$. Using the left exactness of the $\mathrm{Hom}_{\mathbb{Z}}(\cdot, E)$ functor, we obtain

$$B_E^{\psi}[1-\sigma_\ell] \cong \mathrm{Hom}_{\mathbb{Z}}\left(\frac{\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell)}{(1-\sigma_\ell)\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}] \otimes_{\mathbb{Z}[\mathbb{Z}/\ell\mathbb{Z}]} S(\ell)}, E \right)^{\psi} \tag{4.15}$$

where ψ acts on the desired $\mathbb{Z}[\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}]$ module by the matrix multiplication action specified for σ_ℓ and τ_m as outlined above. This implies that as $\mathrm{Gal}(\overline{K}/K)$-modules,

$$B_E^{\psi}[1-\sigma_\ell] \cong \mathrm{Hom}_{\mathbb{Z}}^{\psi}\left(N_{(\ell-1)\times m}(\mathbb{Z}/\ell\mathbb{Z}), E\right) \cong \mathrm{Hom}_{\mathbb{Z}}^{\langle\tau_m\rangle}\left(N_{(\ell-1)\times m}(\mathbb{Z}/\ell\mathbb{Z}), E\right) \cong \left(\prod_{i=1}^{m} E[\ell]\right)^{\langle\tau_m\rangle} \tag{4.16}$$

where the element τ_m acts on the Galois module $(\prod_{i=1}^{m} E[\ell])$ by cyclic permutation of the coordinates of the product. The prescribed Galois action identifies the module as an induced $\mathrm{Gal}(\overline{K}/M)$-module $E[\ell]$ to $\mathrm{Gal}(\overline{K}/K)$. In particular, we achieve

$$B_E^{\psi}[1-\sigma_\ell] \cong \mathrm{Ind}_{\mathrm{Gal}(\overline{K}/M)}^{\mathrm{Gal}(\overline{K}/K)} E[\ell] \cong (\mathrm{Res}_K^M E)[\ell]. \tag{4.17}$$

□

Remark 4.2.8. If L/K is a cyclic $\mathbb{Z}/\ell\mathbb{Z}$ extension, then we recover Mazur and Rubin 2007, Proposition 4.1:

$$B_{L/K}[1-\sigma_\ell] \cong (\mathrm{Res}_K^M E)[\ell] = E[\ell] \tag{4.18}$$

4.3 Random matrix model and Markov operators

We now define the $1-\sigma_\ell$ Selmer group of $m(\ell-1)$ dimensional abelian variety $B_{L/K}$ whose dimension, like nay other Selmer groups of abelian varieties, gives an upper bound on the rank of K-rational points of $B_{L/K}$.

Definition 4.3.1. Let L/K be a $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ Galosi extension. Fix an order ℓ element σ_ℓ of $\mathrm{Gal}(L/K)$. Consider the following short exact sequence of Galois cohomology groups

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{B_{L/K}(K)}{(1-\sigma_\ell)B_{L/K}(K)} & \longrightarrow & H^1(K, B_{L/K}[1-\sigma_\ell]) & \longrightarrow & H^1(K, B_{L/K})[1-\sigma_\ell] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \downarrow & & \\ 0 & \longrightarrow & \prod_v \frac{B_{L/K}(K_v)}{(1-\sigma_\ell)B_{L/K}(K_v)} & \xrightarrow{\prod_v \delta_v} & \prod_v H^1(K_v, B_{L/K}[1-\sigma_\ell]) & \longrightarrow & \prod_v H^1(K_v, B_{L/K})[1-\sigma_\ell] & \longrightarrow & 0 \end{array} \tag{4.19}$$

The $1-\sigma_\ell$ Selmer group of the abelian $m(\ell-1)$-fold $B_{L/K}$, denoted as $\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K)$, is a subspace of $H^1(K, B_{L/K}[1-\sigma_\ell])$ defined as

$$\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K) := \{c \in H^1(K, B_{L/K}[1-\sigma_\ell]),\ :\ \prod_v \mathrm{res}_v(c) \in \mathrm{im} \prod_v \delta_v\} \tag{4.20}$$

Proposition 4.2.4 implies that for any collections of $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ Galois extensions $\{L/K\}$ whose $\mathbb{Z}/m\mathbb{Z}$ Galois subextension M/K is fixed,

$$\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K) \subset H^1(K, B_{L/K}[1-\sigma_\ell]) \cong H^1(K, (\mathrm{Res}_K^M E)[\ell]) \cong H^1(M, E[\ell]) \tag{4.21}$$

where the last statement follows from Shapiro's lemma. A standard argument using Galois cohomology groups demonstrate that $\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K)$ is a finite dimensional $\mathbb{F}_\ell$-vector space.

The Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$ and the cup product induces a $\mathrm{Gal}(\overline{K}/M)$-equivariant

symmetric pairing on $H^1(K, (\mathrm{Res}_K^M E)[\ell])$:

$$H^1(K, (\mathrm{Res}_K^M E)[\ell]) \times H^1(K, (\mathrm{Res}_K^M E)[\ell]) \cong H^1(M, E[\ell]) \times H^1(M, E[\ell]) \to H^2(M, \mu_\ell) \cong \mathbb{F}_\ell. \tag{4.22}$$

However, it is not necessarily true that such a pairing $H^1(K, (\mathrm{Res}_K^M E)[\ell]) \times H^1(K, (\mathrm{Res}_K^M E)[\ell]) \to \mathbb{F}_\ell$ is $\mathrm{Gal}(\overline{K}/K)$-equivariant. There also does not exist an alteranting pairing on the torsion module $B_{L/K}[1-\sigma_\ell]$ whose image is in μ_ℓ, as every polarization of $B_{L/K}$ is divisible by ℓ^2 as shown in Howe 2001. To address this, we introduce the notion of coordinate-wise Lagrangian subspaces of a direct sum $V^{\oplus m}$ of a symmetric space (V, q) over any finite field $k = \mathbb{F}_\ell$.

Definition 4.3.2. Let $q : V \times V \to \mathbb{F}_\ell$ be a non-degenerate quadratic form on a finite dimensional $\mathbb{F}_\ell$- vector space V. For any $n \geq 1$, one obtains a non-degenerate quadratic form $q^{\oplus n} : V^{\oplus n} \times V^{\oplus n} \to \mathbb{F}_\ell^{\oplus n}$. For each $1 \leq i \leq n$, denote by $\pi_i : V^{\oplus n} \to V$ the projection morphism to the i-th coordinate. We say that a subspace $W \subset V^{\oplus n}$ is coordinate-wise Lagrangian if the following two conditions hold for every $1 \leq i \leq n$.

1. The subspace $\pi_i(W) \subset V$ is a maximal isotropic subspace of V with respect to the quadratic form q.

2. The quadratic form q over V is trivial over $\pi_i(W)$.

Using the definition above, we can formulate a generalization of the Poonen-Rains heuristics Poonen and Rains 2012 to non-principally polarized Abelian varieties, where prime Selmer groups of abelian varieties can be identified as an intersection of two maximal isotropic subspaces lying inside an infinite dimensional $\mathbb{F}_\ell$-vector space.

Proposition 4.3.3. *Consider the following diagram*

$$\begin{array}{ccc} & & H^1(K, (Res_K^M E)[\ell]) \\ & & \downarrow \\ \prod_v \frac{B_{L/K}(K_v)}{(1-\sigma_\ell)B_{L/K}(K_v)} & \longrightarrow & \prod_v H^1(K_v, (Res_K^M E)[\ell]) \end{array} \tag{4.23}$$

1. *For each place v of K that admits prime factorization over M as*

$$(v) = \mathfrak{p}_1^e \mathfrak{p}_2^e \cdots \mathfrak{p}_k^e, \tag{4.24}$$

there exists a quadratic form

$$q_v : H^1(K_v, (Res_K^M E)[\ell]) \times H^1(K_v, (Res_K^M E)[\ell]) \to \mathbb{F}_\ell^{\oplus k} \tag{4.25}$$

such that the images of the v-components of horizontal and vertical maps

$$\begin{aligned} loc_v &: H^1(K, (Res_K^M E)[\ell]) \to H^1(K_v, (Res_K^M E)[\ell]) \\ \delta_v &: \frac{B_{L/K}(K_v)}{(1-\sigma_\ell)B_{L/K}(K_v)} \to H^1(K_v, (Res_K^M E)[\ell]) \end{aligned} \tag{4.26}$$

are coordinate-wise Lagrangian subspaces with respect to q_v.

2. *The intersection of the images of the horizontal and vertical maps are isomorphic to the Selmer group* $\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K)$.

Proof. Let v be a place of K that factorizes over M as

$$(v) = \mathfrak{p}_1^e \mathfrak{p}_2^e \cdots \mathfrak{p}_k^e. \tag{4.27}$$

We may identify the localization of M by (v) as

$$M_v \cong \prod_{i=1}^{k} M_{\mathfrak{p}_i}. \tag{4.28}$$

where $M_{\mathfrak{p}_i}$ is a $\mathbb{Z}/\frac{m}{k}\mathbb{Z}$ extension of K_v. Let $M_{m/k}$ be the unramified $\mathbb{Z}/\frac{m}{k}\mathbb{Z}$ Galois extension of K_v. If $e = 1$, i.e. (v) is unramified with respect to M/K, then for every $1 \leq i \leq k$, one has $M_{\mathfrak{p}_i} = M_{m/k}$. If $e \neq 1$, then each $M_{\mathfrak{p}_i}$ is a ramified $\mathbb{Z}/\frac{m}{k}\mathbb{Z}$ Galois extension of K_v. By Shapiro's lemma,

$$H^1(K_v, (\mathrm{Res}_K^M E)[\ell]) \cong H^1(M_{\mathfrak{p}_i}, E[\ell]^{\oplus k}) \tag{4.29}$$

The Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$ induces a symmetric pairing $q_{\mathfrak{p}_i}$ for each i

$$q_{\mathfrak{p}_i} : H^1(M_{\mathfrak{p}_i}, E[\ell]) \times H^1(M_{\mathfrak{p}_i}, E[\ell]) \to \mu_\ell \tag{4.30}$$

which induces a coordinate-wise symmetric pairing on

$$q_v := \oplus_{i=1}^k q_{\mathfrak{p}_i} : H^1(K_v, (\mathrm{Res}_K^M E)[\ell]) \times H^1(K_v, (\mathrm{Res}_K^M E)[\ell]) \to \mu_\ell^{\oplus k}. \tag{4.31}$$

Then it follows from Mazur and Rubin 2007, Section 4 and Poonen and Rains 2012, Section 4 that both images of the morphisms loc_v and δ_v are coordinate-wise Lagrangian subspaces of $H^1(K_v, (\mathrm{Res}_K^M E)[\ell])$. That is, each coordinate is a maximal isotropic subspace V of $H^1(M_{m/k}, E[\ell])$ such that $q_v|V = 0$, thus proving statement (1). Statement (2) follows immediately from the definition of $\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K)$ and Proposition 4.2.4, which implies for any desired Galois extension L/K,

$$H^1(K, B_{L/K}[1 - \sigma_\ell]) \cong H^1(K, (\mathrm{Res}_K^M E)[\ell]). \tag{4.32}$$

□

Remark 4.3.4. Let v be a place of K that factorizes over M as $(v) = \mathfrak{p}_1^e \mathfrak{p}_2^e \cdots \mathfrak{p}_k^e$. Suppose that the elliptic curve E/K has good reduction over v.

The unramified coordinate-wise Lagrangian subspace of $H^1(K_v, (\mathrm{Res}_K^M E)[\ell])$ is the direct sum of unramified Galois cohomology group of $H^1(M_{\mathfrak{p}_i}, E[\ell])$, i.e.

$$H^1_{ur}(K_v, (\mathrm{Res}_K^M E)[\ell]) = \oplus_{i=1}^k H^1_{ur}(M_{\mathfrak{p}_i}, E[\ell]) \tag{4.33}$$

If v is a place that is unramified with respect to the field extension L/K, then one achieves that the image of the local Kummer map δ_v is the unramified cohomology group $H^1_{ur}(K_v, (\mathrm{Res}_K^M E)[\ell])$.

We say that a coordinate-wise Lagrangian subspace is ramified if it is not the unramified coordinate-wise Lagrangian subspace $H^1_{ur}(K_v, (\mathrm{Res}_K^M E)[\ell])$. Denote by $\mathcal{H}_{ram}(K_v, E, M, k)$

the set of ramified coordinate-wise Lagrangian subspaces of $H^1(K_v, (\mathrm{Res}_K^M E)[\ell])$. The proof of Proposition 4.3.3 and Klagsbrun, Mazur, and Rubin 2014, Lemma 5.5 demonstrate that the number of coordinate-wise Lagrangian subspaces of $H^1(K_v, (\mathrm{Res}_K^M E)[\ell])$ is:

$$\#\mathcal{H}_{ram}(K_v, E, M, k) = \lceil \ell^{\sum_{i=1}^{k} (\dim_{\mathbb{F}_\ell} E[\ell](M_{\mathfrak{p}_i})-1)} \rceil. \tag{4.34}$$

If v is a place that is unramified with respect to the field extension M/K, then the above equation simplifies to

$$\#\mathcal{H}_{ram}(K_v, E, M, k) = \lceil \ell^{k(\dim_{\mathbb{F}_\ell} E[\ell](M_{m/k})-1)} \rceil \tag{4.35}$$

As before, we pay particular focus to the family of abelian varieties $\{B_{L/K}\}_L$ parametrized by families of $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ Galois extensions L/K with a fixed $\mathbb{Z}/m\mathbb{Z}$ extension M/K. Because every polarization of such abelian varieties $B_{L/K}$ has degree divisible by ℓ^2 Howe 2001, it is not possible to directly utilize the Poonen-Rains heuristics Poonen and Rains 2012, where the random matrix model is obtained from identifying the probability distribution of the dimensions of intersection of two random maximal isotropic subspaces of a symmetric space (V, q) with respect to the symmetric pairing $q : V \times V \to \mathbb{F}_\ell$. Proposition 4.3.3, nevertheless, shows that the arithmetic statistics of $\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K)$ can still be understood from computing the probability distribution of desired dimensions with respect to coordinate-wise symmetric pairing $\oplus_{i=1}^m q : V^{\oplus m} \times V^{\oplus m} \to \mathbb{F}_\ell^{\oplus m}$.

Definition 4.3.5. Let V be a vector space over a finite field $\mathbb{F}_\ell$ equipped with a symmetric pairing $q : V \times V \to \mathbb{F}_\ell$. We denote by $b_{d,k,n}$ the probability

$$b_{d,k,n} := \mathbb{P}[\dim_{\mathbb{F}_\ell}(W \cap Z) = d \mid {\scriptstyle W,Z \subset V^{\oplus k} \text{coordinate-wise Lagrangian w.r.t. } q^{\oplus k}: V^{\oplus k} \times V^{\oplus k} \to \mathbb{F}_\ell^{\oplus k}}^{\dim_{\mathbb{F}_\ell} W = \dim_{\mathbb{F}_\ell} Z = n}] \tag{4.36}$$

We denote by $Y_{k,n}$ the random variable denoting the dimension of intersection of two coordinate-wise Lagrangian subspaces $W, Z \subset V^{\oplus k}$ with respect to coordinate-wise quadratic form $q^{\oplus k} : V^{\oplus k} \times V^{\oplus k} \to \mathbb{F}_\ell^{\oplus k}$, where one of the subspaces Z is fixed and

the other subspace W is chosen uniformly at random.

The probabilities $b_{d,k,n}$ can be explicitly computed as shown in the proposition stated below.

Proposition 4.3.6. *1. The random variable $Y_{k,n}$ is a sum of k copies of Bernoulli random variables $B_1, B_2, \cdots, B_n$ where B_i is equal to 1 with probability $\frac{1}{\ell^{i-1}+1}$ and 0 otherwise.*

2. For any n,

$$\sum_{d\geq 0} b_{d,k,n} z^d = \prod_{i=0}^{n-1} \left(\frac{z+\ell^i}{1+\ell^i}\right)^k \tag{4.37}$$

3. Denote by $b_{d,k} := \lim_{n\to\infty} b_{d,k,n}$. Then

$$\sum_{d\geq 0} b_{d,k} z^d = \prod_{i=0}^{\infty} \left(\frac{1+\ell^{-i}z}{1+\ell^{-i}}\right)^k \tag{4.38}$$

4. We have

$$b_{d,k} = \sum_{\substack{k_0,k_1,\cdots,k_{n-1}\in\mathbb{Z}_{\geq 0} \\ k_1+2k_2+\cdots+(n-1)k_{n-1}=d \\ k_0+k_1+\cdots+k_{n-1}=k}} \binom{k}{k_0, k_1, \cdots, k_{n-1}} \prod_{i=0}^{n-1} \pi_i^{k_i} \tag{4.39}$$

where

$$\pi_i := \prod_{j\geq 0} \frac{1}{1+\ell^{-j}} \prod_{j=1}^{i} \frac{\ell}{\ell^j - 1} \tag{4.40}$$

Proof. Part (1) of the proposition follows from adapting the proof of Poonen and Rains 2012, Proposition 2.6 to the random variable $Y_{k,n}$, where the original proposition verifies the desired statement for the case when $k = 1$. The rest of the parts follows from comparing the generating function of the sums of Bernoulli random variable with $Y_{k,n}$. □

Combining Proposition 4.2.4 and Proposition 4.3.6, we can formulate the following heuristic on the dimensions of $1 - \sigma_\ell$ Selmer groups of twist families $\{B_{L/K}\}_L$ assuming some strong conditions on the distribution of images of local Kummer maps δ_v.

Definition 4.3.7. We introduce a number of subfamilies of the families of Galois extensions $\mathcal{L}_M$.

1. Pick a place v of K. We denote by $\mathcal{L}_{M,v} \subset \mathcal{L}_M$ a subcollection of Galois extensions $L \in \mathcal{L}_M$ such that v is ramified in L/K. We denote by $\mathcal{L}_{M,v}(X)$ a subcollection of Galois extensions $L \in \mathcal{L}_{M,v}$ whose absolute value of the discriminant is bounded above by X.

2. Given any integer k which divides $m = [M : K]$, we denote by $\mathcal{L}_M^{[k]} \subset \mathcal{L}_M$ the subcollection of Galois extensions $L \in \mathcal{L}_M$ which are unramified away from places v of K which is unramified over M/K and admits prime decomposition over M as $(v) = \prod_{i=1}^{k} \mathfrak{p}_i$. We denote by $\mathcal{L}_M^{[k]}(X)$ a subcollection of Galois extensions $L \in \mathcal{L}_M^{[k]}$ whose absolute value of the discriminant is bounded above by X.

3. Given any integer $l > 0$, we denote by $\mathcal{L}_{M,[l]} \subset \mathcal{L}_M$ the subcollection of Galois extensions $L \in \mathcal{L}_M$ such that $\dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K) = l$. (Here, we note that l is not necessarily equal to ℓ).

Definition 4.3.8. 1. Given a choice of a place v of K, we define the projection map $\Phi_v : \mathcal{L}_{M,v} \to \mathcal{H}_{ram}(K_v, E, M, k)$ as

$$\begin{aligned} \Phi_v : \mathcal{L}_{M,v} &\to \mathcal{H}_{ram}(K_v, E, M, k) \\ L &\mapsto \delta_v \left(\frac{B_{L/K}(K_v)}{(1-\sigma_\ell) B_{L/K}(K_v)} \right) \end{aligned} \tag{4.41}$$

where δ_v is the local Kummer map of the abelian variety $B_{L/K}$.

2. Given a choice of a place $\mathfrak{p}$ of M lying above a place v of K, denote by $w(\mathfrak{p})$ the dimension of $E[\ell](M_\mathfrak{p})$ for each prime $\mathfrak{p}$ lying above v. We define the projection map $\Psi_\mathfrak{p} : \mathcal{L}_{M,[l]} \to \mathrm{Hom}(\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K), H^1_{ur}(M_\mathfrak{p}, E[\ell]) \cong M_{\ell \times \mathfrak{v}}(\mathbb{F}_\ell)$ as

$$\begin{aligned} \Psi_\mathfrak{p} : \mathcal{L}_{M,[l]} &\to \mathrm{Hom}(\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K), H^1_{ur}(K, (\mathrm{Res}^M_K E)[\ell]) \cong M_{\ell \times w(\mathfrak{p})}(\mathbb{F}_\ell) \\ L &\mapsto \mathrm{loc}_\mathfrak{p}. \end{aligned} \tag{4.42}$$

Condition 4.3.9. 1. Given a choice of a place v of K, we endow a uniform probability distribution $\nu_{\mathcal{L}_{M,v}(X)}$ over the finite collection of Galois extensions $\mathcal{L}_{M,v}(X)$. Then the pushforward measure $\Phi_v^*\nu_{\mathcal{L}_{M,v}(X)}$ converges to a uniform distribution over $\mathcal{H}_{ram}(K_v, E, M, k)$ as X grows arbitrarily large. In other words, given any ramified coordinate-wise Lagrangian subspace $V \in \mathcal{H}_{ram}(K_v, E, M, k)$,

$$\lim_{X\to\infty} \mathbb{P}\left[\Phi_v(L) = V \mid L \in \mathcal{L}_{M,v}(X)\right] = \frac{1}{\#\mathcal{H}_{ram}(K_v, E, M, k)}. \tag{4.43}$$

2. Given a choice of a place $\mathfrak{p}$ lying above v of K, we endow a uniform probability distribution $\nu_{\mathcal{L}_{M,[l]}(X)}$ over the finite collection of Galois extensions $\mathcal{L}_{M,[l]}(X)$. Then the pushforward measure $\Psi_{\mathfrak{p}}^*\nu_{\mathcal{L}_{M,[l]}(X)}$ converges to a uniform distribution over $\mathcal{M}_{\ell\times w(\mathfrak{p})}(\mathbb{F}_\ell)$ as X grows arbitrarily large. In other words, given any matrix $M \in M_{\ell\times w(\mathfrak{p})}(\mathbb{F}_\ell)$,

$$\lim_{X\to\infty} \mathbb{P}\left[\Psi_{\mathfrak{p}}(L) = M \mid L \in \mathcal{L}_{M,[l]}(X)\right] = \frac{1}{\#M_{\ell\times w(\mathfrak{p})}(\mathbb{F}_\ell)}. \tag{4.44}$$

Theorem 4.3.10. *Assume Condition 4.3.9.*

1. *For any $k \mid m$, the probability distribution of dimensions of $1-\sigma_\ell$ Selmer groups of families $\{B_{L/K}\}_{L\in\mathcal{L}_M^{[k]}}$ is given by*

$$\lim_{X\to\infty} \frac{\#\{L \in \mathcal{L}_M^{[k]}(X) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K) = d\}}{\#L_M^{[k]}(X)} = b_{d,k}. \tag{4.45}$$

2. *There exists an irreducible aperiodic Markov chain $\mathcal{M}_k$ over the state space $\mathbb{Z}_{\geq 0}^k$ with the unique stationary distribution $\hat{\pi}_k : \mathbb{Z}_{\geq 0}^k \to [0,1]$ such that*

$$b_{d,k} = \sum_{d_1+d_2+\cdots+d_k=d} \hat{\pi}_k(d_1, d_2, \cdots, d_k). \tag{4.46}$$

Proof. Proposition 4.2.4 shows that regardless of the choice of $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/\ell\mathbb{Z}$ Galois

extensions L/K with a fixed $\mathbb{Z}/m\mathbb{Z}$ Galois extension M/K, the image of the morphism

$$\prod_v \mathrm{loc}_v : H^1(K, B_{L/K}[1-\sigma_\ell]) \cong H^1(K, (\mathrm{Res}_K^M E)[\ell]) \to \prod_v H^1(K_v, (\mathrm{Res}_K^M)[\ell]) \tag{4.47}$$

is a fixed coordinate-wise Lagrangian subspace of $\prod_v H^1(K_v, (\mathrm{Res}_K^M)[\ell])$. Proposition 4.3.3 hence demonstrates that the dimension of $1-\sigma_\ell$ Selmer group of $B_{L/K}$ is determined by the image of the local Kummer map δ_v of the abelian variety $B_{L/K}$. Fix an integer $k \mid m$. Restricting the families of abelian varieties to Galois extensions $L \in \mathcal{L}_M^{[k]}$, Condition 4.3.9 implies that the random variable $\lim_{n\to\infty} Y_{k,n}$ governs the probability distribution of the dimension of the intersection of $\prod_v \mathrm{im}(\delta_v)$ and $\prod_v \mathrm{im}(\mathrm{loc}_v)$. This proves statement (1) of the theorem.

To prove statement (2) of the theorem, consider the Markov operator $\mathcal{M}_{\ell,L} := [m_{i,j}^{[\ell]}]$ defined over the countable state space $\mathbb{Z}_{\geq 0}$:

$$m_{i,j}^{[\ell]} = \begin{cases} 1-\ell^{-i} & \text{if } j = i-1 \geq 0 \\ \ell^{-i} & \text{if } j = i+1 \\ 0 & \text{else} \end{cases}$$

Using $\mathcal{M}_{\ell,L}$, we construct the Markov chain $\mathcal{M}_\ell$ defined over the countable state space $\mathbb{Z}_{\geq 0}$.

$$\mathcal{M}_\ell := \left(1 - \frac{\ell}{\ell^2-1}\right) + \frac{1}{\ell}\mathcal{M}_{\ell,L} + \frac{1}{\ell^3-\ell}\mathcal{M}_{\ell,L}^2. \tag{4.48}$$

The construction of the Markov chain originates from computing the respective probability that the maximal isotropic subspaces originating from the two images

$$\begin{aligned} \mathrm{loc}_{\mathfrak{p}} &: H^1(K, (\mathrm{Res}_K^M E)[\ell]) \to H^1(M_{\mathfrak{p}}, E[\ell]) \\ \delta_{\mathfrak{p}} &: \frac{B_{L/K}(K_v)}{B_{L/K}[1-\sigma_\ell]} \to H^1(K_v, (\mathrm{Res}_K^M E)[\ell]) \to H^1(M_{\mathfrak{p}}, E[\ell]) \end{aligned}$$

at each place $\mathfrak{p}$ of M lying above a place v of K agree with each other, as outlined in Klagsbrun, Mazur, and Rubin 2014, Section 7, 9. The Markov chain can be constructed by

considering three cases where $\dim_{\mathbb{F}_\ell} E[\ell](M_\mathfrak{p}) = i$ for $0 \leq i \leq 2$. When $\dim_{\mathbb{F}_\ell} E[\ell](M_\mathfrak{p}) = 0$, then it follows that $H^1(M_\mathfrak{p}, E[\ell]) = 0$, implying that twisting the abelian $m(\ell-1)$ fold by such a place $\mathfrak{p}$ lying above v does not alter the dimension of $1-\sigma_\ell$ Selmer groups. When $\dim_{\mathbb{F}_\ell} E[\ell](M_\mathfrak{p}) = 0$, then one has $\dim_{\mathbb{F}_\ell} H^1(M_\mathfrak{p}, E[\ell]) = 2$, and there exists a unique unramified Lagrangian subspace and a unique ramified Lagrangian subspace, each of dimension 1. The second condition of Condition 4.3.9 implies that over the subfamilies of fields $L \in \mathcal{L}_{M,[l]}(X)$, as X grows arbitrarily large, the dimension of the image of $\mathrm{loc}_\mathfrak{q}$ is equal to 1 for all but 1 element of $\mathrm{Hom}(\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K), H^1_{ur}(M_\mathfrak{p}, E[\ell]))$. By Klagsbrun, Mazur, and Rubin 2014, Proposition 7.2, the probability that the dimension of Selmer groups will decrease by 1 is equal to $1-\ell^{-l}$, whereas the probability that the dimension of Selmer groups will increase by 1 is equal to ℓ^{-l}. This gives rise to the construction of the Markov chain $\mathcal{M}_{\ell,L}$ for each $\ell \geq 0$. The case for $\dim_{\mathbb{F}_\ell} E[\ell](M_\mathfrak{p}) = 2$ follows analogously, where one can show that the Markov chain $\mathcal{M}^2_{\ell,L}$ governs the changes in the dimension of $1-\sigma_\ell$ Selmer groups of $B_{L/K}$ with regards to consecutive twist by a place $\mathfrak{p}$ of M. The weighted coefficients determining the Markov chain $\mathcal{M}_\ell$ originate from the number of elements of the special linear group $\mathrm{SL}_2(\mathbb{F}_\ell)$ whose order is not equal to ℓ, is equal to ℓ, and is trivial (see Klagsbrun, Mazur, and Rubin 2014, Section 5 for example). It is not difficult to show that the unique stationary distribution of the Markov chain, denoted as $\pi = (\pi_i)_{i\geq 0}$ is given by the formula

$$\pi_i = \prod_{j\geq 0} \frac{1}{1+\ell^{-j}} \cdot \prod_{j=0}^{i} \frac{\ell}{\ell^j - 1}. \tag{4.49}$$

As a remark, when $k = 1$, i.e. L/K is a cyclic $\mathbb{Z}/\ell\mathbb{Z}$ Galois extension, it is a result of Klagsbrun, Mazur, and Rubin Klagsbrun, Mazur, and Rubin 2014 who demonstrated that assuming $\mu_\ell \subset K$ and $\mathrm{Gal}(K(E[\ell])/K) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$, the stationary distribution of the Markov chain M governs the probability distribution of dimensions of $1-\sigma_\ell$ Selmer groups $\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K)$ as the number of places of K that are ramified with respect to L/K grows arbitrarily large.

The probability distribution $b_{d,k}$ obtained from Proposition 4.3.3 can be interpreted as

the unique stationary distribution of a Markov chain $\mathcal{M}_\ell$ over a k dimensional countable state space. Because the Markov chain $\mathcal{M}_\ell$ over $\mathbb{Z}_{\geq 0}$ is an irreducible aperiodic Markov chain with the unique stationary distribution given by $\pi = (\pi_i)_{i\geq 0}$, the direct-product Markov chain $\boxtimes_{i=1}^k \mathcal{M}_\ell$ is an irreducible aperiodic Markov chain over the space $\mathbb{Z}_{\geq 0}^{\oplus k}$ with the unique stationary distribution $\hat{\pi}$ given by

$$\hat{\pi}(i_1, i_2, \cdots, i_k) := \prod_{j=1}^{k} \pi_{i_j}.$$

Furthermore, the probability distribution $b_{d,k}$ satisfies the condition

$$b_{d,k} = \sum_{\substack{i_1,i_2,\cdots,i_k \in \mathbb{Z}_{\geq 0} \\ i_1+i_2+\cdots+i_k = d}} \hat{\pi}(i_1, i_2, \cdots, i_k).$$

In other words, the probability distribution $b_{d,k}$ obtained from the random matrix model corresponds to a sum of stationary distribution of a k dimensional irreducible aperiodic Markov chain $\boxtimes_{i=1}^k \mathcal{M}_\ell$ along the zero locus of the hyperplane $x_1 + x_2 + \cdots + x_k = d$. $\square$

We now construct a Markov model suitable for governing the probability distribution of dimensions of $1 - \sigma_\ell$ Selmer groups of abelian varieties $B_{L/K}$ constructed from a family of Galois extensions $\{B_{L/K}\}_{L\in\mathcal{L}_M}$. One key issue with directly utilizing the random matrix models constructed for each $\mathcal{L}_M^{[k]}$ is that the symmetric pairings giving rise to the random matrix model have ranges lying in $\mathbb{F}_\ell^{\oplus k}$. Using the fact that every number k we consider satisfies $k \mid m$, we construct a new symmetric pairing whose ranges lie in $\mathbb{F}_\ell^{\oplus m}$. Hence, one obtains the following proposition as a reformulation of Proposition 4.3.3

Proposition 4.3.11. *Consider the following diagram*

$$\begin{array}{ccc} & & H^1(K, (Res_K^M E)[\ell]) \\ & & \downarrow \\ \prod_v \frac{B_{L/K}(K_v)}{(1-\sigma_\ell)B_{L/K}(K_v)} & \longrightarrow & \prod_v H^1(K_v, (Res_K^M E)[\ell]) \end{array} \tag{4.50}$$

Then there exists a quadratic form $Q : \prod_v H^1(K_v, (Res_K^M E)[\ell]) \to \mathbb{F}_\ell^{\oplus m}$ such that the images

of the horizontal and vertical maps are maximal isotropic subspaces with respect to Q, and their intersection is isomorphic to the Selmer group $\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K)$.

Proof. The inflation-restriction sequence of Galois cohomology groups induces an isomorphism given by

$$H^1(K, (\mathrm{Res}_K^M E)[\ell]) \cong H^1(M, E[\ell]^{\oplus m})^{\mathrm{Gal}(M/K)} \tag{4.51}$$

where $\mathrm{Gal}(M/K)$ acts on the cohomology group via cyclic permutation of the coordinates of $E[\ell]^{\oplus m}$. The Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$ induces a symmetric pairing whose image lies in $\mathbb{F}_\ell^{\oplus m}$:

$$H^1(M, E[\ell]^{\oplus m}) \times H^1(M, E[\ell]^{\oplus m}) \to H^2(M, \mu_\ell^{\oplus m}) \cong \mathbb{F}_\ell^{\oplus m}. \tag{4.52}$$

Let v be a place of K such that v factorizes as $v = \mathfrak{p}_1^e \cdots \mathfrak{p}_k^e$ over M. Then the localization of $H^1(K, (\mathrm{Res}_K^M E)[\ell])$ at v, with respect to the inflation-restriction sequence, satisfies

$$\begin{gathered} H^1(K_v, (\mathrm{Res}_K^M E)[\ell]) \cong \oplus_{i=1}^k H^1(M_{\mathfrak{p}_i}, E[\ell]^{\oplus m})^{\mathrm{Gal}(M_{\mathfrak{p}_i}/K_v)} \\ c_v \mapsto (c_{\mathfrak{p}_1}, c_{\mathfrak{p}_2}, \cdots, c_{\mathfrak{p}_k}) \end{gathered} \tag{4.53}$$

where $M_{\mathfrak{p}_i}/K_v$ is a degree $\frac{m}{k}$ Galois extension of K_v appearing as a summand of the localization of M at v, and the Galois group $\mathrm{Gal}(M_{\mathfrak{p}_i}/K_v)$ acts on the first cohomology group the via cyclic permutation of the coordinates of $E[\ell]^{\oplus m}$ as an element of order $\frac{m}{k}$. As before, using the Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$, the coordinate-wise cup product induces a pairing for each prime $\mathfrak{p}_i$ lying above v:

$$q_{\mathfrak{p}_i} : H^1(M_{\mathfrak{p}_i}, E[\ell]^{\oplus m}) \times H^1(M_{\mathfrak{p}_i}, E[\ell]^{\oplus m}) \to H^2(M_{\mathfrak{p}_i}, \mu_\ell^{\oplus m}) \cong \mathbb{F}_\ell^{\oplus m}. \tag{4.54}$$

Note that the cyclic permutation action of $\mathrm{Gal}(M_{\mathfrak{p}_i}/K_v)$ implies that each pairing, restricted

to the $\mathrm{Gal}(M_{\mathfrak{p}_i}/K_v)$-invariant cohomology group, has image lying inside

$$\overline{q_{\mathfrak{p}_i}} : H^1(M_{\mathfrak{p}_i}, E[\ell]^{\oplus m})^{\mathrm{Gal}(M_{\mathfrak{p}_i}/K_v)} \times H^1(M_{\mathfrak{p}_i}, E[\ell]^{\oplus m})^{\mathrm{Gal}(M_{\mathfrak{p}_i}/K_v)} \to H^2(M_{\mathfrak{p}_i}, \mu_\ell^{\oplus m})^{\mathrm{Gal}(M_{\mathfrak{p}_i}/K_v)} \cong \mathbb{F}_\ell^{\oplus k} \tag{4.55}$$

which recovers the coordinate-wise symmetric pairing obtained from (4.29)-(4.31).

We let Q be the quadratic form defined over $\prod_{v \text{ place of } K} H^1(K_v, (\mathrm{Res}_K^M E)[\ell])$ defined as

$$Q : \prod_{v \text{ place of } K} H^1(K_v, (\mathrm{Res}_K^M E)[\ell]) \to (\mathbb{Q}/\mathbb{Z})^{\oplus m} \tag{4.56}$$

$$(c_v)_v \mapsto \sum_{v \text{ place of } K} \sum_{\substack{\mathfrak{p} \text{ place of } M \\ \mathfrak{p}|v}} q_{\mathfrak{p}}(c_{\mathfrak{p}}). \tag{4.57}$$

The coordinate-wise short exact sequences of Brauer groups

$$0 \to H^2(M, E[\ell]^{\oplus m}) \to \oplus_{w \text{ place of } M} H^2(M_v, E[\ell]^{\oplus m}) \to (\mathbb{Q}/\mathbb{Z})^{\oplus m} \to 0 \tag{4.58}$$

imply that the quadratic form Q is trivial when restricted to the image of the localization

$$\prod_v \mathrm{loc}_v : H^1(K, (\mathrm{Res}_K^M E)[\ell]) \to \prod_v H^1(K_v, (\mathrm{Res}_K^M E)[\ell]). \tag{4.59}$$

The 9-term Poitou-Tate exact sequence Milne 2006, Theorem 1.4.10 shows that the image of the localization map is a maximal isotropic subspace with respect to the pairing Q. The rest of the proposition, as in Proposition 4.3.3, follows from the construction of the local Kummer maps and $1 - \sigma_\ell$ Selmer groups of $B_{L/K}$. □

As before, we assume Condition 4.3.9. The proof of Theorem 4.3.10 demonstrates that the Markov chain governing the dimensions of $1 - \sigma_\ell$ Selmer group of $B_{L/K}$ at a place v of K which factorizes over M as $v = \mathfrak{p}_1^e \mathfrak{p}_2^e \cdots \mathfrak{p}_k^e$ is governed by the Markov chain $\boxtimes_{i=1}^k \mathcal{M}_\ell$ over the state space $\mathbb{Z}_{\geq 0}^{\oplus k}$. In lieu of the proof of Proposition 4.3.11, one may, without loss of generality, extend the Markov chain $\boxtimes_{i=1}^k \mathcal{M}_\ell$ to the Markov chain defined over $\mathbb{Z}_{\geq 0}^{\oplus m}$

given by

$$\left(\boxtimes_{i=1}^{k}\mathcal{M}_{\ell}\right)\boxtimes\left(\boxtimes_{i=1}^{m-k}I\right) \tag{4.60}$$

where I is the identity Markov chain over $\mathbb{Z}_{\geq 0}$. As in Theorem 4.3.10, we are able to formulate the probability distribution of dimensions of $1-\sigma_p$ Selmer groups of $\{B_{L/K}\}_{L\in\mathcal{L}_M}$ as follows.

Theorem 4.3.12. *Assume Condition 4.3.9. We recall that $m=[M:K]$. Suppose that ℓ is an odd prime. Then the probability distribution of dimensions of $1-\sigma_\ell$ Selmer groups of families $\{B_{L/K}\}_{L\in\mathcal{L}_M}$ is given by*

$$\lim_{X\to\infty}\frac{\#\{L\in\mathcal{L}_M(X)\mid \dim_{\mathbb{F}_\ell}\mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K)=d\}}{\#\mathcal{L}_M(X)}=b_{d,m}. \tag{4.61}$$

Proof. Consider the Markov chain defined over the countable state space $\mathbb{Z}_{\geq 0}^{\oplus m}$:

$$\mathcal{M}:=\sum_{k\mid m}\frac{\#\{a\in\mathbb{Z}/m\mathbb{Z}\mid \mathrm{ord}(a)=\frac{m}{k}\}}{m}\left(\left(\boxtimes_{i=1}^{k}\mathcal{M}_{\ell}\right)\boxtimes\left(\boxtimes_{i=1}^{m-k}I\right)\right). \tag{4.62}$$

We observe that given any two $k_1,k_2\mid m$, the Markov chains $\left(\boxtimes_{i=1}^{k_1}\mathcal{M}_{\ell}\right)\boxtimes\left(\boxtimes_{i=1}^{m-k_1}I\right)$ and $\left(\boxtimes_{i=1}^{k_2}\mathcal{M}_{\ell}\right)\boxtimes\left(\boxtimes_{i=1}^{m-k_2}I\right)$ commute with each other, because any Markov operator commutes with the identity Markov operator. By construction, the Markov chain $\mathcal{M}$ is an irreducible aperiodic Markov chain over $\mathbb{Z}_{\geq 0}^{\oplus m}$. Adapting the proof of Park 2022, Lemma 4.15, because ℓ is an odd prime, the unique stationary distribution of the Markov chain $\sum_{i=1}^{\ell}a_iM_{p,L}^i$ over $\mathbb{Z}_{\geq 0}$, assuming it is irreducible and aperiodic, is given by $\pi=(\pi_i)_{i\geq 0}$ regardless of the values of a_i's. Using the commutativity of the Markov chains $\left(\boxtimes_{i=1}^{k}\mathcal{M}_{\ell}\right)\boxtimes\left(\boxtimes_{i=1}^{m-k}I\right)$ for any $k\mid m$, we may rewrite the Markov chain $\mathcal{M}^\ell$ for any $\ell\geq 1$ as the irreducible aperiodic Markov chain

$$\mathcal{M}^\ell=\boxtimes_{j=1}^{m}\left(\sum_{i=0}^{2\ell}a_{i,j}\mathcal{M}_{\ell,L}^i\right) \tag{4.63}$$

for some set of coefficients $\{a_{i,j}\}_{0\leq i\leq 2\ell,1\leq j\leq m}$ such that $\sum_{i=0}^{2\ell}a_{i,j}=1$ for all $1\leq j\leq m$.

Given any initial probability distribution $\delta : \mathbb{Z}_{\geq 0}^{\oplus m}$, as ℓ grows arbitrarily large, we obtain

$$\begin{aligned}\lim_{\ell\to\infty} \mathcal{M}^{\ell}\delta(i_1, i_2, \cdots, i_m) &= \lim_{\ell\to\infty} \boxtimes_{j=1}^{m} \left(\sum_{i=0}^{2\ell} a_{i,j}\mathcal{M}_{\ell,L}^{i}\right) \delta(i_1, i_2, \cdots, i_m) \\ &= \boxtimes_{j=1}^{m} \left(\lim_{\ell\to\infty} \sum_{i=0}^{2\ell} a_{i,j}\mathcal{M}_{\ell,L}^{i}\delta(i_j)\right) \\ &= \boxtimes_{j=1}^{m} \pi_{i_j}.\end{aligned} \tag{4.64}$$

Theorem 4.3.10 and the Chebotarev density theorem for cyclic Galois extensions M/K implies that the stationary distribution of $\mathcal{M}$ is the probabiltiy distribution of dimensions of $1 - \sigma_\ell$ Selmer groups of families $\{B_{L/K}\}_{L\in\mathcal{L}_M}$. We note that the commutativity of the Markov chains $\left(\boxtimes_{i=1}^{k}\mathcal{M}_\ell\right) \boxtimes \left(\boxtimes_{i=1}^{m-k} I\right)$ addresses the observation that the dimension of $1 - \sigma_\ell$ Selmer groups of the abelian variety $B_{L/K}$ twisted at ℓ many places over K is invariant under all possible orders in which one consecutively twists the abelian variety by such ℓ many places of K. □

As a corollary, we obtain heuristics on the stability of rank growths of elliptic curves with respect to some non-abelian Galois extensions, and the probability distribution of the sizes of torsion subgroup of Tate-Shafarevich groups of $B_{L/K}$ assuming Condition 4.3.9.

Corollary 4.3.13. *Assume Condition 4.3.9. Let m be a fixed constant. Denote by $P_{\ell,m,d,K}$, $R_{\ell,m,d,K}$, and $Ш_{\ell,m,d,K}$ the probabilities*

$$\begin{aligned}P_{\ell,m,d,K} &:= \frac{\#\{L \in \mathcal{L}_M(X) \mid \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K) = d\}}{\#\mathcal{L}_M(X)} \\ R_{\ell,m,d,K} &:= \frac{\#\{L \in \mathcal{L}_M(X) \mid Rank_{\mathbb{Z}} B_{L/K}(K) = d\}}{\#\mathcal{L}_M(X)} \\ Ш_{\ell,m,d,K} &:= \frac{\#\{L \in \mathcal{L}_M(X) \mid \dim_{\mathbb{F}_\ell} Ш_{B_{L/K}}[1 - \sigma_\ell] \equiv 0 \ mod\ m\}}{\#\mathcal{L}_M(X)}\end{aligned} \tag{4.65}$$

Then the following asymptotic statements hold.

$$\lim_{\ell\to\infty}\lim_{X\to\infty} P_{\ell,m,d,K} = \begin{cases} \binom{m}{d}\cdot\frac{1}{2^m} & \text{if } 0\le d\le m \\ 0 & \text{if } d>m \end{cases} \tag{4.66}$$

$$\lim_{\ell\to\infty}\lim_{X\to\infty}\sum_{d=1}^{\infty} R_{\ell,m,d,K} \le \frac{1}{2^m} \tag{4.67}$$

$$\lim_{\ell\to\infty}\lim_{X\to\infty} Ш_{\ell,m,d,K} = \frac{1}{2^{m-1}} \tag{4.68}$$

In particular, if $m=2$, then as the absolute value of the discriminant X grows arbitrarily large and ℓ grows arbitrarily large, approximately 50% of the $1-\sigma_\ell$ torsion subgroup of the Tate-Shafarevich group $B_{L/K}$ has non-square order.

Proof. The generating function for the probability distribution $\{b_{d,m}\}_{d=0}^{\infty}$ can be rewritten as

$$\sum_{d=0}^{\infty} b_{d,m}z^d = \left(\left(\frac{1}{2}+O(\frac{1}{\ell})\right)+\left(\frac{1}{2}+O(\frac{1}{\ell})\right)z+O(\frac{1}{\ell})z^2+\cdots+O(\frac{1}{\ell^{m(m-1)/2}})z^m+\cdots\right)^m. \tag{4.69}$$

The first part of the corollary hence follows from the fact that as ℓ grows arbitrarily large, the generating function for $\{b_{d,m}\}_{d=0}^{\infty}$ converges to the generating function for the binomial distribution with probability $\frac{1}{2}$, with error terms of order $O(\frac{1}{\ell})$. The second and the third part of the corollary follows from recalling that

$$\mathrm{Rank}_{\mathbb{Z}} B_{L/K}(K) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{1-\sigma_\ell}(B_{L/K}/K) - \dim_{\mathbb{F}_\ell} Ш_{B_{L/K}}[1-\sigma_\ell] \tag{4.70}$$

and that $\mathrm{Rank}_{\mathbb{Z}} B_{L/K}(K) \equiv 0 \bmod m$, because the abelian variety corresponds to the isotypic component of $\ell-1$ direct sums of m dimensional irreducible $\mathbb{Q}$-representations of $\mathbb{Z}/m\mathbb{Z}\rtimes\mathbb{Z}/\ell\mathbb{Z}$, see Remark 4.2.3. □

Remark 4.3.14. We note that $1-\sigma_\ell$ torsion subgroup of the Tate-Shafarevich group of the abelian variety $B_{L/K}$ does not necessarily have square order. This is due to the fact that every polarization of $B_{L/K}$ has degree divisible by ℓ^2 Howe 2001, hence $B_{L/K}$ does

not admit a principal polarization.

Remark 4.3.15. It is an interesting question to verify whether the conditions outlined in Condition 4.3.9 are in fact valid conditions that govern the $1-\sigma_\ell$ Selmer groups of abelian $m(\ell-1)$ folds. An upcoming work by Daniel Keliher and the author of this manuscript focuses on understanding rank growths of elliptic curves over number fields with respect to S_3 cubic field extensions Keliher and Park 2024. It would be interesting to understand under which conditions on the families of S_3 extensions L/K and the elliptic curve E over K the constraints in Condition 4.3.9 remain valid or not.

4.4 Sums of two rational cubes

The statistics of the dimensions of $1-\sigma_\ell$ Selmer groups of twist families of abelian varieties $\{B_{L/K}\}_{L\in\mathcal{L}_M}$ depends heavily on Condition 4.3.9, where one assumes two conditions on the manner of probability distribution of the local Kummer maps and the localization maps. It is hence natural to expect that the probability distribution of $1-\sigma_\ell$ Selmer groups of such twist families of abelian varieties will behave differently if any of Condition 4.3.9 is not satisfied. More concretely, we expect that changes in Condition 4.3.9 will result in giving rise to a differently constructed Markov chain $\mathcal{M}_\ell$ governing the changes in the dimension of $1-\sigma_\ell$ Selmer groups with respect to consecutive twists by places of K. This is precisely the case one observes from cubic twist families of elliptic curves $E_n : y^2 = x^3 - 432n^2$, the rank of the elliptic curves of which are closely related to understanding whether n can be written as a sum of two rational cubes Alpöge, Bhargava, and Shnidman 2022.

Unfortuantely, this current version of the manuscript does not succeed in computing the corank of 3^∞ Selmer groups of elliptic curves E_n or the corank of $(1-\sigma_3)^\infty$ Selmer groups of abelian 4-folds, the first problem of which will be explored in the upcoming work by Peter Koymans and Alex Smith Koymans and Alex Smith 2024. Nevertheless, we aim to demonstrate how the framework of the generalization of Poonen-Rains heuristics is relevant to the problem of understanding the probability that an integer is a sum of two rational cubes. Before we proceed, we sincerely thank Peter Koymans and Alex Smith for

pointing out several errors in the previous version of the manuscript, for giving extremely helpful and constructive feedbacks, and for kindly sharing their current work in progress in approaching the problem of computing the probability that an integer is a sum of two rational cubes.

As stated in Alpöge, Bhargava, and Shnidman 2022, the equation $n = x^3 + y^3$ is equivalent to the Weierstrass equation of the elliptic curve over $\mathbb{Q}$:

$$E_n : y^2 = x^3 - 432n^2. \tag{4.71}$$

We denote by E_n^{-3} the quadratic twist of the elliptic curve E_n by -3:

$$E_n^{-3} : y^2 = x^3 + 16n^2. \tag{4.72}$$

Denote by $\varphi_n : E_n \to E_n^{-3}$ the $\mathbb{Q}$-rational 3-isogeny defined as

$$\varphi_n : E_n \to E_n^{-3}, \;\; (x, y) \mapsto \left(\frac{x^3 - 1728n^2}{9x^2}, \frac{y(x^3 + 3456n^2)}{27x^3} \right) \tag{4.73}$$

see H. Cohen and Pazuki 2009 and Chan 2022 for further details on the properties of these $\mathbb{Q}$-rational 3-isogenies and the associated 3-isogeny Selmer groups of ellitpic curves E_n over $\mathbb{Q}$. The family of curves $\{E_n\}_{n \in \mathbb{Z}}$ forms a cubic twist family of elliptic curves whose endomorphism ring is isomorphic to $\mathbb{Z}[\zeta_3]$, where ζ_3 is a primitive 3rd root of unity. We note that these two isogenies satisfy the condition that

$$\frac{E_n^{-3}(\mathbb{Q})}{\varphi_n E_n(\mathbb{Q})} \cong \mu_3(\mathbb{Q}) \cong 0, \;\; \frac{E_n(\mathbb{Q})}{\hat{\varphi}_n E_n^{-3}(\mathbb{Q})} \cong \mathbb{Z}/3\mathbb{Z} \tag{4.74}$$

In lieu of Definition 4.2.2, we let our base field $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_3, \sqrt[3]{n})$, and $M = \mathbb{Q}(\zeta_3)$. We denote by $B_{L/K}$ the abelian 4-fold over $K = \mathbb{Q}$ defined as

$$B_{L/K} := \mathrm{Ker}\left(\mathrm{Res}_K^L E \to \mathrm{Res}_K^M E \right) \tag{4.75}$$

Over the field L, one obtains the $\mathrm{Gal}(\overline{K}/L)$-equivariant isomorphism

$$B_{L/K} \cong E_n \times E_n^{-3} \times E_{n^2} \times E_{n^2}^{-3}, \tag{4.76}$$

In fact, the fact that E_n is a CM elliptic curve with $\mathrm{End}(E_n(\mathbb{Q})) \supset \mathbb{Z}[\zeta_3]$ implies that the above isomorphism is a $\mathrm{Gal}(\overline{K}/K)$-equivariant isomorphism. Recall that the multiplication by 3 map over $B_{L/K}$ factorizes as

$$B_{L/K} \cong E_n \times E_n^{-3} \times E_{n^2} \times E_{n^2}^{-3} \to E_n^{-3} \times E_n \times E_{n^2}^{-3} \times E_{n^2} \to E_n \times E_n^{-3} \times E_{n^2} \times E_{n^2}^{-3} \cong B_{L/K} \tag{4.77}$$

where the first morphism corresponds to the isogeny $\varphi_n \times \hat{\varphi}_n \times \varphi_{n^2} \times \hat{\varphi}_{n^2}$, and the second morphism corresponds to the isogeny $\varphi_{n^2} \times \hat{\varphi}_{n^2} \times \varphi_n \times \hat{\varphi}_n$. Without loss of generality, we may hence identify the endomorphism $1 - \sigma_3 : B_{L/K} \to B_{L/K}$ with the endomorphism $\varphi_n \times \hat{\varphi}_n \times \varphi_{n^2} \times \hat{\varphi}_{n^2}$ of $E_n \times E_n^{-3} \times E_{n^2} \times E_{n^2}^{-3}$.

It follows from Proposition 4.2.4 that given an order-3 element $\sigma_3 \in \mathrm{Gal}(L/K) \cong S_3$, there exists a $\mathrm{Gal}(\overline{K}/K)$-equivariant isomorphism

$$B_{L/K}[1 - \sigma_3] \cong (\mathrm{Res}_K^M E_1)[3] \tag{4.78}$$

and that regardless of the choice of the Galois extensions L/K, one obtains the natural inclusion

$$\mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) \subset H^1(K, (\mathrm{Res}_K^M E_1)[3]). \tag{4.79}$$

We also note that one obtains the isomorphism of $\mathrm{Gal}(\overline{K}/K)$-modules

$$\mathrm{Sel}_3(B_{L/K}/K) \cong \mathrm{Sel}_{(1-\sigma_3)^2}(B_{L/K}/K). \tag{4.80}$$

Recall that there exists a skew-symmetric pairing (also known as the Cassels-Tate pairing),

$$Q_L : \mathrm{Sel}_3(B_{L/K}/K) \times \mathrm{Sel}_3(B_{L/K}/K) \to \mathbb{F}_3 \tag{4.81}$$

whose kernel satisfies the relation

$$\mathrm{Rank}_{\mathbb{Z}}(B_{L/K}(K)) \leq \dim_{\mathbb{F}_3} \mathrm{Ker}(Q_L) \leq \dim_{\mathbb{F}_3} \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K), \tag{4.82}$$

see in particular Cassels 1959 for the explicit construction of the pairing above using Hilbert norm residue symbol.

We now demonstrate that the dimensions of $\mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K)$ and $\mathrm{Ker}(Q_L)$, as $\mathbb{F}_3$ vector spaces, grow in a similar manner to how the dimensions of φ_n-Selmer groups of E_n grows arbitrarily large as the number of prime factors equivalent to 2 mod 3 grows arbitrarily large. We state the main result as follows.

Theorem 4.4.1. *For any $L \in \mathcal{L}_M$, we obtain*

$$\dim_{\mathbb{F}_3} \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) = 2 \cdot \#\{v \text{ place of } K \mid v \equiv 2 \bmod 3,\ v \neq 2,\ v \text{ ramified over } L\} + \Delta_n \tag{4.83}$$

$$\dim_{\mathbb{F}_3} Ker(Q_L) \geq 2 \cdot \#\{v \text{ place of } K \mid v \equiv 8 \bmod 9,\ v \text{ ramified over } L\} - 3 \tag{4.84}$$

for some integer $-1 \leq \Delta_n \leq 3$.

In particular, as X grows arbitrarily large, the expected value of the dimensions of $1 - \sigma_3$ Selmer groups of $B_{L/K}$ grows at a rate of $\log\log X$, and the expected value of the dimensions of the kernel of the Cassels-Tate pairing grows at least at a rate of $\frac{1}{3}\log\log X$.

Before we prove both statements of Theorem 4.4.1, we first introduce the notion of Selmer groups for local twists of abelian varieties, the theory of which was developed by Klagsbrun, Mazur, and Rubin Klagsbrun, Mazur, and Rubin 2013; Klagsbrun, Mazur, and Rubin 2014 for local twists of elliptic curves over number fields.

We first outline the notations to be used throughout this manuscript, which are analogous to those used in Klagsbrun, Mazur, and Rubin 2014, Sections 5, 7, 9 and Park 2022, Section 4.

Definition 4.4.2. We introduce the following notations, borrowed from corresponding sections in Klagsbrun, Mazur, and Rubin 2013; Klagsbrun, Mazur, and Rubin 2014; Park 2022.

- K: The base field over which the elliptic curve E_1 is defined over. Throughout this manuscript, we will consider the case where $K = \mathbb{Q}$, but for the sake of generalization to other number fields, we will write the definitions in terms of an arbitrary number field K.
- Σ: the set of places of K containing the places of K above primes $(2), (3) \in \mathbb{Z}$ and ∞. (These consist of places of bad reduction of E, places above 2, and archimedean places). One may enlarge Σ to contain other places of K if necessary.
- σ: a square-free product of finite places v of K which are not above the prime $(3) \in \mathbb{Z}$.
- $|\sigma|$: the product of norms of places $v \mid \sigma$, i.e. $|\sigma| = \prod_{v|\sigma} N_{\mathbb{Q}}^{K}(v)$.
- Ω_σ: the set of finite Cartesian products of local homomorphisms

$$(\chi_v)_v \in \prod_{\substack{v\in\Sigma \text{ or} \\ v|\sigma \text{ s.t. } v=2 \bmod 3}} \frac{\mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), S_3)}{\mathrm{Aut}(\mu_3)} \times \prod_{v|\sigma \text{ s.t. } v=1 \bmod 3} \frac{\mathrm{Hom}(\mathrm{Gal}(\overline{K}_v/K_v), \mathbb{Z}/3\mathbb{Z})}{\mathrm{Aut}(\mu_3)}$$

  We assume that the component χ_v is ramified if $v \mid \sigma$.

  For any place $v \in K$ which is not above the ideal (3), up to equivalence of the action of the automorphism group of 3-rd roots of unity $\mathrm{Aut}(\mu_3)$, there are a total of 4 equivalence classes of cyclic order 3 characters, 1 of which is unramified, and 3 of which is tamely ramified.

- Ω_1: the set of finite Cartesian products of local homomorphisms supported over $v \in \Sigma$.
- Ω: the inverse limit of Cartesian products of local homomorphisms $\varprojlim_\sigma \Omega_\sigma$ induced from the projection maps $\phi_{\sigma\sigma',\sigma} : \Omega_{\sigma\sigma'} \to \Omega_\sigma$.

- RES: The restriction map

$$\begin{aligned} \text{RES} : \text{Hom}(\text{Gal}(\overline{K}/K), \mu_3) &\to \Omega \\ \chi &\mapsto (\chi_v)_v \end{aligned} \tag{4.85}$$

  which maps a global character χ corresponding to the cyclic cubic extension L/K to a Cartesian product of local homomorphisms $(\chi_v)_v \in \Omega_\sigma$ such that σ is a squarefree product of places in K ramified over L.

- L^{χ_v}: the local cubic field extension over the local field K_v at a place v associated to the character χ_v.

- E_{χ_v}: the associated local cubic twist of elliptic curve E_1:

$$E_{\chi_v} := \text{Ker}\left(\text{Nm} : \text{Res}_{K_v}^{L^{\chi_v}} E_1 \to E_1\right) \tag{4.86}$$

- δ_v: the local Kummer map at place v defined as

$$\delta_v : E(K_v)/3E(K_v) \to H^1(K_v, E[3]). \tag{4.87}$$

- $\delta_v^{\chi_v}$: the local Kummer map associated to the character χ_v at place v defined as

$$\delta_v^{\chi_v} : E_{\chi_v}(K_v)/(1-\sigma_n)E_{\chi_v}(K_v) \to H^1(K_v, E_1[3]). \tag{4.88}$$

  As a subspace of $H^1(K_v, E^{\chi_v}[1-\sigma_n]) \cong H^1(K_v, E_1[3])$, the images of the local Kummer maps satisfy

$$\text{im}\delta_v^{\chi_v} = \begin{cases} \text{im}\delta_v & \text{if } \chi_v \text{ trivial} \\ \text{Hom}(\text{Gal}(L^{\chi_v}/K_v), E_1[3]) & \text{if } \chi_v \text{ non-trivial.} \end{cases} \tag{4.89}$$

  We refer to Klagsbrun, Mazur, and Rubin 2013, Lemma 5.7 for the proof of the equation above.

- q_v: the uniquely determined Tate quadratic form $q_v : H^1(K_v, E[3]) \times H^1(K_v, E[3]) \to \mu_3$, see for example Klagsbrun, Mazur, and Rubin 2013, Lemma 3.4.

- $\mathcal{H}(K_v)$: the set of Lagrangian subspaces V of $H^1(K_v, E_1[3])$ with respect to the Tate quadratic form q_v. These are subspaces which satisfy $V = V^\perp$ and is a maximal isotropic subspace with respect to q_v, i.e. $q_v(\mathfrak{v}, \mathfrak{w}) = 0$ for any $\mathfrak{v}, \mathfrak{w} \in V$ and $\dim_{\mathbb{F}_3} V = \frac{1}{2} \dim_{\mathbb{F}_3} H^1(K_v, E_1[3])$.

- $\mathcal{H}_{ram}(K_v)$: the set of Lagrangian subspaces V of $H^1(K_v, E_1[3])$ such that

$$V \cap H^1_{ur}(K_v, E_1[3]) = 0 \tag{4.90}$$

  where $H^1_{ur}(K_v, E_1[3])$ is the unramified local first cohomology group.

- $\mathcal{P}_i$: the set of places of v over $\mathcal{O}_K$ that satisfies

$$v \in \mathcal{P}_i \iff \begin{cases} v \notin \Sigma \text{ and} \\ \dim_{\mathbb{F}_3} E_1[3](K_v) = i. \end{cases} \iff \begin{cases} v \notin \Sigma \text{ and} \\ v = 2i \bmod 3. \end{cases} \tag{4.91}$$

  Suppose that $K = \mathbb{Q}$. We note that $v \in \mathcal{P}_1$ if and only if $\mu_3 \notin K_v$, which is equivalent to $v \equiv 2 \bmod 3$. Hence, the Chebotarev density theorem implies that

$$\lim_{n\to\infty} \frac{\#\{v \text{ place of } \mathbb{Z} \mid h(v) < n,\ v \in \mathcal{P}_i\}}{\#\{v \text{ place of } \mathbb{Z} \mid h(v) < n\}} = \begin{cases} 0 & \text{if } i = 0 \\ \frac{1}{2} & \text{if } i = 1 \\ \frac{1}{2} & \text{if } i = 2. \end{cases} \tag{4.92}$$

We recall the following fact about the relations between $\mathcal{P}_i$ and the set of Lagrangian subspaces of $H^1(K_v, E_1[3])$.

Lemma 4.4.3. *The following properties hold for any $v \in \mathcal{P}_i$ for $0 \le i \le 2$.*

1. $\dim_{\mathbb{F}_3} H^1(K_v, E_1[3]) = 2i$.

2. *Every Lagrangian subspace of* $H^1(K_v, E_1[3])$ *have dimensions equal to* i *as* $\mathbb{F}_3$ *vector spaces.*

3. *If we further suppose that* $i \neq 0$*, then* $\#\mathcal{H}_{ram}(K_v) = 3^{i-1}$*. In particular, if* $i = 1$*, then there exists a unique ramified Lagrangian subspace in* $H^1(K_v, E_1[3])$*. If* $i = 2$*, then there exists a bijection between the set of ramified cyclic* 3*-extensions of* K_v *and the elements of* $\mathcal{H}_{ram}(K_v)$*.*

Proof. We refer to Klagsbrun, Mazur, and Rubin 2013, Lemma 3.7 and Klagsbrun, Mazur, and Rubin 2014, Definition 5.7 - Definition 5.10. □

For the remainder of the manuscript, we fix $K = \mathbb{Q}$. With the notations above, given a local character $(\chi_v)_v \in \Omega_\sigma$, we define the locally twisted $1 - \sigma_3$ Selmer groups of the 4-dimensional abelian variety B_E over $\mathbb{Q}$, denoted as $\mathrm{Sel}_{1-\sigma_3}(B_{(\chi_v)_v}/\mathbb{Q})$, as a subspace of $H^1(\mathbb{Q}, E_1[3])^{\oplus 2}$ satisfying

$$\mathrm{Sel}_{1-\sigma_3}(B_{(\chi_v)_v}/\mathbb{Q}) := \left\{ c \in H^1(\mathbb{Q}, E_1[3]^{\oplus 2}) \mid c \in \delta_v^{\chi_v}(B_{(\chi_v)_v}[1-\sigma_3](\mathbb{Q}_v)) \ \forall \text{ place } v \in \mathbb{Z} \right\} \tag{4.93}$$

where the notation $B_{(\chi_v)_v}[1-\sigma_3](\mathbb{Q}_v)$ indicates the maximal isotropic subspace of $H^1(\mathbb{Q}_v, E_1[3]^{\oplus 2}) = H^1(\mathbb{Q}_v, E_1[3])^{\oplus 2}$ for each place v with respect to the direct sum of the Tate quadratic form $q_v \oplus q_v$.

The family of locally twisted Selmer groups we focus are the Selmer groups of form

$$\mathrm{Sel}_{1-\sigma_3}(B_n/\mathbb{Q}) = \mathrm{Sel}_{1-\sigma_3}(B_{\mathrm{RES}(\chi_n)}/\mathbb{Q}) \tag{4.94}$$

where $\mathrm{RES} : \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}(\zeta_3)), \mu_3) \to \Omega$ is the restriction of a global cubic character over $\mathbb{Q}(\zeta_3)$ to Cartesian product of local homomorphisms Ω. In lieu of Lemma 4.4.3, the local Kummer maps characterizing the locally twisted Selmer groups $\mathrm{Sel}_{1-\sigma_3}(B_{\mathrm{RES}(\chi_n)}/\mathbb{Q})$ can be characterized as follows.

Lemma 4.4.4. *The following properties hold for any* $v \in \mathcal{P}_i$ *for* $0 \leq i \leq 2$*.*

1. $\dim_{\mathbb{F}_3} H^1(\mathbb{Q}_v, B_{RES(\chi_n)}[1-\sigma_3]) = 4i$.

2. *Every Lagrangian subspace of* $H^1(K_v, B_{RES(\chi_n)}[1-\sigma_3])$ *with respect to the pairing* $q_v \oplus q_v$ *have dimensions equal to* i *as* $\mathbb{F}_3$ *vector spaces.*

3. *Suppose that* $v \in \mathcal{P}_1$ *or* $v = 3$. *Then there are exactly* 2 *configurations of all possible images of the local Kummer maps of* $B_{RES(\chi_n)}(\mathbb{Q}_v)$ *parametrized over cubefree integers* $n \in \mathbb{Z}$, *which is in bijection to the set of two equivalence classes of local Galois characters* $Hom(Gal(\overline{\mathbb{Q}_v}/\mathbb{Q}_v), S_3)/Aut(\mu_3)$ *characterizing the field extension* $\mathbb{Q}_v(\zeta_3)$ *and* $\mathbb{Q}_v(\zeta_3, \sqrt[3]{v})$.

4. *Suppose that* $v \in \mathcal{P}_2$. *Then there are exactly* 4 *configurations of all possible images of the local Kummer maps of* $B_{RES(\chi_n)}(\mathbb{Q}_v)$ *parametrized over cubefree integers* $n \in \mathbb{Z}$, *which is in bijection to the set of equivalence classes of local homomorphisms in* $Hom(Gal(\overline{\mathbb{Q}_v}/\mathbb{Q}_v), \mu_3)/Aut(\mu_3)$.

Proof. The first two parts of the proposition follow from Proposition 4.2.4 that $B_n[1-\sigma_3] \cong (\mathrm{Res}_K^M E_1)[3]$. Given a twist $\psi_n := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ acting on B_{E_1}, the $\mathbb{Q}_v$-rational points of infinite order of B_n, which is isogenous to $E_n \times E_{n^2}$, are parametrized by the images of the following matrices over $\mathbb{Z}$:

$$\psi_n \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \mapsto P_1 \in E_n(\mathbb{Q}_v), \quad \psi_n \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = 3u \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \mapsto P_2 \in E_n^{-3}(\mathbb{Q}_v) \tag{4.95}$$

$$\psi_n \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ 0 & c \end{bmatrix} \mapsto P_3 \in E_{n^2}(\mathbb{Q}_v), \quad \psi_n \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = 3u \begin{bmatrix} 0 & a \\ 0 & c \end{bmatrix} \mapsto P_4 \in E_{n^2}^{-3}(\mathbb{Q}_v) \tag{4.96}$$

Hence, the image of the local Kummer maps $B_{\mathrm{RES}(\chi_n)(\mathbb{Q}_v)}$ are either simultaneously unramified Lagrangian subspaces or simultaneously ramified Lagrangian subspaces with respect to the pairing q_v at each component of $H^1(\mathbb{Q}_v, E_1[3])$. Lemma 4.4.3 implies that the number of configuration of all possible images of local Kummer maps $B_{\mathrm{RES}(\chi_n)(\mathbb{Q}_v)}$ for $v \in \mathcal{P}_i$ is equal to $1 + 3^{i-1} = 2i$.

One can obtain a bijection between certain types of maximal isotropic subspaces of $H^1(\mathbb{Q}_v, E_1[3]^{\oplus 2})$ and certain equivalence classes of local homomorphisms over $\mathbb{Q}_v$ up to the action of $\mathrm{Aut}(\mu_3)$. Let us recall that the family of abelian varieties we focus on this manuscript ranges over global cubic characters $\chi_n \in \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}(\zeta_3))$ for any cube-free integer $n \in \mathbb{Z}$ associated to the Galois S_3-extension $\mathbb{Q}(\zeta_3, \sqrt[3]{n})$ over $\mathbb{Q}$. If $v = 1 \bmod 3$, then the restriction $\mathrm{res}_v(\chi_n)$ at place v corresponds to cyclic $\mathbb{Z}/3\mathbb{Z}$ Galois extension $\mathbb{Q}_v(\sqrt[3]{n})/\mathbb{Q}_v$, 1 of which is an unramified character and the other 3 of which are ramified characters. If $v = 2 \bmod 3$, then the restriction $\mathrm{res}_v(\chi_n)$ at place v corresponds to the unramified quadratic extension $\mathbb{Q}_v(\zeta_3)/\mathbb{Q}_v$ if $v \nmid n$, and corresponds to the ramified S_3 extension $\mathbb{Q}_v(\zeta_3, \sqrt[3]{v})/\mathbb{Q}_v$ if $v \mid n$. Here we are using the fact that any integer modulo prime v is a cube, except for the integer v itself. There are exactly two such local homomorphisms. If $v = 3$, then the restriction $\mathrm{res}_v(\chi_n)$ at place v corresponds to the quadratic extension $\mathbb{Q}_3(\zeta_3)/\mathbb{Q}_3$ if $3 \nmid n$, or the S_3 extension $\mathbb{Q}_3(\zeta_3, \sqrt[3]{3})/\mathbb{Q}_3$ if $3 \mid n$. Again, we are using the fact that any integer modulo 3 is a cube, except for the integer 3 itself. □

We now present the proof of Theorem 4.4.1.

Proof. **Part (1)**

Given an integer $n \in \mathbb{Z}$, let $L = \mathbb{Q}(\zeta_3, \sqrt[3]{n})$ and $K = \mathbb{Q}$. We use the identification $1 - \sigma_3 : B_{L/K} \to B_{L/K}$ as the morphism $\varphi_n \times \hat{\varphi}_n \times \varphi_{n^2} \times \hat{\varphi}_{n^2} : E_n \times E_n^{-3} \times E_{n^2} \times E_{n^2}^{-3}$ to obtain the factorization of multiplication by $1 - \sigma_3$ map as

$$1 - \sigma_3 = (\varphi_n \times \hat{\varphi_n} \times Id \times Id) \circ (Id \times Id \times \varphi_{n^2} \times \hat{\varphi}_{n^2}) \tag{4.97}$$

where Id is the identity map over any elliptic curve $E/\mathbb{Q}$. Note that we also have the identification

$$\begin{aligned} \mathrm{Sel}_{\varphi_n \times \hat{\varphi_n} \times Id \times Id}(B_{L/K}/K) &\cong \mathrm{Sel}_{\varphi_n \times \hat{\varphi_n}}(E_n \times E_n^{-3}/\mathbb{Q}) \\ \mathrm{Sel}_{Id \times Id \times \varphi_{n^2} \times \hat{\varphi}_{n^2}}(B_{L/K}/K) &\cong \mathrm{Sel}_{\varphi_{n^2} \times \hat{\varphi_{n^2}}}(E_{n^2} \times E_{n^2}^{-3}/\mathbb{Q}) \end{aligned} \tag{4.98}$$

This allows us to obtain the following short exact sequence of Selmer groups

$$0 \to \frac{B_{L/K}[Id \times Id \times \varphi_{n^2} \times \hat{\varphi}_{n^2}](K)}{\varphi_n \times \hat{\varphi}_n \times Id \times Id(B_{L/K}[1-\sigma_3])(K)} \to_{f_n} \mathrm{Sel}_{\varphi_n \times \hat{\varphi}_n}(E_n \times E_n^{-3}/K)$$
$$\to \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) \to \mathrm{Sel}_{\varphi_{n^2} \times \hat{\varphi}_{n^2}}(E_{n^2} \times E_{n^2}^{-3}/K) \to 0 \tag{4.99}$$

We note that one has the identification

$$\frac{B_{L/K}[Id \times Id \times \varphi_{n^2} \times \hat{\varphi}_{n^2}](K)}{\varphi_n \times \hat{\varphi}_n \times Id \times Id(B_{L/K}[1-\sigma_3])(K)} \cong \mathbb{Z}/3\mathbb{Z} \tag{4.100}$$

We hence obtain that

$$\dim_{\mathbb{F}_3} \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) = \dim_{\mathbb{F}_3} \mathrm{Sel}_{\varphi_n \times \hat{\varphi_n}}(E_n \times E_n^{-3}/K) + \dim_{\mathbb{F}_3} \mathrm{Sel}_{\varphi_{n^2} \times \hat{\varphi_{n^2}}}(E_{n^2} \times E_{n^2}^{-3}/K) - 1. \tag{4.101}$$

We note that because as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, $E_n \times E_n^{-3}[\varphi \times \hat{\varphi}] \cong \mathbb{Z}/3\mathbb{Z} \times \mu_3 \cong E_1[3]$, it follows that

$$\mathrm{Sel}_{\varphi_n \times \hat{\varphi_n}}(E_n \times E_n^{-3}/K) \subset H^1(\mathbb{Q}, E_n \times E_n^{-3}[\varphi \times \hat{\varphi}]) \cong H^1(\mathbb{Q}, E_1[3]). \tag{4.102}$$

The probabiltiy distribution of dimensions of $\mathrm{Sel}_{\varphi_n \times \hat{\varphi_n}}(E_n \times E_n^{-3}/K)$ is hence determined from the local Selmer structure $\mathrm{Sel}_3((E_1)_{(\chi_v)_v}/\mathbb{Q})$ given a choice of a local character $(\chi_v)_v \in \Omega_n$, which is defined analogously to the construction of local Selmer structure for abelian 4-folds stated in equation (4.93) as

$$\mathrm{Sel}_3((E_1)_{(\chi_v)_v}/\mathbb{Q}) := \left\{ c \in H^1(\mathbb{Q}, E_1[3]^{\oplus 2} \mid c \in \delta_v^{\chi_v} \left((E_1)_{(\chi_v)_v}[3](\mathbb{Q}_v) \right) \forall \text{ place } v \in \mathbb{Z} \right\} \tag{4.103}$$

and the notation $\delta_v^{\chi_v} \left((E_1)_{(\chi_v)_v}[3](\mathbb{Q}_v) \right)$ denotes the maximal isotropic subspace of $H^1(\mathbb{Q}_v, E_1[3])$ determined from the local Kummer map for each place v with respect to the Tate quadratic form q_v. To elaborate, for every f_n there exists some choice of local character $(\chi_v)_v \in \Omega_n$

such that

$$\dim_{\mathbb{F}_3} \mathrm{Sel}_{\varphi_n \times \hat{\varphi_n}}(E_n \times E_n^{-3}/K) = \dim_{\mathbb{F}_3} \mathrm{Sel}_3((E_1)_{(\chi_v)_v}). \tag{4.104}$$

The analogous relation holds for $\mathrm{Sel}_{\varphi_{n^2} \times \hat{\varphi_{n^2}}}(E_{n^2} \times E_{n^2}^{-3}/K)$ as well.

Let $(\chi_v)_v \in \Omega_n$ be a set of local characters. For any place $\omega \mid n$ such that $\omega \neq 2, 3$, let $(\chi'_v)_v \in \Omega_{n\omega}$ the set of local characters such that $\phi_{n\omega,n}(\chi') = \chi$. Then the images of the local Kummer maps at place v satisfies

$$\begin{aligned} &\mathrm{im}\delta_v \left((E_1)_{(\chi_v)_v}[3](\mathbb{Q}_\omega \right) \cong H^1_{ur}(\mathbb{Q}, E_1[3]) \\ &\mathrm{im}\delta_v \left((E_1)_{(\chi'_v)_v}[3](\mathbb{Q}_\omega \right) \in \mathcal{H}_{ram}(\mathbb{Q}_\omega). \end{aligned} \tag{4.105}$$

The image of the localization map $\mathrm{loc}_\omega : \mathrm{Sel}_3((E_1)_{(\chi_v)_v}/\mathbb{Q}) \to H^1_{ur}(\mathbb{Q}_\omega, E_1[3])$ depends on the whether the place ω splits over $M = \mathbb{Q}(\zeta_3)$ or not. By the proof of Klagsbrun, Mazur, and Rubin 2014, Proposition 7.2, it suffices to compute the dimension of the localization map

$$\mathrm{loc}_\omega \left(\mathrm{Sel}_3((E_1)^{[\omega]}_{(\chi_v)_v} \right) \tag{4.106}$$

where

$$\mathrm{Sel}_3((E_1)^{[\omega]}_{(\chi_v)_v} := \mathrm{Ker} \left(H^1(K, E_1[3]) \to \oplus_{v \neq \omega} H^1(K_v, E_1[3])/\mathrm{im}\delta_v^\chi \right) \tag{4.107}$$

i.e. it is a finite dimensional subspace of $H^1(K, E_1[3])$ which contains $\mathrm{Sel}_3((E_1)^{[\omega]}_{(\chi_v)_v}$ obtained by forgetting the local conditions at place ω. Using the identification $E_1[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mu_3$, it follows that given any place ω of K,

$$\{1, \omega, \omega^2\} \subset \mathrm{Sel}_3((E_1)^{[\omega]}_{(\chi_v)_v} \tag{4.108}$$

This hence implies that

$$\mathrm{loc}_{\omega}\left(\mathrm{Sel}_3((E_1)^{[\omega]}_{(\chi_v)_v}\right) \cap H^1_{ur}(K_v, E_1[3]) = \begin{cases} 1 & \text{if } \omega \equiv 1 \bmod 3 \\ 0 & \text{if } \omega \equiv 2 \bmod 3 \end{cases} \tag{4.109}$$

By Klagsbrun, Mazur, and Rubin 2014, Proposition 7.2, it follows that

$$\dim_{\mathbb{F}_3} \mathrm{Sel}_3((E_1)_{(\chi'_v)_v}) - \dim_{\mathbb{F}_3} \mathrm{Sel}_3((E_1)_{(\chi_v)_v} = \begin{cases} 0 & \text{if } \omega \equiv 1 \bmod 3 \\ 1 & \text{if } \omega \equiv 2 \bmod 3 \end{cases} \tag{4.110}$$

Chebotarev density theorem over the quadratic extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ indicates that the Markov chain M over the countable state space $\mathbb{Z}_{\geq 0}$ governing the dimensions of $\mathrm{Coker} f_n$ is characterized by two Markov operators over the countable state space $\mathbb{Z}_{\geq 0}$: The identity Markov chain Id governing twists by primes $\omega \equiv 1 \bmod 3$: And the Markov chain $\hat{M} := (\hat{m}_{i,j})_{i,j\geq 0}$ governing twists by primes $\omega \equiv 2 \bmod 3$ given by

$$\hat{m}_{i,j} = \begin{cases} 1 & \text{if } j = i+1 \\ 0 & \text{otherwise.} \end{cases} \tag{4.111}$$

For each $k \in \mathbb{Z}_{\geq 0}$, we denote by $\delta_k : \mathbb{Z}_{\geq 0} \to [0,1]$ the initial probability distribution defined as

$$\delta_k(x) = \begin{cases} 1 & \text{if } x = k \\ 0 & \text{otherwise .} \end{cases} \tag{4.112}$$

Given an integer $n \in \mathbb{Z}_{\geq 0}$, denote by $w_1(n)$ (and $w_2(n)$) the number of distinct prime factors of n which are equivalent to 1 mod 3 (and 2 mod 3 that is not 2, respectively).

Then we obtain that there exists some integer $k_n \in \mathbb{Z}_{\geq 0}$ such that

$$\left((Id)^{w_1(n)}(\hat{M})^{w_2(n)}\delta_{k_n}\right)(x) = \begin{cases} 1 & \text{if } x = \dim_{\mathbb{F}_3} \mathrm{Sel}_{\varphi_{n^2}\times\hat{\varphi_{n^2}}}(E_{n^2} \times E_{n^2}^{-3}/K) = k_n + w_2(n) \\ 0 & \text{otherwise} \end{cases} \tag{4.113}$$

We note that the probability distribution δ_{k_n} is determined by the local Kummer maps at places $\omega = 2, 3$. In particular, we obtain that $0 \leq k_n \leq 2$ because $\mu_3 \not\subset \mathbb{Q}_\omega$ for $\omega = 2, 3$. Referring to equation (4.101), we hence obtain that for any $L = \mathbb{Q}(\zeta_3, \sqrt[3]{n})$ and $K = \mathbb{Q}$,

$$\begin{aligned} \dim_{\mathbb{F}_3} \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) &= \dim_{\mathbb{F}_3} \mathrm{Sel}_{\varphi_n\times\hat{\varphi}_n}(E_n \times E_n^{-3}) + \dim_{\mathbb{F}_3} \mathrm{Sel}_{\varphi_{n^2}\times\hat{\varphi}_{n^2}}(E_{n^2} \times E_{n^2}^{-3}) - 1 \\ &= w_2(n) + w_2(n^2) - 1 + k_n + k_{n^2} \\ &= 2w_2(n) - 1 + k_n + k_{n^2}. \end{aligned} \tag{4.114}$$

Setting $\Delta_n := k_n + k_{n^2} - 1$ yields the first statement of the theorem.

Part (2)

As before, we choose $L = \mathbb{Q}(\zeta_3, \sqrt[3]{n})$, $M = \mathbb{Q}(\zeta_3)$, and $K = \mathbb{Q}$. Using the identification

$$\begin{aligned} \mathrm{Sel}_{\varphi_n\times\hat{\varphi_n}}(E_n \times E_n^{-3}/K) &\cong \mathrm{Sel}_{\varphi_n}(E_n/M) \\ \mathrm{Sel}_{\varphi_{n^2}\times\hat{\varphi}_{n^2}}(E_{n^2} \times E_{n^2}^{-3}/K) &\cong \mathrm{Sel}_{\varphi_{n^2}}(E_{n^2}/M) \end{aligned} \tag{4.115}$$

one can define the Cassels-Tate pairings Q_n and Q_{n^2} as outlined in Cassels 1959.

$$\begin{aligned} Q_n &: \mathrm{Sel}_{\varphi_n\times\hat{\varphi_n}}(E_n/M) \times \mathrm{Sel}_{\varphi_n\times\hat{\varphi_n}}(E_n/M) \to \mathbb{F}_3 \\ Q_{n^2} &: \mathrm{Sel}_{\varphi_{n^2}\times\hat{\varphi_{n^2}}}(E_{n^2}/M) \times \mathrm{Sel}_{\varphi_{n^2}\times\hat{\varphi_{n^2}}}(E_{n^2}/M) \to \mathbb{F}_3. \end{aligned} \tag{4.116}$$

More concretely, given a pair of elements $(m_1, m_2) \in \mathrm{Sel}_{\varphi_n\times\hat{\varphi_n}}(E_n \times E_n^{-3}/K)^{\oplus 2}$, the first part of the theorem implies that the pairing Q_n can be characterized by the products of

Hilbert norm residue symbol Cassels 1959, Chapter 10, Appendix B

$$Q_n(m_1, m_2) := \prod_{\substack{\mathfrak{p}|3n \\ \mathfrak{p}\not\equiv 1 \bmod 3}} (\tilde{\ell}\ell_{m_1},\ m_2)_{\mathfrak{p}} \tag{4.117}$$

where $\tilde{\ell} \in M^{\times}$ is some choice of an auxiliary number (this is not the fixed prime number ℓ which was used until the previous section), and $\ell_{m_1} \in M_v^{\times}$ is any element which satisfies the condition that

$$\ell_{m_1} \cdot \frac{\sigma_3(\alpha)}{\sigma_3^2(\alpha)} = F_3(\tilde{m}_1) \tag{4.118}$$

with respect to the morphism $F_3 : M_{\mathfrak{p}}^{\times}/(M_{\mathfrak{p}}^{\times})^3 M_{\mathfrak{p}}^{\times}/(M_{\mathfrak{p}}^{\times})^3$ and some element $\alpha \in L^{\times}/(L^{\times})^3$ such that $\mathrm{Norm}_M^L(\alpha) = m_1$, defined as in Cassels 1959, Lemma 4. We summarize the construction of the map F_3. Any element $m_1 \in \mathrm{Sel}_{\varphi_n \times \hat{\varphi}_n}(E_n \times E_n^{-3}/K)$ can be identified with a triple $(m_x, m_y, m_z) \in M_{\mathfrak{p}}^3$ given by the formulae Cassels 1959, Lemma 0

$$\begin{aligned} x &= \frac{\zeta_3^2}{m_1} X^3 + \zeta_3 m_1 Y^3 + nZ^3 \\ y &= \frac{\zeta_3}{m_1} X^3 + \zeta_3^2 m_1 Y^3 + nZ^3 \\ z &= -3XYZ \end{aligned} \tag{4.119}$$

where $(X, Y, Z) \in M_{\mathfrak{p}}^3$ is an $M_{\mathfrak{p}}$-rational point of the curve

$$\frac{1}{m_1} X^3 + m_1 Y^3 + nZ^3 = 0 \tag{4.120}$$

Then we define the map $F_3 : M_{\mathfrak{p}}^{\times}/(M_{\mathfrak{p}}^{\times})^3 \to M_{\mathfrak{p}}^{\times}/(M_{\mathfrak{p}}^{\times})^3$ as

$$F_3((m_x, m_y, m_z)) := \frac{(\zeta_3 - \zeta_3^2)(y + z\sqrt[3]{n})}{x + y} \tag{4.121}$$

It follows from the construction of ℓ_{m_1} that if $\mathfrak{p} \neq (3)$, then one obtains the identification

Cassels 1959, Appendix B

$$\ell_{m_1} = \zeta_3^{-t_n(m_1,\mathfrak{p})} \cdot \tilde{m}_{1\mathfrak{p}} \tag{4.122}$$

for some element $\tilde{m}_{1\mathfrak{p}}$ which satisfies $(\tilde{m}_{1\mathfrak{p}},\ m_2)_{\mathfrak{p}} = 1$, and $t_n(m_1, \mathfrak{p}) := \frac{v_{\mathfrak{p}}(n)}{v_{\mathfrak{p}}(m_1)} \bmod 3$. This in particular implies that one can rewrite the pairing Q_n as

$$Q_n(m_1, m_2) = \mathfrak{n} \cdot \prod_{\substack{\mathfrak{p}|m_1 \\ \mathfrak{p}\not\equiv 0,1 \bmod 3,}} (\zeta_3^{t_n(m_1,\mathfrak{p})},\ m_2)_{\mathfrak{p}} \cdot (\tilde{\ell}\ell_{m_1},\ m_2)_3 \tag{4.123}$$

for some fixed $\mathfrak{n} \in \mu_3$ independent of the choice of m_1 and m_2. Here, the notation $(-,-)_{\mathfrak{p}} : M_{\mathfrak{p}}^{\times}/M_{\mathfrak{p}}^{\times})^3 \times M_{\mathfrak{p}}^{\times}/(M_{\mathfrak{p}}^{\times})^3 \to \mu_3$ is the Hilbert cubic norm residue symbol over $M_{\mathfrak{p}}$. But because every element $m_2 \in \mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^3$ becomes a cube in $M_{\mathfrak{p}}$ where $\mathfrak{p} \equiv 2 \bmod 3$, it follows that if $m_1 \neq m_2$ (note that because Q_n is a skew-symmetric pairing, $Q_n(m_1, m_2) = 1$), then the pairing Q_n can be further simplified into

$$Q_n(m_1, m_2) = \mathfrak{n} \cdot (\tilde{\ell}\ell_{m_1},\ m_2)_3. \tag{4.124}$$

But notice that if $m_2 \equiv 8 \bmod 9$, then $K_3(\sqrt[3]{m_2}) = K_3$, whereas $m_2 \equiv 2, 5 \bmod 9$, then $K_3(\sqrt[3]{m_2}) \neq K_3$. Therefore, we obtain that

$$Q_n(m_1, m_2) = 1, \text{ for any } m_2 \text{ place of } M \text{ such that } m_2 \equiv 8 \bmod 9. \tag{4.125}$$

Denote by $w_8(n)$ the number of prime divisors of n which are equivalent to 8 mod 9. Then

$$\mathrm{Ker}(Q_n) \geq w_8(n) - 1. \tag{4.126}$$

Recall that we let $Q_L : \mathrm{Sel}_3(B_{L/K}/K) \times \mathrm{Sel}_3(B_{L/K}/K) \to \mathbb{F}_3$ be the Cassels-Tate pairing over the abelian 4-fold $B_{L/K}$. Then it follows that

$$\dim_{\mathbb{F}_3} \mathrm{Ker}(Q_L) = \dim_{\mathbb{F}_3} \mathrm{Ker}(Q_n) + \dim_{\mathbb{F}_3} \mathrm{Ker}(Q_{n^2}) - 1 \tag{4.127}$$

Using (4.126), we hence obtain that

$$\dim_{\mathbb{F}_3} \mathrm{Ker}(Q_L) \geq (w_8(n) - 1) + (w_8(n^2) - 1) - 1 = 2 \cdot w_8(n) - 3. \tag{4.128}$$

□

Remark 4.4.5. The proof of the first part of Theorem 4.4.1 can also be obtained from the result by Stephanie Chan Chan 2022, where she shows using large sieves on cubic residue symbols that for every $\epsilon > 0$,

$$\dim_{\mathbb{F}_3} \mathrm{Sel}_{\varphi_n}(E_n/K) = \dim_{\mathbb{F}_3} \mathrm{Sel}_{\hat{\varphi}_n}(E_n^{-3}/K) + w_2^*(n) + \delta_n \tag{4.129}$$

$$\#\left\{n \in \mathbb{Z} \mid |n| \leq X, n \text{ cubefree}, \dim_{\mathbb{F}_3} \mathrm{Sel}_{\hat{\varphi}_n}(E_n/K) \geq 1\right\} \ll \frac{X}{(\log X)^{-\frac{1}{3}+\epsilon}} \tag{4.130}$$

where

$$w_2^*(n) = \begin{cases} w_2(2n) & \text{if } 4 \nmid n \\ w_2(\frac{n}{4}) & \text{if } 4 \mid n \end{cases} \tag{4.131}$$

and

$$\delta_n = \begin{cases} 1 & \text{if } n \equiv \pm 3 \bmod 9 \\ -1 & \text{if } n \equiv \pm 4 \bmod 9 \\ 0 & \text{otherwise} \end{cases} \tag{4.132}$$

Using the identification

$$\mathrm{Sel}_{\varphi_n \times \hat{\varphi}_n}(E_n \times E_n^{-3}/K) \cong \mathrm{Sel}_{\varphi_n}(E_n/K) \oplus \mathrm{Sel}_{\varphi_n}(E_n^{-3}/K), \tag{4.133}$$

one can hence demonstrate an alternate proof Theorem 4.4.1 that the dimension of $\mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K)$ grows at an order of $O(\log\log D_{L/K})$.

Remark 4.4.6. Denote by $\mathcal{Q} := \{Q_n\}_n$ the collection of Cassels-Tate pairing over $\mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K)$. Note that Theorem 4.4.1 and Erdös-Kac theorem indicates that except for possibly $O(\frac{X}{\sqrt{\log\log X}})$ many exceptions, all Cassels-Tate pairing Q_n with $|n| \leq X$ can be

identified as an element of skew-symmetric matrices $Skew_k(\mathbb{F}_3)$ for some $k \leq \lfloor \log\log X \rfloor + 1$. We may subdivide the collection $\mathcal{Q}$ as

$$\mathcal{Q} := \bigsqcup_{k=1}^{\infty} \mathcal{Q}^{[k]} \subset \bigsqcup_{k=1}^{\infty} Skew_k(\mathbb{F}_3) \tag{4.134}$$

$$\mathcal{Q}^{[k]} := \left\{ Q_n : \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) \times \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) \to \mathbb{F}_3 \mid \dim_{\mathbb{F}_3} \mathrm{Sel}_{1-\sigma_3}(B_{L/K}/K) = k \right\} \tag{4.135}$$

$$\mathcal{Q}^{[k]}(X) := \left\{ Q_n \in \mathcal{Q}^{[k]} \mid |n| \leq X \right\} \tag{4.136}$$

If one can demonstrate that the pushforward of the uniform distribution over $\mathcal{Q}^{[k]}(X)$ with respect to the morphism $\mathcal{Q}^{[k]}(X) \to Skew_k(\mathbb{F}_3)$ converges in distribution to the uniform distribution over $Skew_k(\mathbb{F}_3$, then one can also prove the upper bound on $\mathrm{Ker}(Q_n)$ using Bhargava, D. M. Kane, et al. 2015, Lemma 3.7. Namely, for any $\delta > 0$, there exists large enough X such that for almost all $|n| \leq X$,

$$\dim_{\mathbb{F}_3} \mathrm{Ker}(Q_n) \leq \left(\frac{1}{3} + \delta \right) \cdot \log\log X \tag{4.137}$$

It seems to be the case that demonstrating the convergence to a uniform distribution over $Skew_k(\mathbb{F}_3)$ would require equidistribution or sieve results on Hilbert cubic norm residue symbols over the local field $\mathbb{Q}_3$. To the best of author's knowledge, the results of such nature has not been studied in great depth yet.

For the rest of the remark, let us assume that obtaining such an equidistribution of Hilbert cubic norm residue symbols is within reach. While the above upper bound obtained from the Kernel of Cassels-Tate pairing is also not good enough to determine $\mathrm{Rank}_{\mathbb{Z}}(B_{L/K}(K))$, it is still a better upper bound than what can be obtained from the dimension of $1-\sigma_3$ Selmer groups of $B_{L/K}$. One may hence hope to see whether using the collections of Cassels-Tate pairing

$$Q_n^{[m]} : (1-\sigma_3)^m \mathrm{Sel}_{(1-\sigma_3)^{m+1}}(B_{L/K}/K) \times (1-\sigma_3)^m \mathrm{Sel}_{(1-\sigma_3)^{m+1}}(B_{L/K}/K) \to \mu_3 \tag{4.138}$$

could be of advantage to give effective upper bounds on $\mathrm{Rank}_{\mathbb{Z}}(B_{L/K}(K))$. This very idea of using sequences of Cassels-Tate pairing was carefully explored for quadratic twist families of elliptic curves over number fields K in the seminal work by Alex Smith Alexander Smith 2022a; Alexander Smith 2022b. To the best of author's knowledge, the upcoming work by Peter Koymans and Alex Smith Koymans and Alex Smith 2024 will aim to generalize the philosophy presented in the previous works of Smith, identify the Cassels-Tate pairing as a generalized form of Redei matrices (i.e. entries with a generalized notion of "symbols of primes" appearing in Alexander Smith 2022a, Chapter 3), and demonstrate that the 3-Selmer groups of cubic twist families of elliptic curves E_n (not the abelian 4-fold $B_{L/K}$ discussed in this manuscript) lying inside certain grid classes of cubic twists can be effectively controlled with careful choices of symbols of primes.

4.5 Global root numbers of cubic twists

We recall from Alpöge, Bhargava, and Shnidman 2022[Chapter 4], Várilly-Alvarado 2011, and Rohrlich 1996 that the root number of $E_n : y^2 = x^3 - 432n^2$, apart from local conditions at 2 and 3, is equal to $(-1)^{w_2(n)}$, where w_2 is the number of prime factors of n equivalent to 2 mod 3. In fact, one can prove the following fact on the relations between root numbers of E_n and E_{n^2}.

Proposition 4.5.1. *Given an elliptic curve E over $\mathbb{Q}$, denote by $W(E/\mathbb{Q})$ the global root number of E. Let n be any integer, and denote by $w_2(n)$ the number of distinct prime factors of n equivalent to 2 modulo 3.*

1. *If $v_3(n) \equiv 0$ mod 3, then*

$$W(E_n/\mathbb{Q}) = W(E_{n^2}/\mathbb{Q}) = (-1)^{w_2(n)} \cdot \delta(n) \tag{4.139}$$

where $\delta : \mathbb{Z} \to \{-1, 1\}$ *is a function such that*

$$\delta(n) = \begin{cases} 1 & \text{if } n \equiv 1, 8 \text{ mod } 9 \\ -1 & \text{if } n \equiv 2, 4, 5, 7 \text{ mod } 9 \end{cases} \tag{4.140}$$

2. If $v_3(n) \equiv 1 \text{ mod } 3$*, then*

$$W(E_n/\mathbb{Q}) = -W(E_{n^2}/\mathbb{Q}) = (-1)^{w_2(n)}. \tag{4.141}$$

3. If $v_3(n) \equiv 2 \text{ mod } 3$*, then*

$$W(E_n/\mathbb{Q}) = -W(E_{n^2}/\mathbb{Q}) = (-1)^{w_2(n)+1}. \tag{4.142}$$

In particular, Proposition 4.5.1 and Erdös-Kac theorem affirm the equidistribution of root numbers in the family of cubic twists $\{E_n\}$ as shown in Alpöge, Bhargava, and Shnidman 2022, Section 6.

Proof. The proof follows from the table of root numbers of elliptic curves over $\mathbb{Q}$ outlined in Rohrlich 1996 for local root numbers at places $p \neq 2, 3$ and Rizzo 2003 for local root numbers at places $p = 2$ or 3. The local root number at the place of infinity ∞ is equal to -1. The local root numbers at every finite prime $p \neq 2, 3$ are given by

$$W(E_n/\mathbb{Q}, p) = \left(\frac{p}{3}\right). \tag{4.143}$$

Local root number at $p = 3$.

Fix $p = 3$. Suppose $v_3(n) \equiv 0 \bmod 3$. Using entries $(\geq 4, 6, 9), (4, 6, 9)$, and $(\geq 5, 6, 9)$ of Rizzo 2003[Table 3], the local root number at place $p = 3$ can be shown to be equal to

$$W(E_n/\mathbb{Q}, 3) = \begin{cases} 1 \text{ if } -2^9 \cdot n^2 \equiv 4, 7 \bmod 9 \\ -1 \text{ if } -2^9 \cdot n^2 \equiv 1 \bmod 9 \end{cases} \tag{4.144}$$

Because n is not divisible by 3, we obtain that

$$W(E_n/\mathbb{Q}, p) = -\delta(n). \tag{4.145}$$

Suppose $v_3(n) \equiv 1 \bmod 3$. Then entry $(\geq 2, 2, 1)$ of Rizzo 2003[Table 3] implies that $W(E_n/\mathbb{Q}, 3) = 1$ because the very condition holds if and only if $-2^9 \cdot n^2 \equiv 1 \bmod 3$ is true. Suppose $v_3(n) \equiv 2 \bmod 3$. Then entry $(\geq 3, 4, 5)$ of Rizzo 2003[Table 3] implies that $W(E_n/\mathbb{Q}, 3) = -1$ because the very condition holds if and only if $-2^9 \cdot n^2 \equiv 2 \bmod 3$.

Local root number at $p = 2$.

Suppose $v_2(n) \equiv 0 \bmod 3$. Then E_n has good reduction at 2, so the local root number at $p = 2$ is equal to 1. Suppose $v_2(n) \equiv 1 \bmod 3$. Then the first entry of $(4, 5, 4)$ of Rizzo 2003[Table 3] implies that $W(E_n/\mathbb{Q}, 2) = -1$ because the very condition holds if and only if $0 \equiv 1 \bmod 4$. Suppose $v_2(n) \equiv 2 \bmod 3$. Then entry $(\geq 7, 7, 8)$ of Rizzo 2003[Table 3] implies that $W(E_n/\mathbb{Q}, 2) = -1$. In particular, we achieve

$$W(E_n/\mathbb{Q}, 2) = \begin{cases} 1 \text{ if } 2 \nmid n \\ -1 \text{ if } 2 \mid n. \end{cases} \tag{4.146}$$

Using the fact that the global root number of E is the product of all local root numbers at every place ℓ of $\mathbb{Q}$, we obtain the desired formulae. □

We note that the properties Markov operator M defined in the proof of Theorem 4.4.1 conforms to the properties of global root numbers. Theorem 4.4.1 implies that the Markov operator corresponding to twisting the abelian variety $B_{L/K}$ by a prime $p \equiv 2 \bmod 3$ always increases the dimension of $1 - \sigma_3$ Selmer groups by 2. On the other hand, the Markov operator corresponding to twisting the abelian variety $B_{L/K}$ by a prime $p \equiv 1 \bmod 3$ preserves the dimension of $1 - \sigma_3$ Selmer groups of $B_{L/K}$. Assuming the BSD conjecture, Proposition 4.5.1 implies that the Markov operator corresponding to twisting the abelian variety $B_{L/K}$ by a prime $p \equiv 2 \bmod 3$ must simultaneously increase the ranks $\mathrm{Rank}(E_n(\mathbb{Q}))$

and $\mathrm{Rank}(E_{n^2}(\mathbb{Q}))$ by 1 or decrease them by -1, and that corresponding to twisting the abelian variety $B_{L/K}$ by a prime $p \equiv 1 \bmod 3$ must simultaneously decrease the ranks $\mathrm{Rank}(E_n(\mathbb{Q}))$ and $\mathrm{Rank}(E_{n^2}(\mathbb{Q}))$ by 2 or preserve them. These changes, in turn, correspond to the statement of Proposition 4.5.1 that up to local conditions at 2 or 3, the global root number is determined by the parity of the number of distinct prime factors equivalent to 2 modulo 3.

In light of these observations from global root numbers of E_n's, we may hope formulate the following conjecture.

Conjecture 4.5.2. *Let $B_{L/K}$ be the 4-dimensional abelian variety over $K = \mathbb{Q}$ obtained from the S_3 extension $L = \mathbb{Q}(\zeta_3, \sqrt[3]{n})$.*

1. *The $(1-\sigma_3)^\infty$ torsion subgroup of the Tate Shafarevich group of $B_{L/K}$ satisfies $\dim_{\mathbb{Z}_3} Ш_{B_{L/K}/\mathbb{Q}}[(1-\sigma_3)^\infty] \equiv 0 \bmod 4$.*

2. *Suppose that 3 does not divide n. Then $Rank_{\mathbb{Z}_3}\mathrm{Sel}_{(1-\sigma_3)^\infty}(B_{L/K}/\mathbb{Q}) \equiv 0 \bmod 2$. In particular, one obtains the following probability distribution on the rank of $(1-\sigma_3)^\infty$ Selmer groups of $\{B_{L/K}\}$ for such L/K.*

$$\begin{aligned}
\lim_{X\to\infty} \frac{\#\{n \in \mathbb{Z} \mid |n| \le X,\ Rank_{\mathbb{Z}_3}\mathrm{Sel}_{(1-\sigma_3)^\infty}(B_{L/K}/\mathbb{Q}) = 0\}}{\#\{n \in \mathbb{Z} \mid |n| \le X\}} &= \frac{1}{2} \\
\lim_{X\to\infty} \frac{\#\{n \in \mathbb{Z} \mid |n| \le X,\ Rank_{\mathbb{Z}_3}\mathrm{Sel}_{(1-\sigma_3)^\infty}(B_{L/K}/\mathbb{Q}) = 2\}}{\#\{n \in \mathbb{Z} \mid |n| \le X\}} &= \frac{1}{2} \\
\lim_{X\to\infty} \frac{\#\{n \in \mathbb{Z} \mid |n| \le X,\ Rank_{\mathbb{Z}_3}\mathrm{Sel}_{(1-\sigma_3)^\infty}(B_{L/K}/\mathbb{Q}) \ge 4\}}{\#\{n \in \mathbb{Z} \mid |n| \le X\}} &= 0
\end{aligned} \tag{4.147}$$

3. *Suppose that 3 divides n. Then $Rank_{\mathbb{Z}_3}\mathrm{Sel}_{(1-\sigma_3)^\infty}(B_{L/K}/\mathbb{Q}) \equiv 1 \bmod 2$. In particular, one obtains the following probability distribution on the rank of $(1-\sigma_3)^\infty$ Selmer groups of $\{B_{L/K}\}$ for such n.*

$$\begin{aligned}
\lim_{X\to\infty} \frac{\#\{n \in \mathbb{Z} \mid |n| \le X,\ Rank_{\mathbb{Z}_3}\mathrm{Sel}_{(1-\sigma_3)^\infty}(B_{L/K}/\mathbb{Q}) = 1\}}{\#\{n \in \mathbb{Z} \mid |n| \le X\}} &= 1 \\
\lim_{X\to\infty} \frac{\#\{n \in \mathbb{Z} \mid |n| \le X,\ Rank_{\mathbb{Z}_3}\mathrm{Sel}_{(1-\sigma_3)^\infty}(B_{L/K}/\mathbb{Q}) \ge 3\}}{\#\{n \in \mathbb{Z} \mid |n| \le X\}} &= 0
\end{aligned} \tag{4.148}$$

Recall the following conjecture proposed by Alpöge, Bhargava, and Shnidman Alpöge, Bhargava, and Shnidman 2022.

Conjecture 4.5.3. *For sufficiently large X, the following equation holds.*

$$\begin{aligned}
\lim_{X\to\infty} \frac{\#\{n\in\mathbb{Z} \mid |n|\leq X,\ \mathit{Rank}(E_n(\mathbb{Q}))=0\}}{\#\{n\in\mathbb{Z} \mid |n|\leq X\}} &= \frac{1}{2}\\
\lim_{X\to\infty} \frac{\#\{n\in\mathbb{Z} \mid |n|\leq X,\ \mathit{Rank}(E_n(\mathbb{Q}))=1\}}{\#\{n\in\mathbb{Z} \mid |n|\leq X\}} &= \frac{1}{2}\\
\lim_{X\to\infty} \frac{\#\{n\in\mathbb{Z} \mid |n|\leq X,\ \mathit{Rank}(E_n(\mathbb{Q}))\geq 2\}}{\#\{n\in\mathbb{Z} \mid |n|\leq X\}} &= 0
\end{aligned} \tag{4.149}$$

We end the paper with a note that Conjecture 4.5.2 implies Conjecture 4.5.3 assuming the BSD conjecture for elliptic curves over $\mathbb{Q}$.

Proposition 4.5.4. *Assumign the BSD conjecture for elliptic curves over $\mathbb{Q}$, the statement of Conjecture 4.5.2 implies that of Conjecture 4.5.3.*

Proof. Proposition 4.5.1 implies that the root number is equidistributed in the family of cubic twists $\{E_n\}_{n\in\mathbb{Z}}$. In fact, the root number is equidistributed in the subfamily of cubic twists $\{E_n\}_{\substack{n\in\mathbb{Z}\\ v_3(n)\equiv i \bmod 3}}$ for any fixed $i=0,1,2$. The BSD conjecture hence implies that for any fixed $0\leq i\leq 2$, $\frac{1}{2}$ of elliptic curves $\{E_n\}_{\substack{n\in\mathbb{Z}\\ v_3(n)\equiv i \bmod 3}}$ have even ranks, whereas the other $\frac{1}{2}$ of elliptic curves $\{E_n\}_{\substack{n\in\mathbb{Z}\\ v_3(n)\equiv i \bmod 3}}$ have odd ranks.

Part (2) and (3) of Conjecture 4.5.2 imply that at least $\frac{5}{9}\cdot\frac{1}{2}+\frac{4}{9}\cdot\frac{1}{2}=\frac{1}{2}$ of elliptic curves $\{E_n\}_{n\in\mathbb{Z}}$ must have rank 0. These elliptic curves are comprised of 100% of elliptic curves which satisfy $\mathrm{Rank}(E_n(\mathbb{Q}))+\mathrm{Rank}(E_{n^2}(\mathbb{Q}))=0$, and 50% of elliptic curves which satisfy $\mathrm{Rank}(E_n(\mathbb{Q}))+\mathrm{Rank}(E_{n^2}(\mathbb{Q}))=2$. Therefore, it must be the case that 100% of ellitpic curves $\{E_n\}_{n\in\mathbb{Z}}$ which satisfy $\mathrm{Rank}(E_n(\mathbb{Q}))+\mathrm{Rank}(E_{n^2}(\mathbb{Q}))=2$ must have rank 1. This implies that 50% of elliptic curves have rank 0, whereas the other 50% of elliptic curves have rank 1. □

Bibliography

Park, Sun Woo (2022). "On the prime Selmer ranks of cyclic prime twist families of elliptic curves over global function fields". In: *Preprint available at: https://arxiv.org/abs/2211.11486*.

— (2024a). "A geometric approach to prime Selmer groups of cyclic prime twist families of elliptic curves". In: *In preparation*.

— (2024b). "Remarks on rank growths of elliptic curves over some non-abelian Galois extensions". In: *In preparation*.

Katz, Nicholas M. and Barry Mazur (1985). *Arithmetic Moduli of Elliptic Curves*. Vol. 108. Princeton University Press. URL: https://doi.org/10.1515/9781400881710.

Katz, Nicholas (1998). "Twisted L-Functions and Monodromy". In: *Princeton University Press*, pp. 79–116. URL: https://web.math.princeton.edu/%20nmk/twistedLfctnov052001.pdf.

Poonen, Bjorn and Eric Rains (2012). "Random maximal isotropic subspaces and Selmer groups". In: *Journal of the AMS* 25.1, pp. 245–269.

Bhargava, Manjul, Daniel M. Kane, et al. (2015). "Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves". In: *Cambridge Journal of Mathematics* 3.3, pp. 275–321.

Howe, Everett W. (2001). "Isogeny classes of abelian varieties with no principal polarizations". In: *Moduli of Abelian Varieties (Texel Island, 1999), Birkhauser Progress in Mathematics*, pp. 203–216.

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

— (2014). "A Markov model for Selmer ranks in families of twists". In: *Compositio Mathematica* 150, pp. 1077–1106.

Mazur, Barry and Karl Rubin (2007). "Finding large Selmer rank via an arithmetic theory of local constants". In: *Annals of Mathematics* 166, pp. 579–612.

Mazur, Barry, Karl Rubin, and Alice Silverberg (2007). "Twisting commutative algebraic groups". In: *Journal of Algebra* 314.1, pp. 419–438.

Milne, J.S. (2006). *Arithmetic Duality Theorems*. Second. BookSurge, LLC, pp. 1–138. ISBN: 1-4196-4274-X.

Igusa, J.-I. (1959). "Fibre systems of jacobian varieties (III. Fibre systems of elliptic curves)". In: *American Journal of Mathematics* 81, pp. 453–476.

Bandini, Andrea, Ignazio Longhi, and Stefano Vigni (2009). "Torsion points on elliptic curves over function fields and a theorem of Igusa". In: *Expositiones Mathematicae* 27.3, pp. 175–209.

Bhargava, Manjul and Arul Shankar (2015). "Binary quadratic forms having bounded invariants, and the boundedness of the average rank of elliptic curves". In: *Annals of Mathematics* 181, pp. 1–52.

Heath-Brown, D.R. (1994). "The size of Selmer groups for the congruent number problem, II". In: *Inventiones mathematicae* 118, pp. 331–370.

Swinnerton-Dyer, Peter (2008). "The effect of twisting on the 2-Selmer group". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 145.3, pp. 513–526.

Kane, Daniel (2013). "On the ranks of the 2-Selmer groups of twists of a given elliptic curve". In: *Algebra and Number Theory* 7.5, pp. 1253–1279.

Smith, Alexander (2017). "2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture". In: *Preprint available at https://arxiv.org/abs/1702.02325*.

— (2020). "l^∞-Selmer groupsin degree l twist families". In: *Doctoral dissertation, Harvard University*.

— (2022a). "The distribution of l^∞ Selmer groups in degree l twist families". In: *Preprint available at https://arxiv.org/abs/2207.05674*.

— (2022b). "The distribution of fixed point Selmer groups in twist families". In: *Preprint available at https://arxiv.org/pdf/2207.05143.pdf*.

Koymans, Peter and Carlo Pagano (2021). "On the distribution of $Cl(K)[l^\infty]$ for degree l cyclic fields". In: *Journal of the European Mathematical Society* 24.4, pp. 1189–1283.

— (2022). "On Stevenhagen's conjecture". In: *Preprint available at https://arxiv.org/pdf/2201.13424.pdf*.

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

Jong, A.J. de (2002). "Counting elliptic surfaces over finite fields". In: *Moscow Mathematical Journal* 2, pp. 281–311.

Feng, Tony, Aaron Landesman, and Eric Rains (2023). "The geometric distribution of Selmer groups of elliptic curves over function fields". In: *Mathematische Annalen* 387, pp. 615–687.

Landesman, Aaron (2021). "The geometric average size of Selmer groups over function fields". In: *Algebra and Number Theory* 15.3, pp. 673–709.

Park, Sun Woo and Niudun Wang (2023). "On the average of p-Selmer rank in quadratic twist families of elliptic curves over function field". In: *International Mathematics Research Notices*, rnad095.

Jong, A.J. de and Robert Friedman (2011). "On the geometry of principal homogeneous spaces". In: *American Journal of Mathematics* 133.3, pp. 753–796.

Hall, Chris (2006). "Big symplectic or orthogonal monodromy modulo l". In: *Duke mathematics journal* 141.1, pp. 179–203.

Ellenberg, Jordan, Akshay Venkatesh, and Craig Westerland (2016). "Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields". In: *Annals of Mathematics* 183, pp. 729–786.

Klagsbrun, Zev and Robert J. Lemke Oliver (2015). "The distribution of 2-Selmer ranks of quadratic twists of elliptic curves with partial two-torsion". In: *Mathematika* 62.1, pp. 67–78.

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

Stein, William (2002). “Shafarevich-Tate Groups of Nonsquare Order”. In: *Modular Curves and Abelian Varieties 2002 Barcelona Conference Proceedings, Birkhauser Progressin Mathematics* 224, pp. 277–289.

David, Chantal, Jack Fearnley, and Hershy Kisilevsky (2007). “Vanishing of L-functions of elliptic curves over number fields, Ranks of elliptic curves and random matrix theory”. In: *London Math. Soc. Lecture Note Series* 341, pp. 247–259.

Mazur, Barry and Karl Rubin (2019). “Arithmetic conjectures suggested by the statistical behavior of modular symbols”. In: *To appear in Experimental Mathematics*. URL: https://arxiv.org/abs/1910.12798.

Comeau-Lapointe, Antoine et al. (2022). “On the vanishing of twisted L-functions of elliptic curves over rational function fields”. In: *Preprint*. URL: https://arxiv.org/abs/2207.00197.

Fried, Michael D. and Moshe Jarden (2008). *Field Arithmetic*. Berlin, Germany: Springer, pp. 52–131.

Lagarias, J. and A. Odlyzko (1975). “Effective versions of the Chebotarev density theorem”. In: *Proceedings of Symposia in Pure Mathematics*, pp. 409–464.

Rosen, Michael (2002). *Number theory in function fields*. Berlin, Germany: Springer, pp. 115–147.

Liu, Yu-Ru (2004). “A generalization of the Erdos-Kac Theorem and its applications”. In: *Canadian Mathematical Bulletin* 48.4, pp. 589–606.

Feng, Tingting, Shaochen Wang, and Guangyu Yang (2020). “Large and moderate deviation principles for the Erdos-Kac theorem in function fields”. In: *Statistics and probability letters* 163.

Cohen, Stephen D. (1969). “Further arithmetical functions in finite fields”. In: *Proceedings of the Edinburgh Mathematical Society* 16, pp. 349–363.

Cheong, Gilyoung et al. (2022). “Jordan–Landau theorem for matrices over finite fields”. In: *Linear Algebra and its Applications* 655, pp. 100–128.

Hsu, Chih-Nung (1998). “On certain character sums over $\mathbb{F}_q[T]$”. In: *Proceedings of the American Mathematical Society* 126.3, pp. 647–652.

Friedlander, J.B. et al. (2013). “The spin of prime ideals”. In: *Inventiones Mathematicae*, pp. 697–749.

Meyn, Sean and Richard Tweedie (1993). *Markov chains and stochastic stability*. Berlin, Germany: Springer-Verlag, pp. 354–381.

Hall, Chris (2008). “Big Symplectic Or Orthogonal Monodromy Modulo l”. In: *Duke Math. J.* 141.1, pp. 179–203.

Ellenberg, Jordan, TriThang Tran, and Craig Westerland (2023). “Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and Malle’s conjecture for function fields”. In: *Preprint available at https://arxiv.org/abs/1701.04541*.

Ellenberg, Jordan and Aaron Landesman (2023). “Homological stability for generalized Hurwitz spaces and Selmer groups in quadratic twist families over function fields”. In: *Preprint available at https://arxiv.org/pdf/2310.16286.pdf*.

Kupers, Alexander, Jeremy Miller, and Trithang Tran (2016). “Homological stability for symmetric complements”. In: *Transactions of the American Mathematical Society* 368.11, pp. 7745–7762.

Palmer, Martin (2018). “Twisted homological stability for configuration spaces”. In: *Homology, homotopy, and applications* 20.2, pp. 145–178.

Ogg, Andrew (1962). "Cohomology of Abelian Varieties Over Function Fields". In: *Annals of Mathematics* 76.2, pp. 185–212.

Cesnavicius, Kestutis (2016). "Selmer groups as flat cohomology groups". In: *J. Ramanujan Math. Soc.* 31.1, pp. 31–61.

Billingsley, Patrick (1995). "Probability and Measure, 3rd Edition". In: *wiley series in probability and mathematical statistics*, pp. 388–400.

Sawin, Will and Melanie Matchett Wood (2022). "The moment problem for random objects in a category". In: *Arxiv preprint, available at https://arxiv.org/abs/2210.06279*.

Deligne, Pierre (1974). "La conjecture de Weil: I". In: *Publ. Math. Inst. Hautes Études Sci.* 43, pp. 273–307.

Bombieri, Enrico and Nicholas M. Katz (2010). "A note on lower bounds for Frobenius traces". In: *L'Enseignement Mathematique* 56.2, pp. 203–227.

Chan, Stephanie (2022). "The 3-isogeny Selmer groups of the elliptic curves $y^2 = x^3 + n^2$". In: *Preprint available at https://arxiv.org/pdf/2211.06062.pdf*.

Koymans, Peter and Alex Smith (2024). "To be determined". In: *Work in progress*.

Keliher, Daniel and Sun Woo Park (2024). "Rank growth of elliptic curves over S_3 extensions with fixed quadratic resolvents". In: *Work in progress*.

Alpöge, Levent, Manjul Bhargava, and Ari Shnidman (2022). "Integers expressible as the sum of two rational cubes, with an appendix by Ashay Burungale and Christopher Skinner". In: *Preprint, available at https://arxiv.org/pdf/2210.10730.pdf*.

Cohen, H. and F. Pazuki (2009). "Elementary 3-descent with a 3-isogeny". In: *Acta Arithmetica* 140.4, pp. 369–404.

Cassels, J.W.S. (1959). "Arithmetic on Curves of Genus 1. I. On a conjecture of Selmer." In: *Journal für die reine und angewandte Mathematik* 202, pp. 52–99.

Várilly-Alvarado, A. (2011). "Density of rational points on isotrivial rational elliptic surfaces". In: *Algebra and Number Theory* 5.5, pp. 659–690.

Rohrlich, David E (1996). "Galois theory, elliptic curves, and root numbers". In: *Compositio Mathematica* 100.3, pp. 311–349.

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