Mathematische Annalen (2023) 387:615–687
https://doi.org/10.1007/s00208-022-02429-1

Mathematische Annalen

The geometric distribution of Selmer groups of elliptic curves over function fields

Tony Feng[1] · Aaron Landesman[2] · Eric M. Rains[3]

Received: 26 March 2020 / Revised: 23 December 2021 / Accepted: 13 June 2022 /
Published online: 13 September 2022

Abstract

Fix a positive integer n and a finite field $\mathbb{F}_q$. We study the joint distribution of the rank $\mathrm{rk}(E)$, the n-Selmer group $\mathrm{Sel}_n(E)$, and the n-torsion in the Tate–Shafarevich group $Ш(E)[n]$ as E varies over elliptic curves of fixed height $d \geq 2$ over $\mathbb{F}_q(t)$. We compute this joint distribution in the large q limit. We also show that the "large q, then large height" limit of this distribution agrees with the one predicted by Bhargava–Kane–Lenstra–Poonen–Rains.

Contents

1 Introduction

1.1 Arithmetic statistics of Selmer groups

The statistical behavior of Selmer groups has recently been the focus of much study. In [1], remarkable probability distributions are introduced to model the distribution of the n-Selmer group $\mathrm{Sel}_n(E)$, for E varying through isomorphism classes of elliptic curves over a fixed global field. We refer to the these distributions, and the models

✉ Aaron Landesman
aaronlandesman@gmail.com

[1] University of California, Berkeley, CA, USA

[2] Harvard University, Cambridge, MA, USA

[3] California Institute of Technology, Pasadena, CA, USA

which generate them, as the “BKLPR heuristic”. The BKLPR heuristic is consistent with all known results on the statistics of Selmer groups.

One can also consider the analogous question for elliptic curves over a global function field. The heuristics make sense in that case as well, and it is generally believed that in the “large height, then large q” limit, $\lim_{q\to\infty}\lim_{d\to\infty}$, the statistics of Selmer groups over global function fields should behave the same as in the case of number fields. For example, [10] computes the average size of 3-Selmer groups in this limit, and [19] computes the average size of 2-Selmer groups in this limit. Most notably, breakthrough work of Bhargava–Shankar [3–6] computes the average size of n-Selmer groups for elliptic curves over number fields for $n = 2, 3, 4, 5$; the methods are expected to extend to global function fields with the same answers (and without taking a large q limit!). The proofs of all these results rely on special features of small n, and confirming the BKLPR heuristic for the average size of Sel_n seems out of reach at present when $n > 5$. Our goal is to nevertheless provide some partial evidence for the full BKLPR heuristic, by studying an easier version of the problem.

To this end, we study the limiting process in the reversed order, $\lim_{d\to\infty}\lim_{q\to\infty}$ for elliptic curves over a rational function field $\mathbb{F}_q(t)$. This problem is significantly more accessible by algebraic geometry, which allows us to identify the distribution completely. Informally speaking, we show that in the “large q, then large height” limit, the distribution of $\mathrm{Sel}_n(E)$ is exactly as predicted by the BKLPR heuristic. A novel difficulty of this result is that it cannot be proved simply by computing and comparing the moments of the two distributions, because these distributions are not determined by their moments. Conversely, because the distribution is unbounded, convergence in distribution in the “large q, then large height” limit does not automatically imply convergence of the moments in these limits, though we do show the moments converge to the BKLPR moments as well.

1.2 Statement of results

1.2.1 Some notation

We now introduce notation in order to state our main results precisely. Let $p = \mathrm{char}(\mathbb{F}_q)$. For $p > 2$, an elliptic curve E over $\mathbb{F}_q(t)$ has a minimal Weierstrass model of the form

$$y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

where $a_i(t)$ is a polynomial of degree $2id$ for $i \in \{1, 2, 3\}$ (cf. [10, Sects. 4.2–4.8]). This value of d is uniquely determined by E, and we define $d =: h(E)$ to be the *height* of E. Let $(\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ denote the probability distribution assigning to a pair (r, G), for $r \in \mathbb{Z}$ and G a finite abelian group, the proportion of isomorphism classes of height d elliptic curves over $\mathbb{F}_q(t)$ with algebraic rank r and n-Selmer group isomorphic to G (see Definition 1.3).

1.2.2 The BKLPR heuristic

We summarize the BKLPR heuristic in Sect. 5.3. Briefly put, it models the distribution of the ℓ^∞-Selmer group in terms of the intersection in $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^m$ induced by two maximal isotropic subspaces of $\mathbb{Z}_\ell^m$ (with the standard split quadratic form) as $m \to \infty$. Conditioned on the rank, the ℓ-primary parts of the Selmer group are predicted to behave independently. This gives, in particular, a conjectural joint distribution $(\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}})$ for the rank and n-Selmer group of elliptic curves, described in Definition 5.12.

1.2.3 Main result

We consider the distribution $(\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ as a function on pairs (r, G), where $r \in \mathbb{Z}$ and G is an isomorphism class of finite abelian groups. Then we form

$$\limsup_{\substack{q\to\infty\\ \gcd(q,2n)=1}} (\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q} \quad \text{and} \quad \liminf_{\substack{q\to\infty\\ \gcd(q,2n)=1}} (\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$$

as functions on $\{(r, G)\}$.[1] (Note that because we are taking a pointwise lim inf or lim sup, the resulting function may no longer be a probability distribution, i.e., its sum over all (r, G) may not be 1.) Our main result is the following, which we deduce as a consequence of Theorems 6.1 and 6.4:

Theorem 1.1 *For fixed integers $d \geq 2$ and $n \geq 1$, and q ranging over prime powers, the limits*

$$\lim_{d\to\infty} \limsup_{\substack{q\to\infty\\ \gcd(q,2n)=1}} (rk, Sel_n)^d_{\mathbb{F}_q} \quad \textit{and} \quad \lim_{d\to\infty} \liminf_{\substack{q\to\infty\\ \gcd(q,2n)=1}} (rk, Sel_n)^d_{\mathbb{F}_q}$$

exist, are equal to each other, and coincide with the distribution predicted by the BKLPR heuristic.

As far as we are aware, our results give the first *direct* connection between the heuristics of [1] for general n and the arithmetic of elliptic curves. Further, our results suggest a potential approach to proving the conjectures of [1] in the function field setting via homological stability techniques as used in [13] to prove a version of the Cohen–Lenstra heuristics over function fields.

Remark 1.2 One can deduce a more precise version of Theorem 1.1 with estimates on the error terms in the above limits directly from Theorems 6.1 and 6.4. One may also deduce the same result holds with algebraic rank replaced by analytic rank. Further, one may include the joint distribution of Tate–Shafarevich groups—see Remark 1.8.

[1] To spell this out: the lim inf (resp. lim sup) of a distribution on the discrete set of $\{(r, G)\}$ is, by definition, the measure assigning to (r, G) the lim inf (resp. lim sup) of the probability that (r, G) occurs.

1.2.4 Summary of the main difficulties

Experts will recognize that the distribution in this "large q limit" is completely determined by certain monodromy representations. Letting $\mathscr{W}^{\circ d}_B$ be the "moduli space of smooth height d elliptic surfaces" (described more precisely in Sect. 3.3) the relevant monodromy representations take the form $\rho^d_{n,B} : \pi_1(\mathscr{W}^{\circ d}_B) \to \mathrm{GL}(V^d_n)$. Their significance lies in the fact that they control the number of connected components of moduli spaces parameterizing Selmer elements. Let us call the image of $\rho^d_{n,B}$ the *(arithmetic) monodromy group*, and the image of $\rho^d_{n,B}|_{\pi_1((\mathscr{W}^{\circ d}_B)_{\overline{\mathbb{F}}_q})}$ the *geometric monodromy group*.

Let us talk through some of the difficulties in proving Theorem 1.1 in order to orient the reader where the content of the paper lies. First, it is important that we determine the monodromy group precisely. If we had just wanted to compute the moments of Sel_n, then it would have been enough to know that the geometry monodromy group is "large enough". However, the behavior of the distribution depends more subtly on the arithmetic monodromy group. For example, it turns out that sometimes the Selmer distribution does not have a limit as $q \to \infty$, and this can happen even when q is taken only over powers of a fixed odd prime p. Nevertheless, both the "$\limsup_{q\to\infty}$" and the "$\liminf_{q\to\infty}$" exist, and tend towards each other as the height tends to ∞.

In a bit more detail, it is possible that for fixed height d, the Selmer distribution does not have a well defined limit as $q \to \infty$. Specifically, the $\limsup_{q\to\infty}$ and $\liminf_{q\to\infty}$ do not agree when, for an infinite sequence of q's over which the limits run, the *arithmetic* monodromy group contains an element of non-trivial spinor norm (see Sect. 3.2.2) but the *geometric* monodromy group does not. In this case, the arithmetic monodromy group fluctuates between two possibilities, which ends up creating a discrepancy between $\limsup_{q\to\infty}$ and $\liminf_{q\to\infty}$.

A second substantial issue is that even after having determined the monodromy representations that control the Selmer groups, it is not straightforward to identify the resulting distribution with the BKLPR heuristic. (To be clear, this is a purely combinatorial question, although it turns out to require techniques from algebraic geometry, number theory, etc. to address.) The reason for this difficulty is that the BKLPR heuristic is not described in terms of explicit closed formulas, but in terms of a random algebraic model. For example, it is not determined by its moments, as illustrated in Example 1.12 below. In order to compare the BKLPR distribution to the distribution coming from a monodromy representation, we introduce a "random kernel model" that mediates between the two distributions. We observe that both the BKLPR heuristic and the random kernel model enjoy Markov properties which reduce their comparison to simpler cases that can be computed explicitly, by matching enough moments. (Even this is a little oversimplified: what we need is to establish enough control on the moments already at a "finite height" level—see Sect. 4.)

1.2.5 Defining the random variables

In order to state the next results, we will need to introduce some more notation.

Let Ab_n denote the set of isomorphism classes of finite $\mathbb{Z}/n\mathbb{Z}$-modules. We will next define several distributions on $\mathbb{Z}_{\geq 0} \times \mathrm{Ab}_n$ modeling the joint distribution of the rank and n-Selmer group of an elliptic curves. For E an elliptic curve, we use $\mathrm{rk}(E)$ to denote the algebraic rank of E and $\mathrm{rk}^{\mathrm{an}}(E)$ to denote the analytic rank of E. In what follows, we use E to denote an isomorphism class of elliptic curves.

Definition 1.3 For $n, d \in \mathbb{Z}_{\geq 1}$ and k a finite field, let $(\mathrm{rk}, \mathrm{Sel}_n)_k^d$ and $(\mathrm{rk}^{\mathrm{an}}, \mathrm{Sel}_n)_k^d$ be the distributions on $\mathbb{Z}_{\geq 0} \times \mathrm{Ab}_n$ given by

$$\mathrm{Prob}((\mathrm{rk}, \mathrm{Sel}_n)_k^d = (r, G)) = \frac{\#\{E/k(t){:}h(E) = d, \mathrm{rk}(E) = r, \mathrm{Sel}_n(E) \simeq G\}}{\#\{E/k(t){:}h(E) = d\}}$$

$$\mathrm{Prob}((\mathrm{rk}^{\mathrm{an}}, \mathrm{Sel}_n)_k^d = (r, G)) = \frac{\#\{E/k(t){:}h(E) = d, \mathrm{rk}^{\mathrm{an}}(E) = r, \mathrm{Sel}_n(E) \simeq G\}}{\#\{E/k(t){:}h(E) = d\}},$$

where E varies over isomorphism classes of elliptic curves over $k(t)$. Also, define the distribution $\mathrm{Sel}_n^d/k(t)$ on Ab_n by

$$\mathrm{Prob}(\mathrm{Sel}_n^d/k(t) = G) = \frac{\#\{E/k(t){:}h(E) = d, \mathrm{Sel}_n(E) \simeq G\}}{\#\{E/k(t){:}h(E) = d\}}$$

and define the distributions $\mathrm{rk}^d/k(t)$, $\mathrm{rk}^{\mathrm{an},d}/k(t)$ on $\mathbb{Z}_{\geq 0}$ by

$$\mathrm{Prob}(\mathrm{rk}^d/k(t) = r) = \frac{\#\{E/k(t){:}h(E) = d, \mathrm{rk}(E) = r\}}{\#\{E/k(t){:}h(E) = d\}}$$

$$\mathrm{Prob}(\mathrm{rk}^{\mathrm{an},d}/k(t) = r) = \frac{\#\{E/k(t){:}h(E) = d, \mathrm{rk}^{\mathrm{an}}(E) = r\}}{\#\{E/k(t){:}h(E) = d\}}.$$

For a random variable X, we let $\mathbb{E}[X]$ be denote the expected value of X (if it exists).

Remark 1.4 In Definition 1.3, for the purposes of computing these distributions in the limit $q \to \infty$, we could equally well replace the condition $h(E) = d$ by the condition $h(E) \leq d$. The reason for this is that isomorphism classes of curves with $h(E) < d$ are parameterized by k points of the stack $\underline{\mathscr{W}'}^{i}_{k}$ (defined below in Sect. 2.1.5) for $i < d$, which is a finite type global quotient stack of strictly smaller dimension than $\underline{\mathscr{W}'}^{d}_{k}$. Hence, $\cup_{i \leq d} \underline{\mathscr{W}'}^{i}_{k}$ will only contributes at most $O_{n,d}(q^{-1/2})$ to the probability distributions in question, as can be deduced from the Lang–Weil estimate and [28, Lemma 5.3].

For analogous reasons, one can equally well weight the above counts by automorphisms (which would be the correct "stacky way" to count points) and the distribution in the $q \to \infty$ limit will remain the same. Note that after excising the locus of elliptic curves with more than 2 automorphisms, there will be a factor of one half in both the numerator and denominator in the definition of the distributions in Definition 1.3, which cancel out.

1.2.6 Some consequences

The following result (which is part of Corollary 6.5) is a variant of the Katz-Sarnak minimalist conjecture, stating that for fixed height, in the large q limit, the average rank is $1/2$. Moreover, in the large q limit, the rank takes value 1 and 0 with probability $1/2$, and takes value ≥ 2 with probability 0. It can also be deduced from [23, Theorem 13.3.3], though the more precise error terms given in Corollary 6.5 do not directly follow from [23, Theorem 13.3.3]. We note that the fact that elliptic curves in the large q limit have rank 0 with probability $1/2$ is not a direct consequence of Theorem 1.1, but it comes out of the more refined analysis used to prove Theorem 1.1 for $n = \ell$ a prime.[2]

Proposition 1.5 *(Large q analog of [33, Conjecture 1.2]) For fixed integers $d \geq 2$ and $n \geq 1$, we have*

$$\lim_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \operatorname{Prob}(\operatorname{rk}^d /\mathbb{F}_q(t) = r) = \begin{cases} 1/2 & \textit{if } r \leq 1, \quad (1.1) \\ 0 & \textit{if } r \geq 2. \quad (1.2) \end{cases}$$

Furthermore,

$$\lim_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \mathbb{E}[\operatorname{rk}^d /\mathbb{F}_q(t)] = 1/2.$$

The following calculation of the geometric moments of Selmer groups is a consequence of Corollary 6.6, which includes more precise error terms.

Theorem 1.6 *(Large q analog of [33, Conjecture 1.4]) Let n be a squarefree positive integer, $d \geq 2$, and $\omega(n)$ be the number of prime factors of n.*

(1) Fix $c_\ell \in \mathbb{Z}_{\geq 0}$ for each prime $\ell \mid n$. Then

$$\begin{aligned} &\lim_{d\to\infty} \limsup_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \operatorname{Prob}\left(\operatorname{Sel}_n^d /\mathbb{F}_q(t) \simeq \prod_{\ell \mid n} (\mathbb{Z}/\ell\mathbb{Z})^{c_\ell} \right) \\ &= \lim_{d\to\infty} \liminf_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \operatorname{Prob} \\ &\quad \times \left(\operatorname{Sel}_n^d /\mathbb{F}_q(t) \simeq \prod_{\ell \mid n} (\mathbb{Z}/\ell\mathbb{Z})^{c_\ell} \right) \qquad (1.3) \\ &= \begin{cases} 2^{\omega(n)-1} \prod_{\ell \mid n} \left(\left(\prod_{j\geq 0} (1-\ell^{-j})^{-1} \right) \left(\prod_{j=1}^{c_\ell} \frac{\ell}{\ell^j - 1} \right) \right) & \textit{if all } c_\ell \textit{ have the same parity,} \\ 0 & \textit{otherwise.} \end{cases} \end{aligned}$$

(2) We have

$$\lim_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \mathbb{E}[\#\operatorname{Sel}_n^d /\mathbb{F}_q(t)] = \sigma(n) := \sum_{s \mid n} s.$$

[2] However, the statement that elliptic curves in the large q limit have rank at least 2 with probability 0 does follow from just the computation of the average size of $\#\operatorname{Sel}_n$, see [28, Corollary 1.3].

(3) For $m \leq 6d - 3$*, we have*

$$\lim_{\substack{q\to\infty\\ \gcd(q,2n)=1}} \mathbb{E}[(\#\operatorname{Sel}_n^d/\mathbb{F}_q(t))^m] = \prod_{prime\ \ell|n}\prod_{i=1}^{m}\left(\ell^i+1\right).$$

The following corollary is the more familiar case of Corollary 1.6 when n is taken to be a prime ℓ. One can also deduce a version with explicit error terms in q, as in Corollary 6.6.

Corollary 1.7 *(Large q analogue of [33, Conjecture 1.1]) Let* ℓ *be a prime, and* $d \geq 2$.

(1) We have

$$\begin{aligned}&\lim_{d\to\infty}\limsup_{\substack{q\to\infty\\ \gcd(q,2\ell)=1}} \operatorname{Prob}\left(\operatorname{Sel}_\ell^d/\mathbb{F}_q(t) = (\mathbb{Z}/\ell\mathbb{Z})^c\right)\\ &= \lim_{d\to\infty}\liminf_{\substack{q\to\infty\\ \gcd(q,2\ell)=1}} \operatorname{Prob}\left(\operatorname{Sel}_\ell^d/\mathbb{F}_q(t) = (\mathbb{Z}/\ell\mathbb{Z})^c\right)\\ &= \left(\prod_{j\geq 0}\left(1-\ell^{-j}\right)^{-1}\right)\left(\prod_{j=1}^{c}\frac{\ell}{\ell^j-1}\right).\end{aligned}$$

(2) We have

$$\lim_{\substack{q\to\infty\\ \gcd(q,2\ell)=1}} \mathbb{E}[\#\operatorname{Sel}_\ell^d/\mathbb{F}_q(t)] = \sigma(\ell) := \ell+1.$$

(3) For $m \leq 6d-3$ *the mth moment of* $\operatorname{Sel}_\ell^d/\mathbb{F}_q(t)$ *is*

$$\lim_{\substack{q\to\infty\\ \gcd(q,2n)=1}} \mathbb{E}[(\#\operatorname{Sel}_\ell^d/\mathbb{F}_q(t))^m] = \prod_{i=1}^{m}\left(\ell^i+1\right).$$

Remark 1.8 (Distributions of Tate–Shafarevich groups). Throughout this paper, we mostly work with the joint distribution of ranks and n-Selmer groups of elliptic curves, while [1] also makes predictions for Tate–Shafarevich groups of elliptic curves. Indeed, as an easy consequence of our results, we obtain analogous predictions for Tate–Shafarevich groups, as we now explain. For E a torsion free elliptic curve over $\mathbb{F}_q(t)$, we have an exact sequence

$$0 \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{\operatorname{rk} E} \longrightarrow \operatorname{Sel}_n(E) \longrightarrow Ш(E)[n] \longrightarrow 0. \tag{1.4}$$

Note that the torsion freeness condition is satisfied 100% of the time [1, Lemma 5.7]. Therefore, the algebraic rank and n-Selmer group of E determines $Ш(E)[n]$, and hence the joint distribution of algebraic ranks, and n-Selmer groups determines the joint distribution of algebraic ranks, n-Selmer groups, and n-torsion in Tate–Shafarevich groups. Let $(\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}}, Ш[n]^{\mathrm{BKLPR}})$ denote the conjectural joint distribution for ranks, n-Selmer groups, and n-torsion in Tate–Shafarevich groups described in [1, §5.7] and let $(\mathrm{rk}, \mathrm{Sel}_n, Ш[n])^d_{\mathbb{F}_q}$ denote the joint distribution of algebraic ranks, n-Selmer groups, and n-torsion in Tate–Shafarevich groups of height d elliptic curves over $\mathbb{F}_q$. Then, it follows from Theorem 1.1 and the above remarks that

$$\begin{aligned}(\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}}, Ш[n]^{\mathrm{BKLPR}}) &= \lim_{d\to\infty}\left(\limsup_{\substack{q\to\infty\\ \gcd(q,2n)=1}} (\mathrm{rk}, \mathrm{Sel}_n, Ш[n])^d_{\mathbb{F}_q}\right)\\ &= \lim_{d\to\infty}\left(\liminf_{\substack{q\to\infty\\ \gcd(q,2n)=1}} (\mathrm{rk}, \mathrm{Sel}_n, Ш[n])^d_{\mathbb{F}_q}\right).\end{aligned}$$

One can also bound the error in these limits using Theorems 6.1 and 6.4. We note that for fixed height $d \geq 2$, the proportion of elliptic curves of height up to d over $\mathbb{F}_q$ with analytic rank equal to algebraic rank tends to 1 as $q \to \infty$ over prime powers q with $\gcd(q, 2) = 1$. This follows from Theorem 1.1 and Proposition 6.3. Therefore, the Birch and Swinnerton-Dyer Conjecture holds for all such curves, implying the Tate–Shafarevich group is finite for all such curves.

Remark 1.9 (Families of quadratic twists) In other families of elliptic curves, such as quadratic twist families, the “geometric distribution” will similarly be controlled by the analogous monodromy representations to those described in Sect. 1.2.4. Adapting our arguments will yield similar results for such families whenever the geometric monodromy group is large enough. However, the precise distribution that results depends rather delicately on the precise monodromy group, for the same reasons as described in Sect. 1.2.4.

For example, in forthcoming work [34], Park and Wang carry out an analog of the results of [28] for quadratic twist families of elliptic curves, at least in the case of n-Selmer groups for n prime. We note this should often be extendable to composite n, see [28, Remark 1.7]. Suppose one chooses a quadratic twist family such that the sheaf on that family constructed analogously to $\mathcal{S}^{\circ d}_{n,B}$ on the universal family has geometric monodromy containing the commutator of the relevant orthogonal group, but with nontrivial Dickson invariant (see Sect. 3.2.4). Given such a family, via similar arguments to those in this paper, if one first takes $\liminf_{q\to\infty}$ or $\limsup_{q\to\infty}$, and then a large height limit, the joint distribution of the rank and n-Selmer group will agree with $(\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}})$. We note that triviality or nontriviality of the Dickson invariant can often be verified for explicit examples, as in the proof of [46, Theorem 4.1].

On the other hand, it is possible for the Dickson invariant to be trivial in quadratic twist families; explicit such examples are constructed in [46, Sects. 5 and 6]. In these cases, the distribution of ranks and Selmer groups in the quadratic twist family will differ from those predicted in [1]. E.g., the minimalist conjecture will fail as 100% of elliptic curves in such families will have rank 0. Nevertheless, for sufficiently high degree twists, the large q limit mth moments in these quadratic twist families will agree with those predicted in [1]. Additionally, it is possible to choose quadratic twist families where the relevant geometric monodromy does not contain the commutator of the relevant orthogonal group, in which case the large q limit statistics of ranks and Selmer groups may differ drastically from those predicted in [1].

Remark 1.10 (The inverse Galois problem) For ℓ a prime, let Q_ℓ^d denote the quadratic form defined in Definition 3.1, which we note has discriminant 1 and hence is equivalent to the standard quadratic form $x_1x_2 + x_3x_4 + \cdots + x_{12d-5}x_{12d-4}$. In order to prove Theorem 1.1, we perform a certain monodromy computation in Theorem 3.14, which shows that for even $d \geq 2$, and $\ell \nmid d - 1$, $O(Q_\ell^d)$ occurs as a Galois group over $\mathbb{Q}(t_1, \ldots, t_{10d+2})$, and hence also as a Galois group over $\mathbb{Q}$ by Hilbert irreducibility ([36, Sect. 9.2, Proposition 2] in conjunction with [36, Sect. 13.1, Theorem 3]). To our knowledge, it was not previously known that these groups all appear as Galois groups over $\mathbb{Q}$.

Closely related constructions to ours are given in [46, Theorem 1.1], and the techniques of [46] can likely be adapted to construct the Galois groups $O(Q_\ell^d)$ when $\ell \geq 5$. However, our results also apply in the cases $\ell = 2$ and $\ell = 3$, to which the techniques of [46] seem not to apply.

Remark 1.11 An interesting byproduct of the proof of Theorem 1.1 is that the analytic rank of an elliptic curve over $\mathbb{F}_q(t)$ with smooth minimal proper regular model is realized as the dimension of the generalized 1-eigenspace of a certain matrix associated to an action of Frobenius (see Lemma 3.18) while the ℓ^∞-Selmer rank is the dimension of the 1-eigenspace of that same matrix (see Lemma 6.2). These dimensions agree for 100% of elliptic curves of fixed height d over $\mathbb{F}_q(t)$ in the large q limit and also agree with the rank of the elliptic curve (see Proposition 6.3). Hence, at least in the function field setting, this gives an answer to the question raised in [32, Remark 1.1.4] as to whether there exists a natural matrix coming from the arithmetic of elliptic curves giving rise to the rank and Selmer group of an elliptic curve.

Example 1.12 (A distribution not determined by its moments) Consider the three distributions

$$\begin{aligned}
&(\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}}),\\
&((\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}}) | \, \mathrm{rk}^{\mathrm{BKLPR}} \equiv 0 \mod 2),\\
&((\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}}) | \, \mathrm{rk}^{\mathrm{BKLPR}} \equiv 1 \mod 2),
\end{aligned}$$

with the latter two the distributions conditioning upon whether the rank is even or odd. These give examples of three distinct distributions which we claim have the same mth moments for all $m \geq 0$.

We now justify why the moments of these three distributions agree. For simplicity, we assume n is prime, though the same claim holds true for general composite n, as can be deduced from the Markov properties verified in Sect. 5. By Theorem 6.4, the above three distributions agree with the three distributions

$$\lim_{d \to \infty} \liminf_{q \to \infty} (\mathrm{Rrk}, \mathrm{RSel}_n)^d_{\mathbb{F}_q},$$

$$\lim_{d\to\infty} \liminf_{q\to\infty}((\mathrm{Rrk}, \mathrm{RSel}_n)^d_{\mathbb{F}_q} \,|\, \mathrm{rk} \equiv 0 \mod 2),$$
$$\lim_{d\to\infty} \liminf_{q\to\infty}((\mathrm{Rrk}, \mathrm{RSel}_n)^d_{\mathbb{F}_q} \,|\, \mathrm{rk} \equiv 1 \mod 2)$$

respectively. By Definition 4.2, these distributions are all given by the limit as $d \to \infty$ of the the dimension of the kernel of a random matrix drawn from certain cosets of the orthogonal group of rank $12d - 4$. The distribution conditioned on even rank corresponds to the cosets with Dickson invariant 0 while that conditioned on odd rank corresponds to cosets with Dickson invariant 1. Therefore, by Theorem 4.10, the moments of these distributions all stabilize in d (in fact once $6d - 3 \geq m$), and are equal to $\prod_{i=1}^m \left(\ell^i + 1\right)$.

1.3 Overview of the proof

We next indicate the idea of the proof of Theorem 1.1. There is a moduli stack $\underline{\mathscr{W}}'^d_{\mathbb{F}_q}$ parameterizing Weierstrass equations for elliptic curves over $\mathbb{F}_q(t)$ of height d. For $(n, q) = 1$, we define in Sect. 2.1 a moduli stack $\underline{\mathrm{Sel}}'^d_{n,\mathbb{F}_q}$ that approximately parameterizes pairs (E, α) for $[E] \in \underline{\mathscr{W}}'^d_{\mathbb{F}_q}$ an elliptic curve and $\alpha \in \mathrm{Sel}_n(E)$. The basic point here is that there is a dense open set of points of $\underline{\mathscr{W}}'^d_{\mathbb{F}_q}$ whose corresponding minimal Weierstrass models are smooth over $\mathbb{F}_q$. For elliptic curves E corresponding to points in this open set, if $\mathscr{E}^0$ is the identity component of the Néron model of E over $\mathbb{P}^1_{\mathbb{F}_q}$, $\mathrm{Sel}_n(E) = H^1_{\acute{e}t}(\mathbb{P}^1_{\mathbb{F}_q}, \mathscr{E}^0[n])$. (We observe that $\mathscr{E}^0[n]$ is étale over $\mathbb{P}^1_{\mathbb{F}_q}$ by our assumption that $(n, q) = 1$: indeed, by miracle flatness it suffices to check this is étale over each point of $\mathbb{P}^1_{\mathbb{F}_q}$. Each fiber of $\mathscr{E}^0$ is a 1-dimensional group scheme isomorphic to $\mathbb{G}_a$, $\mathbb{G}_m$, or an elliptic curve E, in which case its n-torsion is id, μ_n, or $E[n]$, all of which are étale when $(n, q) = 1$.) In other words, $\underline{\mathrm{Sel}}'^d_{n,\mathbb{F}_q}$ is the stack classifying E along with étale $\mathscr{E}^0[n]$-torsors over $\mathbb{P}^1_{\mathbb{F}_q}$.

There is an natural quasi-finite map $\pi : \underline{\mathrm{Sel}}'^d_{n,\mathbb{F}_q} \to \underline{\mathscr{W}}'^d_{\mathbb{F}_q}$, and over an open dense substack $\underline{\mathscr{W}}^{\circ d}_{\mathbb{F}_q} \subset \underline{\mathscr{W}}'^d_{\mathbb{F}_q}$ the restriction

$$\pi : \underline{\mathrm{Sel}}^{\circ d}_{n,\mathbb{F}_q} := \underline{\mathrm{Sel}}'^d_{n,\mathbb{F}_q}|_{\underline{\mathscr{W}}^{\circ d}_{\mathbb{F}_q}} \to \underline{\mathscr{W}}^{\circ d}_{\mathbb{F}_q} \tag{1.5}$$

is finite étale. The n-Selmer group of $[E] \in \underline{\mathscr{W}}^{\circ d}_{\mathbb{F}_q}(\mathbb{F}_q)$ is then identified with $\mathbb{F}_q$-points of $\pi^{-1}(E)$. The cover π is associated to a monodromy representation $\rho^d_{n,\mathbb{F}_q} : \pi_1(\underline{\mathscr{W}}^{\circ d}_{\mathbb{F}_q}) \to O(Q^d_n)$, where (V^d_n, Q^d_n) is a particular rank $12d - 4$ quadratic space over $\mathbb{Z}/n\mathbb{Z}$, and $\pi^{-1}(E)(\mathbb{F}_q)$ identifies with $\ker(\rho^d_{n,\mathbb{F}_q}(\mathrm{Frob}_E) - \mathrm{id}) \subset V^d_n$.

After determining the monodromy group, this reduces to a combinatorial problem: compute the distribution of $\dim \ker(g - \mathrm{id})$ for a g drawn randomly from the monodromy group. For V^d_n over $\mathbb{Z}/\ell\mathbb{Z}$, (i.e., the case that $n = \ell$ is prime,) and g drawn from the full $O(Q^d_\ell)$, this computation was done in unpublished work of Rudvalis and Shinoda, as we learned from [15]. We give an alternative proof which generalizes

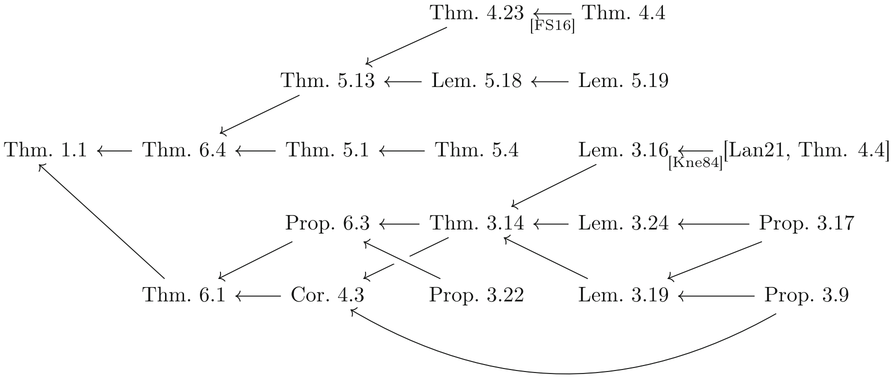

Fig. 1 A schematic diagram depicting the structure of the proof of Theorem 1.1

to the case where g is drawn from certain proper subgroups of $O(Q_\ell^d)$ related to the monodromy group (which is needed for our results).

After handling the case where $n = \ell$ is prime, we move on to the case of Sel_{ℓ^e}. In this case, we prove that there is a characterization of $\ker(g - \mathrm{id})$ in terms of a Markov property, and that the BKLPR heuristic is also characterized by this same Markov property. The case of general Sel_n for n composite follows from the prime power case by the Chinese remainder theorem.

1.4 Outline of paper

We next give a brief outline of the content of the various sections in this paper. In Sect. 2 we recall the construction of Selmer spaces, which parameterize Selmer elements of elliptic curves. The Selmer spaces mentioned above are generically finite étale covers of the moduli space of height d elliptic surfaces. In Sect. 3 we compute the monodromy associated to these covers. Next, in Sect. 4 we establish that the geometric distribution of prime order Selmer groups agree with that predicted by the BKLPR heuristic. In Sect. 5, we show that both the BKLPR heuristic distribution and our geometric distribution agree for prime powers, by relating the two distributions for ℓ^j-Selmer groups to the two distributions for ℓ^{j+1}-Selmer groups via separate Markov processes. Finally, in Sect. 6 we put the pieces together to the prove our main results.

2 Summary of Selmer spaces

2.1 Reviewing the definition of the Selmer space

Here, we briefly recall the construction of the Selmer space and related spaces introduced in [28, Sect. 3]. The new content in this section occurs in Sect. 2.3 where we introduce an sheaf is isomorphic to the Selmer sheaf (Sect. 2.1.4 for the definition) on a dense open. This sheaf is closely related to the L-function of elliptic curves, and hence gives us a way to access the analytic ranks of elliptic curves in terms of the

Selmer sheaf. Our notation differs slightly from that of [28] due to a minor error (only appearing in characteristic 3), as we will explain further in Remark 2.1.

2.1.1 The space of Weierstrass equations

Throughout this section, we work relatively over a scheme B on which 2 is invertible. As in [28, Definition 3.1], define $\mathbb{P}^1_B := \operatorname{Proj}_B \mathscr{O}_B[s,t]$. Form the affine space,

$$\mathbb{A}_B^{12d+3} := \operatorname{Spec}_B \mathscr{O}_B[a_{2,0}, a_{2,1} \dots, a_{2,2d}, a_{4,0}, \dots, a_{4,4d}, a_{6,0} \dots, a_{6,6d}].$$

For $i \in \{1,2,3\}$, define $a_{2i}(s,t) := \sum_{j=0}^{2id} a_{2i,j} t^j s^{2id-j}$. Let $\mathscr{W}'^d_B \subset \mathbb{A}_B^{12d+3}$ denote the open subscheme parameterizing those points such that the Weierstrass equation

$$y^2 z = x^3 + a_2(s,t)x^2 z + a_4(s,t)xz^2 + a_6(s,t)z^3$$

defines an elliptic surface with smooth generic fiber. This is open as it corresponds to the open subscheme of $\mathbb{A}_B^{12d+3}$ such that the discriminant is nonzero.

Remark 2.1 There was a minor error in [28, Definition 3.1] where it was claimed that a Weierstrass model is minimal if and only if it is of the form $y^2z = x^3 + a_2(s,t)x^2z + a_4(s,t)xz^2 + a_6(s,t)z^3$ with no non-constant polynomial $f \in k[s,t]$ with $f^{2i} \mid a_{2i}(s,t)$ for all $i \in \{1,2,3\}$. However, it is only true that it can be written in this form after a change of variables.

This makes it less obvious that in characteristic 3, the locus of minimal Weierstrass equations is open $\mathbb{A}_B^{12d+3}$. It is fairly simple to see this is true in characteristic neither 2 nor 3, since one can make a change of variables to assume $a_2(s,t) = 0$, and then the resulting equation $y^2z = x^3 + a_4(s,t)xz^2 + a_6(s,t)z^3$ is minimal if and only if there is no non-constant polynomial $f \in k[s,t]$ with $f^{2i} \mid a_{2i}(s,t)$ for all $i \in \{2,3\}$. In characteristic 3, this non-minimal locus is still open, but we only found a somewhat involved proof which involves tracing through the steps of Tate's algorithm.

To avoid this fairly involved proof, we opt to work over a slightly larger open set $\mathscr{W}'^d_B$, which does not parameterize minimal Weierstrass models, but instead parameterizes all Weierstrass models over $\mathbb{A}_B^{12d+3}$ with smooth generic fiber. Since the two open subsets differ by a divisor, their point counts do not contribute in the large q limit, and so which set we work with does not substantially alter the argument.

2.1.2 The universal Weierstrass equation

Similarly to [28, Definition 3.1], one can construct a family of minimal Weierstrass models $\mathscr{U}\mathscr{W}'^d_B$ over $\mathbb{P}^1 \times \mathscr{W}'^d_B$ as the subscheme of

$$\operatorname{Proj}_{\mathbb{P}^1_B \times_B \mathscr{W}'^d_B} \operatorname{Sym}^\bullet \left(\mathscr{O}_{\mathbb{P}^1_B \times_B \mathscr{W}'^d_B} \oplus \mathscr{O}_{\mathbb{P}^1_B \times_B \mathscr{W}'^d_B}(-2d) \oplus \mathscr{O}_{\mathbb{P}^1_B \times_B \mathscr{W}'^d_B}(-3d)\right)$$

cut out by the equation

$$y^2 z = x^3 + a_2(s,t)x^2 z + a_4(s,t)xz^2 + a_6(s,t)z^3.$$

As mentioned in Remark 2.1, we work over $\mathscr{W}'^d_B$, a set including non-minimal elliptic curves, which is slightly different than that used in [28, Definition 3.1].

2.1.3 An open subset

Recall our definition of $\mathscr{W}'^d_B$ from Sect. 2.1.1 as a moduli space of height d minimal Weierstrass equations. Similarly to [28, Definition 3.9], let $\mathscr{W}^{\circ d}_B \subset \mathscr{W}'^d_B$ denote the open subscheme over which $\mathscr{U}\mathscr{W}'^d_B \to \mathscr{W}'^d_B$ is smooth. In the case B is a field k, $\mathscr{W}^{\circ d}_k$ parameterizes elliptic curves of height d over $k(t)$ so that the associated minimal Weierstrass elliptic surface is smooth over k. Let $\mathscr{U}\mathscr{W}^{\circ d}_B := \mathscr{U}\mathscr{W}'^d_B \times_{\mathscr{W}'^d_B} \mathscr{W}^{\circ d}_B$ denote the universal elliptic surface over $\mathscr{W}^{\circ d}_B$. We also introduce $\mathscr{W}^{\boxslash d}_B \subset \mathscr{W}'^d_B$ as the open subscheme parameterizing elliptic surfaces with squarefree discriminant and let $\mathscr{U}\mathscr{W}^{\boxslash d}_B := \mathscr{U}\mathscr{W}'^d_B \times_{\mathscr{W}'^d_B} \mathscr{W}^{\boxslash d}_B$; these subsets are indeed open and dense over B as is explained in [28, Lemma 3.14]. Loosely speaking, the idea is to show that the elliptic surfaces of height d with squarefree discriminant are the complement of two divisors: the divisor parameterizing elliptic surfaces of height d which are singular and the divisor paramterizing elliptic surfaces of height d with some cuspidal fiber. These two divisorial subschemes can be defined via incidence correspondences. One can then use these incidence correspondences to compute the dimensions of these subschemes, and verify they are indeed divisors, implying that the open locus of elliptic surfaces of height d is fiberwise nonempty, hence fiberwise dense.

2.1.4 The Selmer space

Similarly to [28, Definition 3.3], (but see Remark 2.1 for a slight difference) denote by f and g the projection maps

$$\mathscr{U}\mathscr{W}'^d_B \xrightarrow{f} \mathbb{P}^1_B \times_B \mathscr{W}'^d_B \xrightarrow{g} \mathscr{W}'^d_B.$$

Assuming further that $2n$ is invertible on B. Define the *n-Selmer sheaf over B of height d* as $\mathcal{S}e\ell'^d_{n,B} := R^1 g_*(R^1 f_* \mu_n)$. Define the *$n$-Selmer space over B of height d*, denoted $\mathrm{Sel}'^d_{n,B}$ as the algebraic space representing the sheaf of $\mathbb{Z}/n\mathbb{Z}$ modules $\mathcal{S}e\ell'^d_{n,B}$. Let

$$\begin{aligned}\mathrm{Sel}^{\circ d}_{n,B} &:= \mathrm{Sel}'^d_{n,B} \times_{\mathscr{W}'^d_B} \mathscr{W}^{\circ d}_B,\ \mathrm{Sel}^{\boxslash d}_{n,B} := \mathrm{Sel}'^d_{n,B} \times_{\mathscr{W}'^d_B} \mathscr{W}^{\boxslash d}_B,\ \mathcal{S}e\ell^{\circ d}_{n,B} \\ &:= \mathcal{S}e\ell'^d_{n,B} \times_{\mathscr{W}'^d_B} \mathscr{W}^{\circ d}_B.\end{aligned}$$

2.1.5 A moduli stack of elliptic curves

Note that $\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m$ acts on $\mathscr{U}\mathscr{W}'^d_B$ and $\mathscr{W}'^d_B$ compatibly. Loosely speaking, $(r_0, \ldots, r_{2d}) \in \mathbb{G}_a^{2d+1}$ acts by sending $x \mapsto x + r_0 s^{2d} + r_1 t s^{2d-1} + \cdots + r_{2d} t^{2d}$ and $\lambda \in \mathbb{G}_m$ acts by sending $a_{2i}(s,t) \mapsto \lambda^{2i} a_{2i}(s,t)$, see [28, Definition 3.4] for a more precise formulation in terms of Weierstrass equations. By [38, III.3.1(b)], any two points in $\mathscr{W}'^{d}_{B}$ corresponding to isomorphic elliptic curves lie in the same orbit of this action. Similarly to [28, Definition 3.4], we define the *moduli stack of height d minimal Weierstrass models over B* as the quotient stack

$$\underline{\mathscr{W}}'^{d}_{B} := \left[\mathscr{W}'^{d}_{B}/\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m\right].$$

2.1.6 The Selmer stack

Similarly to [28, Definition 3.4], we define the *n-Selmer stack over B of height d* as the quotient stack

$$\underline{\mathrm{Sel}}'^{d}_{n,B} := \left[\mathrm{Sel}'^{d}_{n,B}/\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m\right].$$

Since the action of $\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m$ restricts to an action on $\mathscr{UW}^{\circ d}_{B}$, $\mathscr{W}^{\circ d}_{B}$, and $\mathrm{Sel}^{\circ d}_{n,B}$, we similarly define

$$\underline{\mathscr{W}}^{\circ d}_{B} := \left[\mathscr{W}^{\circ d}_{B}/\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m\right], \ \underline{\mathscr{W}}^{\boxslash B}_{d} := \left[\mathscr{W}^{\boxslash d}_{B}/\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m\right],$$

and

$$\underline{\mathrm{Sel}}^{\circ d}_{n,B} := \left[\mathrm{Sel}^{\circ d}_{n,B}/\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m\right], \ \underline{\mathrm{Sel}}^{\boxslash d}_{n,B} := \left[\mathrm{Sel}^{\boxslash d}_{n,B}/\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m\right].$$

Remark 2.2 For $x \in \mathscr{W}'^{d}_{B}$ or $x \in \underline{\mathscr{W}}'^{d}_{B}$, we use E_x denote the corresponding elliptic curve. Specifically, for $x \in \mathscr{W}'^{d}_{B}$, if $f : \mathscr{UW}'^{d}_{B} \to \mathbb{P}^1 \times \mathscr{W}'^{d}_{B}$, then $E_x = f^{-1}(\eta \times x)$, for η the generic point of $\mathbb{P}^1$. We often notate this by $[E_x] = x \in \mathscr{W}'^{d}_{B}$. Similarly, for $x \in \underline{\mathscr{W}}^{\circ d}_{B}$, we notate $[E_x] = x$ where E_x is the elliptic curve corresponding to x.

2.2 The relation between Selmer spaces and Selmer groups

We have now defined the Selmer space, but have not yet explained the connection to Selmer groups of elliptic curves. The following lemma provides the relation.

Lemma 2.3 *([28, Corollary 3.24]) Let $n \geq 1, d > 0, m \geq 0$. Let B be a noetherian scheme with $2n$ invertible, and let $\pi : Sel'^{d}_{n,B} \to \mathscr{W}'^{d}_{B}$ denote the projection map. For $[E_x] = x \in \mathscr{W}^{\circ d}_{B}(\mathbb{F}_q)$, we have*

$$\#\,\mathrm{Sel}_n(E_x) = \#\left(\pi^{-1}(x)\left(\mathbb{F}_q\right)\right). \tag{2.1}$$

2.3 The sheaf governing rank

In this section, we introduce a sheaf $\mathcal{S}^{\circ d}_{n,B}$. This is closely related to the Selmer sheaf $\mathcal{S}e\ell^{\circ d}_{n,B}$ and governs the rank of the elliptic curve. This sheaf is not new, and has previously appeared in the literature, see Remark 2.5. Our goal will be to show the two sheaves are isomorphic on the fiberwise over B dense open of $\mathscr{W}^{\circ d}_B$ parameterizing elliptic surfaces with squarefree discriminant. We now define $\mathcal{S}^{\circ d}_{n,B}$.

Notation 2.4 Let B be a scheme with $2n$ invertible on B. Let $j : U \subset \mathbb{P}^1_B \times_B \mathscr{W}^{\circ d}_B$ denote the open subscheme over which the projection $f : \mathscr{UW}^{\circ d}_B \to \mathbb{P}^1_B \times_B \mathscr{W}^{\circ d}_B$ is smooth. Let $g : \mathbb{P}^1_B \times_B \mathscr{W}^{\circ d}_B \to \mathscr{W}^{\circ d}_B$ denote the projection. Then, if $\alpha_S : S \to \mathscr{W}^{\circ d}_B$ is a map of schemes, set up the following commutative diagram, where both squares are fiber squares.

$$\begin{tikzcd}
\mathscr{UW}^{\circ d}_B \times_{\mathscr{W}^{\circ d}_B} S \arrow[dr, "f^S"] & U_S \arrow[r, "\alpha'_S"] \arrow[d, "j^S"] \arrow[dd, bend right=60, "\overline{g}^S"'] & U \arrow[d, "j"] \arrow[dd, bend left=60, "\overline{g}"] & \mathscr{UW}^{\circ d}_B \arrow[dl, "f"'] \\
& \mathbb{P}^1_B \times_B S \arrow[r] \arrow[d, "g^S"] & \mathbb{P}^1_B \times_B \mathscr{W}^{\circ d}_B \arrow[d, "g"] & \\
& S \arrow[r, "\alpha_S"] & \mathscr{W}^{\circ d}_B &
\end{tikzcd}$$

Define $\mathcal{E}[n]_S := (j^S)^* R^1 f^S_* \mu_n$ (we note that $\mathcal{E}[n]_S$ is a slight abuse of notation since it depends on the map α_S and not just the scheme S). This sheaf represents the relative n torsion of f^S. Define the sheaf $\mathcal{S}^{\circ d}_{n,B} := R^1 g_*(j_* \mathcal{E}[n]_{\mathscr{W}^{\circ d}_B})$, with the implicit map $\alpha_{\mathscr{W}^{\circ d}_B} : \mathscr{W}^{\circ d}_B \to \mathscr{W}^{\circ d}_B$ taken to be the identity.

Remark 2.5 Sheaves defined analogously to $\mathcal{S}^{\circ d}_{n,B}$ appeared in the context of quadratic twist families of elliptic curves in [18, Sect. 6.2] and [46, Sect. 3.2]. In fact, $\mathcal{S}^{\circ d}_{n,B}$ is itself a reasonable candidate for the Selmer sheaf, but we will instead work with $\mathcal{S}e\ell^{\circ d}_{n,B}$, which has the advantage that it commutes with base change. On the other hand, we are not sure if $\mathcal{S}^{\circ d}_{n,B}$ commutes with base change in general, though it does over $\mathscr{W}^{\not\square d}_B$, as we show in Lemma 2.6.

Having defined $\mathcal{S}^{\circ d}_{n,B}$, we next wish to show it agrees with $\mathcal{S}e\ell^{\circ d}_{n,B}$, at least when both are restricted to $\mathscr{W}^{\not\square d}_B$. To verify this isomorphism, we will construct a map between them and check it is an isomorphism by checking it on fibers. The verification on fibers is fairly immediate once we know that the formation of $\mathcal{S}^{\circ d}_{n,B}$ commutes with base change, as we now verify. A variant of the following Lemma 2.6 is explained in [22, Construction-Proposition 5.2.1(3)].

Lemma 2.6 *With maps f and g as in Notation 2.4, the sheaf $\mathcal{S}^{\circ d}_{n,B}$ is a constructible sheaf of $\mathbb{Z}/n\mathbb{Z}$ modules whose formation commutes with base change on $\mathscr{W}^{\not\square d}_B$. More precisely, for any base scheme S factoring through $\mathscr{W}^{\not\square d}_B$, the base change map*

$$\alpha_S^* R^1 g_*(j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}) \to R^1 g^S_*(j^S_* {\alpha'_S}^* \mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}),$$

is an isomorphism.

Proof Let $R^1\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B} \xrightarrow{\phi} \mathcal{S}^{\circ d}_{n,B}$ denote the map induced by $j_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B} \to j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$, using the identification $R^1\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B} = R^1 g_*(j_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B})$. Let $\mathcal{S}^{\circ d}_{n,B} \xrightarrow{\psi} R^1\overline{g}_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ denote the map induced from the composition of functors spectral sequence for $g \circ j$. We will show that $\mathcal{S}^{\circ d}_{n,B}$ is the image of the composition $R^1\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B} \xrightarrow{\phi} \mathcal{S}^{\circ d}_{n,B} \xrightarrow{\psi} R^1\overline{g}_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$. Once we show this, it will immediately follow that $\mathcal{S}^{\circ d}_{n,B}$ is constructible, being the image of a map of constructible sheaves.

By the Leray spectral sequence, ψ is always injective. Hence, to identify $\mathcal{S}^{\circ d}_{n,B}$ as the image of $\psi \circ \phi$, we only need to show ϕ is surjective. To this end, define M as the quotient sheaf $j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}/j_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$. Note that M is supported on the complement of U which is finite over $\mathscr{W}^{\circ d}_B$. Therefore, $R^1 g_* M = 0$ and we conclude that $R^1\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B} = R^1 g_*(j_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}) \to R^1 g_*(j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}) = \mathcal{S}^{\circ d}_{n,B}$ is surjective. Hence, $R^1 g_*\left(j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}\right)$ is a constructible $\mathbb{Z}/n\mathbb{Z}$ module, being the image of a map of constructible $\mathbb{Z}/n\mathbb{Z}$ modules.

To conclude, we show that the formation of $\mathcal{S}^{\circ d}_{n,B}$ commutes with base change over $\mathscr{W}^{\boxslash d}_B$. Since $\mathcal{S}^{\circ d}_{n,B}$ is the image of $\psi \circ \phi : R^1\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B} \to R^1\overline{g}_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$, it suffices to show that the formation of both $R^1\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ and $R^1\overline{g}_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ commute with base change over $\mathscr{W}^{\boxslash d}_B$. The former commutes with base change by proper base change with compact supports.

To conclude, it remains to show the formation of $R^1\overline{g}_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ commutes with base change over $\mathscr{W}^{\boxslash d}_B$. We will do this using Poincaré duality and Deligne's semicontinuity theorem for Swan conductors [29, Corollaire 2.1.2 and Remarque 2.1.3]. We first use Deligne's semicontinuity theorem to show $R^i\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ is locally constant constructible for all $i \geq 0$. The semicontinuity theorem says that $R^i\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ will be locally constant over any open subscheme of $\mathscr{W}^{\circ d}_B$ for which the degree of $\mathbb{P}^1 \times \mathscr{W}^{\circ d}_B - U \to \mathscr{W}^{\circ d}_B$ is constant and the total Swan conductor associated to $\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ is constant.

We now verify the hypotheses of Deligne's semicontinuity theorem by verifying $\mathbb{P}^1 \times \mathscr{W}^{\circ d}_B - U \to \mathscr{W}^{\circ d}_B$ has constant fiber degree over $\mathscr{W}^{\boxslash d}_B$ and that the Swan conductor vanishes over $\mathscr{W}^{\boxslash d}_B$. Indeed, any elliptic curve corresponding to a point of $\mathscr{W}^{\boxslash d}_B$ has reduced discriminant, and hence $12d$ geometric fibers of type I_1 reduction and no other singular fibers, by Tate's algorithm. This shows $\mathbb{P}^1 \times \mathscr{W}^{\circ d}_B - U \to \mathscr{W}^{\circ d}_B$ has constant fiber degree over $\mathscr{W}^{\boxslash d}_B$. Finally, the Swan conductor always vanishes when the reduction is multiplicative [37, IV.10.2(b)].

Using that $R^1\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ is locally constant constructible over $\mathscr{W}^{\boxslash d}_B$ we next deduce $R^1\overline{g}_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ is as well via Poincare duality. Namely, Poincaré duality [42] gives an isomorphism of sheaves in the derived category

$$R\overline{g}_*R\,\mathscr{H}\mathrm{om}(\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B},\mu_n[2]) \simeq R\,\mathscr{H}\mathrm{om}(R\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B},\mu_n).$$

Note that the [2] denotes a cohomological shift by 2 while the $[n]$ refers to the n-torsion.

We will now take (-1)st cohomology of both sides. By construction of U, $\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ is locally constant on U, and therefore the ith cohomology of $R\overline{g}_*R\mathscr{H}om(\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B},\mu_n[2])$ is given by $R^{i+2}\overline{g}_*\,\mathscr{H}\mathrm{om}(\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B},\mu_n) \simeq R^{i+2}\overline{g}_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$, the latter isomorphism induced by the Weil pairing. Additionally, since $R^{-i}\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ is locally constant constructible, we get that the ith cohomology of $R\,\mathscr{H}\mathrm{om}(R\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B},\mu_n[2])$ is given by $\mathscr{H}\mathrm{om}(R^{-i}\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B},\mu_n)$. Therefore, taking (-1)st cohomology of the Poincaré duality isomorphism yields an isomorphism $R^1\overline{g}_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B} \simeq (R^1\overline{g}_!\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B})^\vee$. Since the right hand side is locally constant constructible over $\mathscr{W}^{\boxslash d}_B$, the left hand side is as well, and therefore commutes with base change. □

We next produce an isomorphism $\mathcal{S}e\ell^{\circ d}_{n,B}|_{\mathscr{W}^{\boxslash d}_B} \simeq \mathcal{S}^{\circ d}_{n,B}|_{\mathscr{W}^{\boxslash d}_B}$ over $\mathscr{W}^{\boxslash d}_B$, crucially using that the formation of both sheaves commute with base change.

Proposition 2.7 *Retain notation from Notation 2.4. There is canonical map $R^1f_*\mu_n \to j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$ of sheaves on $\mathbb{P}^1_B \times_B \mathscr{W}^{\circ d}_B$. This map induces an isomorphism $R^1g_*(R^1f_*\mu_n)|_{\mathscr{W}^{\boxslash d}_B} \simeq R^1g_*(j_*\mathcal{E}[n]_{\mathscr{W}^{\boxslash d}_B})$, which commutes with base change.*

Proof Retaining notation from Notation 2.4, define the maps j' and f' as in the fiber square

$$\begin{tikzcd} W_U \arrow[r, "j'"] \arrow[d, "f'"] & \mathscr{U}\mathscr{W}^{\circ d}_B \arrow[d, "f"] \\ U \arrow[r, "j"] & \mathbb{P}^1_B \times_B \mathscr{W}^{\circ d}_B. \end{tikzcd} \tag{2.2}$$

We have canonical maps coming from Leray spectral sequences

$$\begin{aligned} R^1f_*(\mu_n) &\simeq R^1f_*(j'_*\mu_n) \\ &\to R^1(f\circ j')_*\mu_n \\ &= R^1(j\circ f')_*\mu_n \\ &\to j_*R^1f'_*\mu_n. \end{aligned} \tag{2.3}$$

Using the Kummer exact sequence (possible since n is invertible by Notation 2.4) and the assumption that the fibers of f' are smooth connected elliptic curves so [2, Sect. 9.5, Theorem 1] applies, we obtain isomorphisms

$$j_*R^1 f'_*\mu_n \simeq j_* \operatorname{Pic}_{W_U/U}[n] \simeq j_* \operatorname{Pic}^0_{W_U/U}[n] \simeq j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}. \tag{2.4}$$

Composing (2.3) with (2.4), we obtain the desired map $R^1 f_*(\mu_{n,W}) \to j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B}$.

We show this map induces an isomorphism $R^1 g_*(R^1 f_*\mu_n))|_{\mathscr{W}^{\square d}_B} \to R^1 g_*(j_*\mathcal{E}[n]_{\mathscr{W}^{\square d}_B})$. To verify this is an isomorphism, it suffices to do so on stalks. As the formation of both sides commutes with base change by proper base change and Lemma 2.6, we can check this is an isomorphism in the case that the base is a geometric point.

Thus, it suffices to show that if $f^x : W_x \to \mathbb{P}^1_x$ is a smooth minimal Weierstrass model corresponding to a point $x \in \mathscr{W}^{\circ d}_B$, j^x is the restriction of j to x, and g^x is the restriction of g to x, then the map on stalks $\phi_x : R^1 g^x_*(R^1 f^x_* \mu_n) \to R^1 g^x_*(j^x_*(\mathcal{E}[n]_x))$ is an isomorphism. It suffices to check the map $R^1 f^x_* \mu_n \to j^x_*(\mathcal{E}[n]_x)$ inducing ϕ_x under $R^1 g^x_*$ is an isomorphism. To this end, by [28, Lemma 3.7], the étale sheaf $R^1 f^x_* \mu_n$ is represented by the Néron model of $E_x[n]$ on the small étale site of $\mathbb{P}^1_x$, while $j^x_*(\mathcal{E}[n]_x)$ is also represented by the Néron model of $E_x[n]$ by the Néron mapping property. The Néron mapping property implies that to check the map $R^1 f^x_* \mu_n \to j^x_*(\mathcal{E}[n]_x)$ constructed in (2.3) is an isomorphism, it suffices to check its restriction to U is an isomorphism. That is, we want to show the base change of $j^*R^1 f_*(\mu_n) \to j^* j_*\mathcal{E}[n]_{\mathscr{W}^{\circ d}_B} \simeq R^1 f'_* j'^*\mu_n$ to x is an isomorphism. If we could show this is the natural base change map, it would indeed be an isomorphism by proper base change.

So, to conclude the proof, we only need to check the constructed map $j^* R^1 f_*(\mu_n) \to R^1 f'_* j'^* \mu_n$, coming from pulling back (2.3) along j, is the base change map. Indeed, this follows from the definitions. In more detail, recall that for $\mathscr{F}$ a sheaf on $\mathscr{U}\mathscr{W}^{\circ d}_B$, the base change map is given as the map of δ-functors $j^* \circ (R^\bullet f_*)\mathscr{F} \to (R^\bullet f'_*) \circ j'^* \mathscr{F}$ induced via the degree 0 composition $j^* f_*\mathscr{F} \to j^* f_* j'_* j'^* \mathscr{F} \to j^* j_* f'_* j'^* \mathscr{F} \to f'_* j'^* \mathscr{F}$, see [14, Sect. 6, p. 60–61]. However, pulling back the map of (2.3) along j is given by the composition $j^* R^1 f_* \mu_n \to j^* R^1 f_*(j'_* j'^* \mu_n) \to j^* R^1 (j \circ f')_*(j'^* \mu_n) \to R^1 f'_*(j'^* \mu_n)$. This is precisely the resulting map on degree 1 δ-functors, and hence is the natural base change map. □

7

3 The precise monodromy of Selmer spaces

The main result of this section is Theorem 3.14 where we compute precisely the monodromy group associated to the cover $\underline{\mathrm{Sel}}^{\circ d}_{n,B} \to \underline{\mathscr{W}}^{\circ n}_B$. In order to state the theorem, we first introduce some various notation relating to orthogonal groups and the monodromy representation. Following this, we recall a general result on equidistribution of Frobenius elements in Sect. 3.4. The remainder of the section is devoted to proving Theorem 3.14, whose proof is outlined at the end of Sect. 3.5.

3.1 Adelic notation

For R an integral noetherian ring with fraction field $\mathrm{Frac}(R)$ such that $\mathrm{char}(\mathrm{Frac}(R)) = p$, let

$$\widehat{\mathbb{Z}}^{(p)} := \lim_{\gcd(n,p)=1} \mathbb{Z}/n\mathbb{Z} \simeq \prod_{\substack{\ell \text{ prime} \\ r \neq p}} \mathbb{Z}_\ell.$$

We allow $p = 0$, in which case $\widehat{\mathbb{Z}}^{(0)} = \widehat{\mathbb{Z}}$.

3.2 Notation for orthogonal groups

3.2.1 Notation for quadratic forms

Let R be a ring. A *quadratic space* over R is a pair (V, Q) where V is a free module over R and $Q : V \to R$ is a quadratic form. We say a quadratic space (V, Q) is *nondegenerate* if the hypersurface defined by the vanishing of Q in $\mathbb{P}V^\vee$ is smooth over $\mathrm{Spec}\, R$. When 2 is invertible or $\mathrm{rk}\, V$ is even, this is equivalent to the discriminant of Q being a unit on $\mathrm{Spec}\, R$, see [9, Remark C.1.1]. See [9, C.1] for a characterization in terms of non-degeneracy of the associated bilinear form on fibers. Let $O(Q)$ the corresponding orthogonal group. Note that we will use $O(Q)$ to denote both the group and the group scheme. We will primarily consider it as a group, and whenever we use it to denote the group scheme $O(Q)$, we refer to it as "the algebraic group $O(Q)$".

For $\phi : R \to S$ a map of rings, we denote $(V_\phi, Q_\phi) := (V \otimes_R S, Q \otimes_R S)$. When the map ϕ is understood, we notate this as $(V_S, Q_S) := (V_\phi, Q_\phi)$. In the special case that $S = \mathbb{Z}/n\mathbb{Z}$, we will also use $(V_n, S_n) := (V_{\mathbb{Z}/n\mathbb{Z}}, Q_{\mathbb{Z}/n\mathbb{Z}})$.

Definition 3.1 For $d \geq 1$, define the quadratic space $(V_{\mathbb{Z}}^d, Q_{\mathbb{Z}}^d)$ to be the rank $12d - 4$ free $\mathbb{Z}$ module associated to $U^{\oplus(2d-2)} \oplus (-E_8)^{\oplus d}$, for U a hyperbolic plane and $-E_8$ the E_8 lattice with the negative of its usual pairing. Then (V_n^d, Q_n^d) denotes the reduction of this quadratic space modulo n.

For Q a quadratic form on a free module V over a ring R, the *associated bilinear form* $B_Q : V \times V \to R$ is defined by

$$B_Q(x, y) := Q(x + y) - Q(x) - Q(y).$$

In what follows, we assume the quadratic form Q is nondegenerate.

For $v \in V$, with $Q(v) \in R^\times$ invertible, denote the *reflection about* v (sometimes also called an *orthogonal transvection*, cf. [43, 3.8.1])

$$\begin{aligned} r_v : V &\to V \\ w &\mapsto w - \frac{B_Q(w, v)}{Q(v)} v. \end{aligned}$$

Remark 3.2 When R is a field, $O(Q)$ is generated by these reflections so long as $(R, \mathrm{rk}\, V) \neq (\mathbb{F}_2, 4)$ [8, I.5.1].

3.2.2 The spinor norm

For completeness, we briefly recall the formal definition of the -1-spinor norm. We follow [9, p. 349] which gives the definition in the more general context of algebraic groups. Let (V, Q) be a quadratic space over R, and suppose that either rk V is even or 2 is invertible on R. The $+1$-spinor norm is then defined as the boundary map on cohomology

$$\mathrm{sp}_Q^+ : O(Q) \to H^1(\mathrm{Spec}\, R, \mu_2) \simeq R^\times / \left(R^\times\right)^2$$

induced by the sequence of algebraic groups $\mu_2 \to \mathrm{Pin(Q)} \to O(Q)$. Then the -1-*spinor norm* on $O(Q)$ is the $+1$-spinor norm for $O(-Q)$ composed with the identification $O(Q) \xrightarrow{\sim} O(-Q)$ [9, Remark C.4.9, Remark C.5.4, and p. 348].[3]

In the case $Q(v) \in R^\times$, the reflection r_v satisfies $\mathrm{sp}_Q^-(r_v) = [-Q(v)]$, the coset represented by $-Q(v)$ in $R^\times / \left(R^\times\right)^2$. Note that the spinor norm is trivial in the case $R = \mathbb{F}_2$. When $R = k$ is a field with $k \neq \mathbb{F}_2$, then $O(Q)$ is generated by reflections (cf. Remark 3.2), and sp_Q^- is then characterized by $\mathrm{sp}_Q^-(r_v) = [-Q(v)]$.

Definition 3.3 For (V, Q) a nondegenerate quadratic space over a ring R, define $O_-^*(Q) := \ker \mathrm{sp}_Q^- \subset O(Q)$ to be the kernel of the -1-spinor norm.

3.2.3 The adelic spinor map

We now spell out some notation to describe the spinor map for a quadratic form over $\widehat{\mathbb{Z}}^{(p)}$. Let p either be a prime or $p = 0$. Let (V, Q) be a nondegenerate quadratic space over $\widehat{\mathbb{Z}}^{(p)}$. Let

$$\mathrm{sp}_Q^- : O(Q) \to \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times / \left(\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times\right)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \prod_{\text{odd primes } \ell \neq p} \mathbb{Z}/2\mathbb{Z},$$

where the first copy of $(\mathbb{Z}/2\mathbb{Z})^2$ comes from $(\mathbb{Z}/2\mathbb{Z})^2 \cong \mathbb{Z}_2^\times / \left(\mathbb{Z}_2^\times\right)^2 \simeq (\mathbb{Z}/8\mathbb{Z})^\times / \left((\mathbb{Z}/8\mathbb{Z})^\times\right)^2$ and the copy of $\mathbb{Z}/2\mathbb{Z}$ indexed by an odd prime ℓ comes from $\mathbb{Z}_\ell^\times / \left(\mathbb{Z}_\ell^\times\right)^2 \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times / \left((\mathbb{Z}/\ell\mathbb{Z})^\times\right)^2$. When $p \neq 0$ and q is a power of p, we let

$$[q] \in \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times / \left(\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times\right)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \prod_{\text{odd primes } \ell \neq p} \mathbb{Z}/2\mathbb{Z}$$

denote the element induced by multiplication by q on $\widehat{\mathbb{Z}}^{(p)}$.

[3] Although it will not be relevant to this paper, as we shall ultimately only be interested in the even rank quadratic space of Definition 3.1, one can define the spinor norm on $O(Q)$ in the case that R is a field of characteristic 2 and rk V is odd. This can be done using the equality $O(Q) = SO(Q)$ as abstract groups (even though the corresponding *group schemes* are not isomorphic) since the group scheme $SO(Q)$ is the underlying reduced subscheme of the group scheme $O(Q)$, see [9, Remark C.5.12].

3.2.4 The Dickson invariant

Next, for (Q, V) a quadratic space over a ring R with Spec R connected, the *Dickson invariant* is a map

$$\mathrm{D}_Q : O(Q) \to \mathbb{Z}/2\mathbb{Z},$$

as defined in [9, (C.2.2) and Remark C.2.5]. In the case (Q, V) is a quadratic space over a ring R such that Spec R is a disjoint union of finitely many connected components, such as when $R = \mathbb{Z}/n\mathbb{Z}$, we define the Dickson invariant as the resulting map

$$\mathrm{D}_Q : O(Q) \to (\mathbb{Z}/2\mathbb{Z})^{\#\pi_0(\mathrm{Spec}\, R)},$$

obtained by restricting to a given connected component of Spec R and then applying the Dickson invariant on that component.

In the case $R = \widehat{\mathbb{Z}}^{(p)}$, we define the Dickson invariant as the resulting composition

$$\mathrm{D}_Q : O(Q) \to \prod_{\text{primes } \ell \neq p} O(Q|_{\mathbb{Z}_\ell}) \xrightarrow{\prod_{\text{primes } \ell \neq p} \mathrm{D}_{Q|_{\mathbb{Z}_\ell}}} \prod_{\text{primes } \ell \neq p} \mathbb{Z}/2\mathbb{Z}.$$

In all cases above, for $\mathrm{D}_Q : O(Q) \to \prod_{s \in S} \mathbb{Z}/2\mathbb{Z}$ for an appropriate set S, we let $\Delta_{\mathbb{Z}/2\mathbb{Z}} : \mathbb{Z}/2\mathbb{Z} \to \prod_{s \in S} \mathbb{Z}/2\mathbb{Z}$ denote the diagonal inclusion sending $1 \mapsto (1, 1, \ldots, 1)$.

Warning 3.4 Our definition of the Dickson invariant for a quadratic space over $\widehat{\mathbb{Z}}^{(p)}$ may differ from the more general scheme theoretic definition given in [9, (C.2.2) and Remark C.2.5]. There, it is defined as a map to $(\mathbb{Z}/2\mathbb{Z})\,(\mathrm{Spec}\, R)$, the global sections of the locally constant sheaf $\mathbb{Z}/2\mathbb{Z}$ on Spec R. However, there is a natural map $(\mathbb{Z}/2\mathbb{Z})\,(\mathrm{Spec}\, \widehat{\mathbb{Z}}^{(p)}) \to \prod_{\text{primes } \ell \neq p} \mathbb{Z}/2\mathbb{Z}$, and our definition of the Dickson invariant is the composition of the Dickson invariant as in [9, (C.2.2) and Remark C.2.5] with this natural map.

Remark 3.5 In the case that 2 is invertible on R with Spec R connected, the Dickson invariant agrees with the determinant [9, Corollary C.3.2]. However, over a field k of characteristic 2, the determinant is trivial while the Dickson invariant is nontrivial (and it is nontrivial on k-points when the rank of the quadratic space is even) [9, Proposition C.2.8].

Over a field of characteristic 2, the Dickson invariant is sometimes also called the pseudodeterminant, and the following explicit description, which follows from the fact that reflections always have nontrivial Dickson invariant, will be useful: For any $T \in O(Q)$, and any expression of T as a product of reflections $T = r_{v_1} \cdots r_{v_s}$, (which exists so long as $(k, \mathrm{rk}\, V) \neq (\mathbb{F}_2, 4)$ by Remark 3.2,) the Dickson invariant is given by the map $O(Q) \to \mathbb{Z}/2\mathbb{Z}$ which sends $T \mapsto s \bmod 2$.

3.2.5 The Joint Kernel

Definition 3.6 Define $\Omega(Q) \subset O(Q)$ as $\Omega(Q) := \ker \mathrm{D}_Q \cap \ker \mathrm{sp}_Q^-$.

Because the -1-spinor norm agrees with the $+1$-spinor norm when restricted to $SO(Q)$, it follows that $\Omega(Q)$ is also the joint kernel of the Dickson map and the $+1$-spinor norm.

3.3 Notation for the monodromy representation

When $d > 0$, the map $\pi : \mathrm{Sel}^{\circ d}_{n,B} \to \mathscr{W}^{\circ d}_B$ is finite étale, representing a locally constant constructible sheaf of rank $12d - 4$ free $\mathbb{Z}/n\mathbb{Z}$ modules by [28, Corollary 3.22]. For B an integral noetherian $\mathbb{Z}[1/2n]$ scheme, letting V_n^d denote the rank $12d-4$ free $\mathbb{Z}/n\mathbb{Z}$ module corresponding to the geometric generic fiber of π, we obtain a monodromy representation $\rho^d_{n,B} : \pi_1(\mathscr{W}^{\circ d}_B) \to \mathrm{GL}(V_n^d)$ [28, Definitions 4.1 and 4.2].

Remark 3.7 Strictly speaking, we should keep track of base points in our fundamental groups. However, as we will ultimately be concerned with integral base schemes B, changing basepoint only changes the map $\rho^d_{n,k}$ by conjugation on the domain. Since we will only care about the image of $\rho^d_{n,k}$, we will often omit the basepoint from our notation.

For R a ring, we use $\rho^d_{n,R}$ to denote $\rho^d_{n,\mathrm{Spec}\, R}$.

3.3.1 The adelic monodromy map

For $n' \mid n$ both prime to $\mathrm{char}(k)$, we obtain a map $\mathrm{Sel}^{\circ d}_{n,R} \to \mathrm{Sel}^{\circ d}_{n',R}$ over $\mathscr{W}^{\circ d}_R$ induced by the corresponding map $\phi_{n,n'} : \mu_n \to \mu_{n'}$ sending $y \mapsto y^{n/n'}$ in the definition of $\mathrm{Sel}'^d_{n,R}$ from Sect. 2.1.4. Because $\phi_{n,n''} = \phi_{n',n''} \circ \phi_{n,n'}$, the monodromy maps $\rho^d_{n,R} : \pi_1(\mathscr{W}^{\circ d}_R) \to \mathrm{GL}(V_n^d)$ fit together compatibly to define a monodromy representation $\rho^d_{\widehat{\mathbb{Z}}^{(p)},R} : \pi_1(\mathscr{W}^{\circ d}_R) \to \mathrm{GL}(V^d_{\widehat{\mathbb{Z}}^{(p)}})$. For n prime to p, we have a natural reduction mod n map $r_n : \mathrm{GL}(V^d_{\widehat{\mathbb{Z}}^{(p)}}) \to \mathrm{GL}(V_n^d)$ and $\rho^d_{\widehat{\mathbb{Z}}^{(p)},R}$ is uniquely characterized by the property that for all n prime to p, $r_n\left(\rho^d_{\widehat{\mathbb{Z}}^{(p)},R}\right) = \rho^d_{n,R}$.

3.4 An equidistribution result

For $x \in \mathscr{W}'^d_{\mathbb{Z}[1/2]}$ let Frob_x be the conjugacy class of (geometric) Frobenius at x in $\pi_1(\mathscr{W}'^d_{\mathbb{Z}[1/2]})$. In this section we prove an equidistribution result for Frobenius classes in the monodromy group, in the large q limit. To state the proposition, we define the "mult" map.

Definition 3.8 Let X be a geometrically connected finite type scheme over $\mathbb{F}_q$, let G be a profinite group, and let $\lambda : \pi_1(X) \to G$ be a group homomorphism. Let G_0

denote the image of the composition $\pi_1^{\mathrm{geom}}(X) := \pi_1(X_{\overline{\mathbb{F}}_q}) \to \pi_1(X) \to G$ and let $\Gamma := G/G_0$. Then, we define $\mathrm{mult} : G \to \Gamma$ as the natural projection. Because $\pi_1(\mathrm{Spec}\,\mathbb{F}_q) = \pi_1(X)/\pi_1^{\mathrm{geom}}(X)$, we obtain a resulting map $\pi_1(\mathrm{Spec}\,\mathbb{F}_q) \to \Gamma$. We let γ_q denote the image in Γ of geometric Frobenius.

The following is an equidistribution result for Frobenii in a monodromy group, which is a generalization of [26, Theorem 1].

Proposition 3.9 *Let $\mathcal{X}$ be a smooth affine scheme of finite type over $\mathcal{O}[1/S]$, where $\mathcal{O}$ is a ring of integers in a number field, with geometrically irreducible fibers. For $\mathfrak{q}$ a maximal ideal of $\mathcal{O}[1/S]$ with residue field $\mathbb{F}_q$, write $X := \mathcal{X}|_{\mathcal{O}/\mathfrak{q}}$. Assume that we have a commutative diagram*

$$\begin{tikzcd}
1 \arrow[r] & \pi_1^{geom}(X) \arrow[r] \arrow[d, "\lambda_0"] & \pi_1(X) \arrow[r, "\deg"] \arrow[d, "\lambda"] & \widehat{\mathbb{Z}} \arrow[r] \arrow[d, "1\mapsto\gamma_q^{-1}"] & 1 \\
1 \arrow[r] & G_0 \arrow[r] & G \arrow[r, "\mathrm{mult}"] & \Gamma \arrow[r] & 1
\end{tikzcd} \tag{3.1}$$

with λ_0 tamely ramified and surjective, G a finite group, and Γ abelian. Suppose $C \subset G$ is a conjugacy-invariant subset. Then

$$Prob\{x \in X(\mathbb{F}_{q^n}) : \lambda(\mathrm{Frob}_x) \in C\} = \frac{\#C \cap G^{\mathrm{mult}\,\gamma_q^n}}{\#G_0} + O_{\mathcal{X}}\left(\#G\sqrt{\frac{\#C \cap G^{\mathrm{mult}\,\gamma_q^n}}{q^n}}\right).$$

where $G^{\mathrm{mult}\,\gamma_q^n} := \mathrm{mult}^{-1}(\gamma_q^n)$. Here the constant in the error term $O_{\mathcal{X}}\left(\#G\sqrt{\frac{\#C\cap G^{\mathrm{mult}\,\gamma_q^n}}{q^n}}\right)$ is independent of $\mathfrak{q}$, the choice of G, and the choice of λ, so long as λ_0 is tamely ramified and surjective.

Proof By the Lang–Weil bound, we have $\#\mathcal{X}(\mathbb{F}_q) = q^{\dim \mathcal{X}_{\mathbb{F}_q}} + O_{\mathcal{X}}(q^{\dim \mathcal{X}_{\mathbb{F}_q} - 1/2})$ and so after multiplying both sides by $\#\mathcal{X}(\mathbb{F}_q)$ (see also [26, Remark 2]), this statement nearly appears in [26, Theorem 1]. There are two differences however: First, Kowalski assumes that $\#G$ is prime to q instead of only that λ_0 is tamely ramified. Second, Kowalski works over a field instead of over $\mathcal{O}[1/S]$. The proof of Proposition 3.9 is the same as that given in [26, Theorem 1], once these two differences are addressed.

First we address the tamely ramified constraint. Indeed, a careful examination of the proof of [26, Theorem 1], shows that the only reason for assuming $\#G$ is prime to q appears in the reference to [25, Proposition 4.7], which in turn only uses this assumption in its reference to [25, Proposition 4.5], which in turn only uses this assumption in [25, (4.13)]. However, [25, (4.13)] holds whenever λ_0, or the associated map labeled ϕ in [25], is tamely ramified, see [21, 2.6, Cor 2.8]. We note that a generic hyperplane section of a tamely ramified cover remains tamely ramified, using Bertini's theorem to ensure that the hyperplane intersects the divisor of ramification generically. Hence, [25, Proposition 4.6], used in the proof of [25, Proposition 4.5], can be suitably generalized to include the assumption that the restriction of ϕ to the hyperplane is tamely ramified.

Second, we address the issue of working over $\mathcal{O}[1/S]$ in place of a finite field. The proof in [26] shows that if X comes as the reduction of a smooth $\mathcal{X}$ over $\mathcal{O}[1/S]$, then the constant in the error term $O_{\mathcal{X}}\left(\#G\sqrt{\frac{\#C}{q^n}}\right)$ of Proposition 3.9 can be taken to be a sum of (compactly supported) Betti numbers of $\mathcal{X}$, which is uniform in q by Ehresmann's Theorem and proper base change for compactly supported étale cohomology. This applies in particular to the Selmer spaces, as they are smooth over $\mathbb{Z}[1/2]$. □

In computing the image of the monodromy representation associated to the Selmer space, the following criterion for when an irreducible cover is geometrically connected will be crucial.

Corollary 3.10 *Let Y be a geometrically irreducible finite type $\mathbb{F}_q$ scheme and let $\pi : X \to Y$ be a finite étale connected Galois G cover corresponding to a surjective map $\rho : \pi_1(Y) \to G$ which is tamely ramified. Then, X is geometrically disconnected if and only if there exist infinitely many positive integers i such that for all $y \in Y(\mathbb{F}_{q^i})$, $\rho(\mathrm{Frob}_y) \neq \mathrm{id} \in G$.*

Proof If X is geometrically connected, then once i is sufficiently large, there do exist $y \in Y(\mathbb{F}_{q^i})$ with $\rho(\mathrm{Frob}_y) = \mathrm{id}$, using the equidistribution of Frobenius elements in G resulting from Proposition 3.9 (using that $G = G_0$ in that statement).

We next show the converse. Suppose X is geometrically disconnected and let j denote the number of components of $X_{\overline{\mathbb{F}}_q}$. We claim that for any i relatively prime to j, $X_{\mathbb{F}_{q^i}}$ is connected. Indeed, if $X_{\mathbb{F}_{q^i}}$ is disconnected, $\mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q) \simeq \mathbb{Z}/i\mathbb{Z}$ would act nontrivially on the components of $X_{\mathbb{F}_{q^i}}$, implying that $\gcd(j, i) > 1$.

To conclude the proof, it suffices to show that for any such i relatively prime to j, and any $y \in Y(\mathbb{F}_{q^i})$, $\rho(\mathrm{Frob}_y) \neq \mathrm{id} \in G$. Indeed, if $\rho(\mathrm{Frob}_y) = \mathrm{id} \in G$, the fiber of $\pi : X \to Y$ over y would necessarily be $\deg \pi$ copies of y, so in particular, X would have some $\mathbb{F}_{q^i}$ point. However, since $X_{\mathbb{F}_{q^i}}$ is connected but geometrically disconnected, the j geometric components of $X_{\overline{\mathbb{F}}_q}$ must be nontrivially permuted by the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^i})$. In particular, this Galois action on the fiber X_y over y must be nontrivial, and so X cannot have any $\mathbb{F}_{q^i}$ points. □

Corollary 3.11 *Retain the notation of Definition 3.8. For any $n \geq 1$ and $C \subset \mathrm{im}\,\rho^d_{n,\mathbb{Z}[1/2n]}$ a conjugacy class and $\mathbb{F}_q$ a finite field of characteristic p with $\gcd(p, 2n) = 1$, we have*

$$\frac{\#\left\{x \in \mathscr{W}^{\circ d}_{\mathbb{Z}[1/2n]}(\mathbb{F}_q) : \rho^d_{n,\mathbb{Z}[1/2n]}(\mathrm{Frob}_x) \in C\right\}}{\#\mathscr{W}^{\circ d}_{\mathbb{Z}[1/2n]}(\mathbb{F}_q)}$$

$$= \begin{cases} \frac{\#C}{\#\,\mathrm{im}\,\rho^d_{n,\overline{\mathbb{F}}_p}} + O_{n,d}\left(q^{-1/2}\right) & \textit{if } \mathrm{mult}(C) = \gamma_q, \\ 0 & \textit{if } \mathrm{mult}(C) \neq \gamma_q. \end{cases}$$

The same statement holds true with $\underline{\mathscr{W}}^{\circ d}_k$ in place of $\mathscr{W}^{\circ d}_k$.

Proof Note that in this setting, the tameness assumption on $\rho^d_{n,\overline{k}}$ was verified in the proof of [28, Proposition 4.9], see especially the end of the first paragraph of [28, p. 702]. The first statement follows immediately from Proposition 3.9. Note here that G and C as in the statement of Proposition 3.9 are fixed, and so we may absorb their orders into the constant in the error term $O_{n,d}(q^{-1/2})$.

To deduce the equidistribution statement for $\underline{\mathscr{W}}^{\circ d}_k$ from $\mathscr{W}^{\circ d}_k$, note that the monodromy representation for $\underline{\mathscr{W}}^{\circ d}_k$ is induced by the cover $\underline{\mathrm{Sel}}^{\circ d}_{n,k} \to \underline{\mathscr{W}}^{\circ d}_k$. Further $\mathrm{Sel}^{\circ d}_{n,k}$ is the pullback of $\underline{\mathrm{Sel}}^{\circ d}_{n,k}$ along $\mathscr{W}^{\circ d}_k \to \underline{\mathscr{W}}^{\circ d}_k$, i.e. the diagram

$$\begin{tikzcd}
\mathrm{Sel}^{\circ d}_{n,k} \arrow[r] \arrow[d] & \underline{\mathrm{Sel}}^{\circ d}_{n,k} \arrow[d] \\
\mathscr{W}^{\circ d}_k \arrow[r] & \underline{\mathscr{W}}^{\circ d}_k
\end{tikzcd}$$

is cartesian. In other words, the monodromy representation associated to $\mathrm{Sel}^{\circ d}_{n,k} \to \mathscr{W}^{\circ d}_k$ factors through $\pi_1(\mathscr{W}^{\circ d}_k) \twoheadrightarrow \pi_1(\underline{\mathscr{W}}^{\circ d}_k)$. This implies that if $x, y \in \mathscr{W}^{\circ d}_k$ map to the same point in $\underline{\mathscr{W}}^{\circ d}_k$ then $\rho^d_{n,k}(\mathrm{Frob}_x) = \rho^d_{n,k}(\mathrm{Frob}_y)$. Because $\underline{\mathscr{W}}^{\circ d}_k = [\mathscr{W}^{\circ d}_k/\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m]$, Lang's theorem applied to the group $\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m$ shows that each $z \in \underline{\mathscr{W}}^{\circ d}_k(\mathbb{F}_q)$ (counted with multiplicity according to automorphisms) has precisely $\mathbb{G}_a^{2d+1} \rtimes \mathbb{G}_m(\mathbb{F}_q)$ points lying over it in $\mathscr{W}^{\circ d}_k(\mathbb{F}_q)$, all mapping to the same conjugacy class under $\rho^d_{n,k}$. Therefore, the distribution of $\rho^d_{n,k}(\mathrm{Frob}_x)$ for $x \in \mathscr{W}^{\circ d}_k(\mathbb{F}_q)$ agrees with the distribution $\rho^d_{n,k}(\mathrm{Frob}_z)$ for $z \in \underline{\mathscr{W}}^{\circ d}_k(\mathbb{F}_q)$. □

3.5 Determining the image of monodromy

In [28, Theorem 4.4], a partial description of $\operatorname{im} \rho^d_{n,k}$ was given for k a field. The goal of this section is to precisely compute $\operatorname{im} \rho^d_{n,k}$. First, we recall the description from [28, Theorem 4.4]. Keeping notation as in Sect. 3.2.1, for (V, Q) a quadratic space over a ring R with a map $R \to \mathbb{Z}/n\mathbb{Z}$, we let $(V_n, Q_n) := (V_{\mathbb{Z}/n\mathbb{Z}}, Q_{\mathbb{Z}/n\mathbb{Z}})$ and let $r_n : O(Q) \to O(Q_n)$ denote the induced reduction $\bmod n$ map of orthogonal groups. We will be most concerned with the case $R = \mathbb{Z}$ or $R = \widehat{\mathbb{Z}}^{(p)}$.

In [28, Theorem 4.4] a quadratic space $(V^d_{\mathbb{Z}}, Q^d_{\mathbb{Z}})$ over $\mathbb{Z}$ is defined. This agrees with that defined in Definition 3.1 by [28, Remark 4.5]. With these definitions, [28, Theorem 4.4] states

$$r_n(O^*_-(Q^d_{\mathbb{Z}})) \subset \operatorname{im} \rho^d_{n,\overline{k}} \subset \operatorname{im} \rho^d_{n,k} \subset O(Q^d_n).$$

We next recall a slight generalization of the usual cyclotomic character, which we shall need to characterize $\operatorname{im} \rho^d_{n,k}$.

Definition 3.12 For k a field of characteristic p, allowing $p = 0$, we define the *cyclotomic character* as the map $\chi_{\mathrm{cyc}} : \mathrm{Gal}(\overline{k}/k) \to \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times$ defined as follows: For ν a positive integer with $(\nu, p) = 1$ when $p > 0$ and ν arbitrary when $p = 0$, let ζ_ν be a primitive νth root of unity. For $\sigma \in \mathrm{Gal}(\overline{k}/k)$, suppose $\sigma(\zeta_\nu) = \zeta_\nu^{a_{\nu,\sigma}}$. Then, define $\chi_{\mathrm{cyc}}(\sigma) := (a_{\nu,\sigma})_\nu$, considered as an element of $\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times$.

Remark 3.13 Note that χ_{cyc} of Definition 3.12 is the usual cyclotomic character when $\mathrm{char}(k) = 0$. Further, from the definition, in the case $p \neq 0$, $k = \mathbb{F}_p$, and q is a power of p, we have $\chi_{\mathrm{cyc}}(\mathrm{Frob}_q) = q \in \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times$.

For the statement of Theorem 3.14, recall the notation for the spinor norm and Dickson invariant from Sect. 3.2. Also, let $\Delta_{\mathbb{Z}/2\mathbb{Z}} : \mathbb{Z}/2\mathbb{Z} \to \prod_{\text{primes } \ell \neq p} \mathbb{Z}/2\mathbb{Z}$ the diagonal inclusion. For k a field of characteristic p and $d \in \mathbb{Z}_{\geq 2}$, let χ^{d-1} denote the composition

$$\mathrm{Gal}(\overline{k}/k) \xrightarrow{\chi_{\mathrm{cyc}}^{d-1}} \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times \to \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times / \left(\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times\right)^2.$$

Theorem 3.14 *Let k be a field of characteristic p, allowing $p = 0$, and let $d \in \mathbb{Z}_{\geq 2}$. With $\Delta_{\mathbb{Z}/2\mathbb{Z}}$ and χ^{d-1} defined above,*

$$\mathrm{im}\, \rho^d_{n,k} = D^{-1}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}(\mathrm{im}\, \Delta_{\mathbb{Z}/2\mathbb{Z}}) \cap \left(sp^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}\right)^{-1}(\mathrm{im}\, \chi^{d-1}).$$

Example 3.15 Let's explicate what Theorem 3.14 says in the cases

- If k is algebraically closed or d is odd, then

$$\mathrm{im}\, \rho^d_{\widehat{\mathbb{Z}}^{(p)},\overline{k}} = \mathrm{D}^{-1}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}(\mathrm{im}\, \Delta_{\mathbb{Z}/2\mathbb{Z}}) \cap \ker\left(\mathrm{sp}^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}\right).$$

- If d is even and $k = \mathbb{F}_q$ has characteristic $p > 0$, using Remark 3.13, we have

$$\mathrm{im}\, \rho^d_{\widehat{\mathbb{Z}}^{(p)},k} = \mathrm{D}^{-1}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}(\mathrm{im}\, \Delta_{\mathbb{Z}/2\mathbb{Z}}) \cap (\mathrm{sp}^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}})^{-1}(\langle [q] \rangle)$$

where $\langle [q] \rangle$ is the group generated by the class of q.

We will prove Theorem 3.14 at the end of this section in Sect. 3.10. The general outline of the proof is as follows. First, in Sect. 3.6, we show the image of the monodromy representation contains $\Omega(Q^d_{\widehat{\mathbb{Z}}^{(p)}})$. Next, in Sect. 3.7, we explain how to compute the spinor norm and Dickson invariant of images of Frobenius, in certain cases. Then, in Sect. 3.8 and Sect. 3.9 we compute the spinor norm and Dickson invariants on $\mathrm{im}\, \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}$, for k a finite field. Finally, we piece these parts together in Sect. 3.10.

3.6 Showing the monodromy is big

We next explain how to deduce $\Omega(Q^d_{\widehat{\mathbb{Z}}^{(p)}}) \subset \mathrm{im}\, \rho^d_{\widehat{\mathbb{Z}}^{(p)},\overline{k}}$ by combining [28, Theorem 4.4] with some group theory.

Lemma 3.16 *For $d \geq 2$ and $n \geq 1$, we have $r_n(O^*_-(Q^d_{\mathbb{Z}})) \supset \Omega(Q^d_n)$. In particular, combining this with [28, Theorem 4.4] gives $\Omega(Q^d_n) \subset \operatorname{im} \rho^d_{n,\overline{k}}$ and so $\Omega(Q^d_{\widehat{\mathbb{Z}}^{(p)}}) \subset \operatorname{im} \rho^d_{\widehat{\mathbb{Z}}^{(p)},\overline{k}}$.*

Proof The last sentence follows from the first by [28, Theorem 4.4], which says $O^*_-(Q^d_{\mathbb{Z}}) \subset \operatorname{im} \rho^d_{\widehat{\mathbb{Z}}^{(p)},\overline{k}}$.

We turn our attention to proving the first statement. For every $v \in V^d_n$, with $Q^d_n(v) = -1$, there exists a lift $\widetilde{v} \in V^d_{\mathbb{Z}}$ with $Q^d_{\mathbb{Z}}(\widetilde{v}) = -1$, as is shown in the proof of [11, Lemma 4.13] (which implicitly assumes $d \geq 2$ so that $(V^d_{\mathbb{Z}}, Q^d_{\mathbb{Z}})$ contains summands isomorphic to the hyperbolic plane). Let $R(Q^d_n)$ denote the subgroup of $O(Q^d_n)$ generated by elements of the form r_w for $v \in V^d_n$ and let $R'(Q^d_n)$ denote the subgroup of $O(Q^d_n)$ generated by elements of the form $r_v \circ r_w$ for $v, w \in V^d_n$ with $Q^d_n(v) = Q^d_n(w) = -1$. We next show $R(Q^d_n) = O(Q^d_n)$ and $R'(Q^d_n) = \Omega(Q^d_n)$.

Recall a quadratic space (V, Q) over $\mathbb{Z}$ is *unimodular* if B_Q is invertible as a linear transformation over $\mathbb{Z}$ or equivalently the natural map induced by B_Q from V to $V^\vee$, the dual lattice, is an isomorphism.

In the case that n is a prime power, since $(V^d_{\mathbb{Z}}, Q^d_{\mathbb{Z}})$ is unimodular and nondegenerate of rank more than 5 (see [28, Remark 4.5]), it follows from [24, Satz 2] that $R(Q^d_n) = O(Q^d_n)$. By [24, Satz 3] it follows $R'(Q^d_n) = \Omega(Q^d_n)$. Note that [24, Satz 3] is stated for $R'(Q^d_n)$ generated by elements of the form $r_v \circ r_w$ for $v, w \in V^d_n$ with $Q^d_n(v) = Q^d_n(w) = 1$, instead of $Q^d_n(v) = Q^d_n(w) = -1$. However, we may arrange the latter by applying [24, Satz 3] to $-Q^d_n$ in place of Q^d_n. Therefore, $\Omega(Q^d_n) = R'(Q^d_n) \subset r_n(O(Q^d_{\mathbb{Z}}))$.

For the general case, write $n = \prod_{i=1}^t p_i^{a_i}$ for pairwise distinct primes p_i. Since $\Omega(Q^d_n) = \prod_{i=1}^t \Omega(Q^d_{p_i^{a_i}})$, it suffices to show the image of $\Omega(Q^d_{p_i^{a_i}}) \to \prod_{i=1}^t \Omega(Q^d_{p_i^{a_i}})$, included as the ith component, is contained in $r_n(O^*_-(q))$. For this, choose $v, w \in V^d_{p_i^{a_i}}$ with $Q^d_{p_i^{a_i}}(v) = Q^d_{p_i^{a_i}}(w) = -1$ and choose lifts $\widetilde{v}, \widetilde{w}$ to V^d_n so that $\widetilde{v} \equiv \widetilde{w} \mod \prod_{1 \leq j \leq n, j \neq i} p_j^{a_j}$ and $Q^d_n(\widetilde{v}) = Q^d_n(\widetilde{w}) = -1$. We then find that $r_{\widetilde{v}} \circ r_{\widetilde{w}}$ agrees with $r_v \circ r_w$ when reduced $\mod p_i^{a_i}$ and is the identity when reduced $\mod p_j^{a_j}$ for any $j \neq i$. It follows that $r_n(O^*_-(q)) \supset \operatorname{im}(\Omega(Q^d_{p_i^{a_i}}) \to \prod_{i=1}^t \Omega(Q^d_{p_i^{a_i}}))$, as desired. □

3.7 Tools to compute the Dickson invariant and spinor norm of Frobenius

In this section, we prove Proposition 3.17 which allows us to compute the spinor norm and Dickson invariants of the images of Frobenius elements under the monodromy representation. The following result essentially appears as [46, Proposition 2.9], where an analog is stated over $\mathbb{Z}/\ell\mathbb{Z}$ in place of $\widehat{\mathbb{Z}}^{(p)}$. The following generalization has essentially the same proof, using that L-functions associated to elliptic curves are power series with coefficients in $\mathbb{Z}$. Slight care must be taken to deal with the fact that the determinant disagrees with the Dickson invariant over fields of characteristic 2.

For E an elliptic curve over $\mathbb{F}_q(t)$, we let $L(T, E)$ denote the *L-function* associated to E and let $\varepsilon_E \in \{\pm 1\}$ denote *root number* associated to E, see [46, Sect. 2.3] and [46, Sect. 2.2] respectively for a definitions. The only property of root numbers we will use is that they appear in the functional equation of the L function associated to E. Recall our notation $[E_x] = x \in \mathscr{W}'^d_k$ where E_x is the elliptic curve corresponding to x as in Remark 2.2.

Proposition 3.17 *(Mild generalization of [46, Proposition 2.9]) Let $d \geq 1$.*

(1) For $[E_x] = x \in \mathscr{W}^{\circ d}_{\mathbb{F}_p}(\mathbb{F}_q)$, $D_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}(\rho^d_{\widehat{\mathbb{Z}}^{(p)},k}(\mathrm{Frob}_x)) = \Delta_{\mathbb{Z}/2\mathbb{Z}}((1 - \varepsilon_{E_x})/2)$.

(2) For $[E_x] = x \in \mathscr{W}^{\boxslash d}_{\mathbb{F}_p}(\mathbb{F}_q)$, whenever $\det(\mathrm{id} - \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}(\mathrm{Frob}_x)) \neq 0$, we have

$$sp^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}(\rho^d_{\widehat{\mathbb{Z}}^{(p)},k}(\mathrm{Frob}_x)) = [q^{d-1}],$$

where $[q]$ is the class of the integer q in $\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times / \left(\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times\right)^2$.

In order to prove Proposition 3.17 we will need the following Lemma, which is essentially shown in [46, p. 10].

Lemma 3.18 *Let $d \geq 1$, p an odd prime, ℓ a prime with $\ell \neq p$, and $[E_x] = x \in \mathscr{W}^{\boxslash d}_{\mathbb{F}_p}(\mathbb{F}_q)$. Then, letting $L(T, E_x)$ be the L-function associated to E_x, we have*

$$\det(\mathrm{id} - \rho^d_{\mathbb{Z}_\ell,\mathbb{F}_p}(\mathrm{Frob}_x)T | V^d_{\mathbb{Z}_\ell}) = L(T/q, E_x),$$

viewed as an equality of polynomials with coefficients in $\mathbb{Z}_\ell$. In particular, the analytic rank of E_x is equal to the $\mathbb{Z}_\ell$-rank of the generalized 1-eigenspace of $\rho^d_{\mathbb{Z}_\ell,\mathbb{F}_p}(\mathrm{Frob}_x)$ on $V^d_{\mathbb{Z}_\ell}$.

Proof Let $L(T, E_x)$ denote the L-function of E_x, which is in fact a polynomial of degree $12d - 4$ with integral coefficients [46, Theorem 2.2]. Define $g_{x,\ell} := \rho^d_{\mathbb{Z}_\ell,\mathbb{F}_p}(\mathrm{Frob}_x)$. It suffices to show that

$$\det(\mathrm{id} - g_{x,\ell}T | V^d_{\mathbb{Z}_\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) = L(T/q, E_x)$$

viewed as an equality with coefficients in $\mathbb{Q}_\ell$. As explained in [46, p. 10], we have

$$L(T/q, E_x) = \det(\mathrm{id} - \mathrm{Frob}_x\, T | H^1(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, j_* T_\ell(E_{\overline{x}})) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$$

where $j_* T_\ell(E_{\overline{x}})$ is defined as follows. Let U denote the open subscheme of $\mathbb{P}^1_{\overline{\mathbb{F}}_q}$ over which the minimal proper regular model of E_x is smooth. Let $j : U \to \mathbb{P}^1_{\overline{\mathbb{F}}_q}$ denote the inclusion morphism. Let $E_{\overline{x}}[\ell^k]$ denote the rank 2 locally free sheaf of $\mathbb{Z}/\ell^k\mathbb{Z}$ modules parameterizing the ℓ^k torsion of the smooth minimal proper regular model of $E_{\overline{x}}$ over

U with $j_*E_x[\ell^j]$ the pushforward sheaf on $\mathbb{P}^1_{\overline{\mathbb{F}}_q}$. Define $j_*T_\ell(E_{\overline{x}}) := \varprojlim_k j_*E_{\overline{x}}[\ell^k]$ with transition maps $j_*E_x[\ell^{k+1}] \to j_*E_x[\ell^k]$ given by multiplication by ℓ.

We next identify $H^1(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, j_*T_\ell(E_{\overline{x}}))$ with $V^d_{\mathbb{Z}_\ell}$ so as to compare this representation with $\rho^d_{\mathbb{Z}_\ell,\mathbb{F}_p}$. By Lemma 2.7, there is a natural identification between the geometric fiber of the Selmer space over x, $\mathrm{Sel}^{\boxslash^d}_{\ell^k,\mathbb{F}_p} \times_{\mathscr{W}^{\boxslash^d}_{\mathbb{F}_p},x} \operatorname{Spec} \overline{\mathbb{F}}_q \simeq H^1(\mathbb{P}^1_{\overline{\mathbb{F}}_q}, j_*E_{\overline{x}}[\ell^k])$. Further, these are both free $\mathbb{Z}/\ell^k\mathbb{Z}$ modules of rank $12d-4$ by [28, Corollary 3.19]. By compatibility of these isomorphisms with the maps $E[\ell^{k+1}] \to E[\ell^k]$ we obtain the equality $\det(\mathrm{id} - g_{x,\ell}T | V^d_{\mathbb{Z}_\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) = L(T/q, E_x)$, viewed as an equality of polynomials with coefficients in $\mathbb{Q}_\ell$.

To conclude the proof, it remains to explain why the final statement regarding analytic rank follows from the equality $\det(\mathrm{id} - g_{x,\ell}T) = L(T/q, E_x)$. The analytic rank is the largest power of $T-1$ dividing $L(T/q, E_x) = \det(\mathrm{id} - g_{x,\ell}T)$. This agrees with the largest power of $T-1$ dividing $\det\left(g^{-1}_{x,\ell} - T\right)$, which is the characteristic polynomial of $g^{-1}_{x,\ell}$. Hence, the analytic rank agrees with the dimension of the generalized 1-eigenspace of $g^{-1}_{x,\ell}$, which is the same as the dimension of the generalized 1-eigenspace of $g_{x,\ell}$. □

Proof of Proposition 3.17 Define $g_{x,\ell} := \rho^d_{\mathbb{Z}_\ell,\mathbb{F}_p}(\mathrm{Frob}_x)$. First, we verify (1) regarding the Dickson invariant. From the definition of the Dickson invariant from Sect. 3.2.4, to compute the $\mathrm{D}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}(\rho^d_{\widehat{\mathbb{Z}}^{(p)},\mathbb{F}_p}(\mathrm{Frob}_x))$, it is equivalent to compute $\mathrm{D}_{Q^d_{\mathbb{Z}_\ell}}(\rho^d_{\mathbb{Z}_\ell,\mathbb{F}_p}(\mathrm{Frob}_x))$ for each prime $\ell \neq p$ separately and show this is equal to $(1-\varepsilon_{E_x})/2$.

Next, observe that $\det(T - g_{x,\ell}) = \det(T - g^{-1}_{x,\ell})$.

Indeed, for any nondegenerate quadratic space (V, Q) and $M \in O(Q)$, and for M^t the transpose of M, we have $M^t B_Q M = B_Q \implies M^t = B_Q^{-1} M^{-1} B_Q$. Hence, the characteristic polynomial of M agrees with that of M^t which agrees with that of M^{-1}. Therefore, the characteristic polynomial of $g_{x,\ell}$ agrees with that of $g^{-1}_{x,\ell}$ using $g_{x,\ell} \in O(Q^d_{\mathbb{Z}_\ell})$ by the easier containment of [28, Theorem 4.4].

Therefore, we have

$$\begin{aligned} T^{12d-4}\det(\mathrm{id} - g_{x,\ell}T^{-1}) &= \det(T - g_{x,\ell}) = \det(T - g^{-1}_{x,\ell}) \\ &= \det(-g^{-1}_{x,\ell})\det(\mathrm{id} - g_{x,\ell}T) \\ &= (-1)^{12d-4}\det(g_{x,\ell})\det(\mathrm{id} - g_{x,\ell}T) \\ &= \det(g_{x,\ell})\det(\mathrm{id} - g_{x,\ell}T). \end{aligned}$$

By [46, Theorem 2.2] in conjunction with Lemma 3.18, we also have

$$T^{12d-4}\det(\mathrm{id} - g_{x,\ell}T^{-1}) = \varepsilon_{E_x}\det(\mathrm{id} - g_{x,\ell}T),$$

implying $\det(g_{x,\ell}) = \varepsilon_{E_x}$. Note that in the case $\ell = 2$, we are using crucially that we are working over $\mathbb{Z}_2$ which does not have characteristic 2. The relation between the Dickson invariant and the determinant for matrices over $\mathbb{Z}_2$ given in [9, Corollary C.3.2] implies (1).

We next verify (2). It suffices to verify $\mathrm{sp}^-_{Q^d_{\mathbb{Z}_\ell}}(\rho^d_{\mathbb{Z}_\ell,k}(\mathrm{Frob}_x)) = [q^{d-1}]$, for every prime $\ell \neq p$. As in the previous part, let $g_{x,\ell} := \rho^d_{\mathbb{Z}_\ell,\mathbb{F}_p}(\mathrm{Frob}_x)$. First, observe that as $\det(\mathrm{id} - g_{x,\ell}) \neq 0$, it follows that $g_{x,\ell}$ has trivial 1-eigenspace. Because the Dickson invariant for an orthogonal group over a nondegenerate free module of even rank is congruent to the rank of the 1-eigenspace mod 2 by [39, p. 160], we find $g_{x,\ell} \in SO(Q^d_{\mathbb{Z}_\ell})$. Therefore, $\mathrm{sp}^-_{Q^d_{\mathbb{Z}_\ell}}(g_{x,\ell}) = \mathrm{sp}^+_{Q^d_{\mathbb{Z}_\ell}}(g_{x,\ell})$. By [45, Sect. 2, Cor.] (see also [9, Theorem C.5.7]), and $\mathrm{sp}^-_{Q^d_{\mathbb{Z}_\ell}}(-1) = \mathrm{disc}(Q^d_{\mathbb{Z}_\ell})$ [9, Lemma C.5.8], one can compute the spinor norm of $g_{x,\ell}$ as

$$\begin{aligned}
\mathrm{sp}^-_{Q^d_{\mathbb{Z}_\ell}}(g_{x,\ell}) &= \mathrm{sp}^+_{Q^d_{\mathbb{Z}_\ell}}(g_{x,\ell}) \\
&= \mathrm{sp}^+_{Q^d_{\mathbb{Z}_\ell}}(-\mathrm{id})\mathrm{sp}^+_{Q^d_{\mathbb{Z}_\ell}}(-g_{x,\ell}) \\
&= \mathrm{disc}(Q^d_{\mathbb{Z}_\ell}) \cdot \det\left(\frac{1-g_{x,\ell}}{2}\right) \cdot (\mathbb{Z}_\ell^\times)^2 = 2^{\mathrm{rk}\, V^d_{\mathbb{Z}_\ell}} \det(1-g_{x,\ell})) \cdot (\mathbb{Z}_\ell^\times)^2 \\
&= \det(\mathrm{id} - g_{x,\ell}) \cdot (\mathbb{Z}_\ell^\times)^2.
\end{aligned}$$

Then, using the identification $\det(\mathrm{id} - g_{x,\ell}T | V^d_{\mathbb{Z}_\ell}) = L(T/q, E_x)$ of Lemma 3.18,

$$\mathrm{sp}^-_{Q^d_{\mathbb{Z}_\ell}}(g_{x,\ell}) = \det(\mathrm{id} - g_{x,\ell}) \cdot (\mathbb{Z}_\ell^\times)^2 = L(1/q, E_x) \cdot (\mathbb{Z}_\ell^\times)^2.$$

To conclude the proof, we only need check $L(1/q, E) \in q^{d-1}(\mathbb{Z}_\ell^\times)^2$. In fact, considering $L(T, E)$ as a polynomial with integer coefficients, we will verify $L(1/q, E) \in q^{d-1}(\mathbb{Q}^\times)^2$, and the fact that both $L(1/q, E)$ and q^{d-1} lie in $\mathbb{Z}_\ell^\times$ will imply they agree up to a square in $\mathbb{Z}_\ell^\times$. Since $\det(\mathrm{id} - g_{x,\ell}) = L(1/q, E_x)$ and $\det(\mathrm{id} - g_{x,\ell}) \neq 0$, we find that the L function of E_x has analytic rank 0, meaning that $\mathrm{ord}_{T=1/q} L(T, E_x) = 0$ or equivalently $L(1/q, E_x) \neq 0$. It follows from [46, Corollary 2.6] (as is deduced from the Birch and Swinnerton Dyer conjecture, applicable because the analytic rank and algebraic rank are both 0) that $L(1/q, E_x) = q^{0-1+d} c_{E_x} \cdot \left(\mathbb{Q}^\times\right)^2$, for c_{E_x} the Tamagawa number of E_x. Observing that $c_{E_x} = 1$ as $x \in \mathscr{W}^{\circ d}_k$, we find $L(1/q, E_x) = q^{-1+d} \cdot \left(\mathbb{Q}^\times\right)^2$, as desired. □

3.8 Controlling the Dickson invariant

Using Proposition 3.17, we next compute the image of $\mathrm{im}\, \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}$ under the Dickson invariant map.

Lemma 3.19 *For any field k of characteristic $p \neq 2$ (allowing $p = 0$) and any height $d \geq 2$, the image of the map*

$$D_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}} \circ \rho^d_{\widehat{\mathbb{Z}}^{(p)},k} : \pi_1(\mathscr{W}^{\circ d}_k) \to \prod_{primes\ \ell \neq p} \mathbb{Z}/2\mathbb{Z}$$

is $\mathrm{im}(\Delta_{\mathbb{Z}/2\mathbb{Z}})$.

Proof First, because $r_n(O^*_-(Q^d_{\mathbb{Z}})) \subset \rho^d_{n,\overline{k}}$ by [28, Theorem 4.4], the Dickson invariant must be nontrivial on im $\rho^d_{n,\overline{k}}$, as it is nontrivial on $O^*_-(Q^d_{\mathbb{Z}})$. Therefore, it is similarly nontrivial on im $\rho^d_{\widehat{\mathbb{Z}}^{(p)},\overline{k}}$. Therefore, to conclude the proof, it suffices to show im $\mathrm{D}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}} \circ \rho^d_{\widehat{\mathbb{Z}}^{(p)},k} \subset$ im $\Delta_{\mathbb{Z}/2\mathbb{Z}}$. Further, from the definition of profinite groups as a limit of finite groups, it suffices to show that for any integer n of the form $n = \ell_1 \cdots \ell_t$, for primes $\ell_1, \ldots, \ell_t$ with no $\ell_i = p$, im $\mathrm{D}_{Q^d_n} \circ \rho^d_{n,k}$ is contained in im $\Delta_{\mathbb{Z}/2\mathbb{Z}}$.

By base change, it suffices to establish the containment im $\mathrm{D}_{Q^d_n} \circ \rho^d_{n,k} \subset$ im $\Delta_{\mathbb{Z}/2\mathbb{Z}}$ when k is either $\mathbb{Q}$ or a finite field of odd characteristic. If the composition $\mathrm{D}_{Q^d_n} \circ \rho^d_{n,k}$ defines a surjective map $\pi_1(\mathscr{W}^{\circ d}_k) \to G$, we obtain a resulting finite étale Galois G-cover $U_{G,n,d,k} \to \mathscr{W}^{\circ d}_k$. By Chebotarev density, for example as in [12, Lemma 1.2], it suffices to establish that $U_{G,n,d,\mathbb{Q}}$ is geometrically connected and to establish the claim for all finite fields k of odd characteristic. Further, geometric irreducibility for $U_{G,n,d,\mathbb{Q}}$ follows from geometric irreducibility of $U_{G,n,d,\mathbb{F}_p}$ for all but finitely many primes p, because $U_{G,n,d,k} \to \mathscr{W}^{\circ d}_k \to \mathrm{Spec}\, k$ is in fact the base change of a map $U_{G,n,d,\mathbb{Z}[1/2]} \to \mathscr{W}^{\circ d}_{\mathbb{Z}[1/2]} \to \mathrm{Spec}\, \mathbb{Z}[1/2]$, and the set of fibers on which a map is geometrically connected is constructible [16, Corollaire 9.7.9]. Hence, it suffices to demonstrate that for each finite field k of odd characteristic, im $\mathrm{D}_{Q^d_n} \circ \rho^d_{n,k}$ is contained in im $\Delta_{\mathbb{Z}/2\mathbb{Z}}$ and $U_{G,n,d,k}$ is geometrically connected.

For all finite fields k of odd characteristic and all $x \in \mathscr{W}^{\circ d}_k(k)$, by Proposition 3.17 we have $\mathrm{D}_{Q^d_n} \circ \rho^d_{n,k}(\mathrm{Frob}_x) \subset$ im $\Delta_{\mathbb{Z}/2\mathbb{Z}}$. For all sufficiently large finite fields of odd characteristic, it follows from Proposition 3.9 applied to the G-cover $U_{G,n,d,k} \to \mathscr{W}^{\circ d}_k$ constructed above that im $\mathrm{D}_{Q^d_n} \circ \rho^d_{n,k} \subset$ im $\Delta_{\mathbb{Z}/2\mathbb{Z}}$. Since the reverse containment also holds, we have equality for all sufficiently large (in the sense of divisibility of cardinality) finite fields.

We claim that the cover $U_{G,n,d,k} \to \mathscr{W}^{\circ d}_k$ is tamely ramified. Indeed, this holds because we are assuming k does not have characteristic 2, while the cover $U_{G,n,d,k} \to \mathscr{W}^{\circ d}_k$ has degree which is a power of 2 because the Dickson invariant takes values in a 2-group.

It follows from Corollary 3.10 that over any finite field k, the resulting G-cover is geometrically connected, and so the containment $\mathrm{D}_{Q^d_n} \circ \rho^d_{n,k}(\mathrm{Frob}_x) \subset$ im $\Delta_{\mathbb{Z}/2\mathbb{Z}}$ in fact holds for all finite fields of odd characteristic. □

3.9 Controlling the spinor norm

We next use Proposition 3.17(2) to analyze the spinor norm applied to im $\rho^{d}_{\widehat{\mathbb{Z}}^{(p)},k}$. The general strategy in what follows will be to compute the image of the spinor norm restricted to the kernel of the Dickson invariant, and then use this to deduce the joint image of the spinor norm and Dickson invariant.

For this proof, we will need to know there are many elliptic curves $[E_x] \in \mathscr{W}^{\circ d}_k$ with trivial 1-eigenspace. This will follow from the group theoretic statement soon established in Proposition 3.22. In order to state this precisely, we recall a relevant distribution on the ℓ-adic points of a finite type scheme from [1]. All but the last statement appears in [1, Lemma 2.1(b)], while the last statement appears in [35, Corollaire, p. 146].

Lemma 3.20 *Let X be a finite type $\mathbb{Z}_\ell$ scheme of dimension d and equip $X(\mathbb{Z}_\ell)$ with the ℓ-adic topology. There exists a unique bounded $\mathbb{R}_{\geq 0}$-valued measure μ_X on the Borel σ-algebra of $X(\mathbb{Z}_\ell)$ such that for any open and closed subset S of $X(\mathbb{Z}_\ell)$, we have*

$$\mu_X(S) = \lim_{e\to\infty} \frac{\#\,(\textit{image of } S \textit{ in } X(\mathbb{Z}/\ell^e\mathbb{Z}))}{(\ell^e)^d}.$$

If $Y \subset X$ is a subscheme of dimension $< d$, $\mu_X(Y(\mathbb{Z}_\ell)) = 0$ and

$$\#\left(\mathrm{im}\left(Y(\mathbb{Z}/\ell^e\mathbb{Z}) \to X(\mathbb{Z}/\ell^e\mathbb{Z})\right)\right) = O_Y(\ell^{e(d-1)}).$$

Remark 3.21 Lemma 3.20 is correct as stated, but the proof in [1, Proposition 2.1(b)] has a minor error. There, it is stated that $\#Y(\mathbb{Z}/\ell^e\mathbb{Z}) = O\left((\ell^e)^{d-1}\right)$, which is not in general true. The correct statement is that $\mathrm{im}\,(Y(\mathbb{Z}_\ell) \to Y(\mathbb{Z}/\ell^e\mathbb{Z})) = O\left((\ell^e)^{d-1}\right)$. A counterexample to the incorrect statement is provided by the subscheme $Y = \mathrm{Spec}\,\mathbb{Z}[x]/(x^2)$ and $X = \mathbb{A}^1_{\mathbb{Z}_\ell}$. In this case, we easily see that $\#Y(\mathbb{Z}_\ell) = 1$ because $\mathbb{Z}_\ell$ is reduced, but $\#Y(\mathbb{Z}/\ell^e\mathbb{Z}) = \ell^{\lfloor e/2 \rfloor}$ as such points are in bijection with elements of $\mathbb{Z}/\ell^e\mathbb{Z}$ which square to 0.

In the following proposition only, we use $O(Q)$ and $SO(Q)$ to denote the algebraic groups associated to a quadratic form Q, and $O(Q)(R)$ to denote its Spec R points, for R a ring.

Proposition 3.22 *Let (V, Q) be a nondegenerate quadratic space of even rank at least 4 over $\mathbb{Z}_\ell$. There is a Zariski closed pure codimension 1 subscheme $Z \subset O(Q)$, such that $g \in Z$ if and only if g has a generalized 1-eigenspace of dimension at least 2.*

Further, any $g \in (O(Q) - Z)(\mathbb{Z}_\ell)$ has a zero dimensional generalized 1-eigenspace and zero dimensional 1-eigenspace when $g \in SO(Q)(\mathbb{Z}_\ell)$ and a one dimensional generalized 1-eigenspace and one dimensional 1-eigenspace when $g \notin SO(Q)(\mathbb{Z}_\ell)$.

In particular, $Z(\mathbb{Z}_\ell)$ has measure 0 with respect to the distribution of Lemma 3.20.

Proof For V_L an even dimensional free module over a field L and $g : V_L \to V_L$, let $V_L^{g=\lambda}$ denote the λ-eigenspace and $V_L^{[g=\lambda]}$ denote the generalized λ-eigenspace.

Let Q_L be a nondegenerate quadratic form on V_L. Recall that the Dickson invariant agrees with $\dim V_L^{g=1} \mod 2$, using that $\dim V_L$ is even and [39, p. 160]. (In [39, p. 160] the notation $[V, f]$ is used for $\mathrm{im}(1-f)$, whose rank taken $\mod 2$ agrees with $\dim V_L^{g=1} \mod 2$ since $\dim V_L$ is even.)

In particular, every element in $(O(Q_L) - SO(Q_L))(L)$ has odd dimensional 1-eigenspace while every element of $SO(Q_L)(L)$ has even dimensional 1-eigenspace. Now, let (V, Q) be a nondegenerate even rank quadratic space over $\mathbb{Z}_\ell$ as in the statement of the proposition. We may apply the above discussion to the base change $(V_{\mathbb{Q}_\ell}, Q_{\mathbb{Q}_\ell})$ to deduce that any element $g \in SO(Q)(\mathbb{Z}_\ell)$ has $\mathrm{rk}\, V_L^{g=1} \equiv 0 \mod 2$ and any element of $g \in (O(Q) - SO(Q))(\mathbb{Z}_\ell)$ has $\mathrm{rk}\, V_{\mathbb{Q}_\ell}^{g=1} \equiv 1 \mod 2$.

Further, the condition that an element $g \in SO(Q)(\mathbb{Z}_\ell)$ has $\mathrm{rk}\, V_{\mathbb{Q}_\ell}^{[g=1]} > 0$ is Zariski closed and nonempty in the algebraic group $SO(Q)$ over $\mathbb{Z}_\ell$; it is Zariski closed because this condition can be expressed as $T - 1$ dividing the characteristic polynomial of g and it is nonempty because there are elements in a maximal torus with $\dim V_{\mathbb{Q}_\ell}^{g=1} = 0$. Similarly, the condition that an element $g \in (O(Q) - SO(Q))(\mathbb{Z}_\ell)$ has $\mathrm{rk}\, V_{\mathbb{Q}_\ell}^{[g=1]} > 1$ is Zariski closed and nonempty. (This uses that $\mathrm{char}\, \mathbb{Z}_\ell = 0 \neq 2$, as in characteristic 2 every element of $O(Q) - SO(Q)$ would have generalized 1 eigenspace of dimension at least 2.) Therefore, to establish the statement regarding generalized 1-eigenspaces, it suffices to show that a proper Zariski closed subscheme of an integral scheme over $\mathbb{Z}_\ell$ parameterizes a measure 0 subset, which is the content of Lemma 3.20.

The statement for generalized 1-eigenspaces established above implies the corresponding statement for 1-eigenspaces because when the generalized 1-eigenspace is at most 1 dimensional, it is equal to the 1-eigenspace. The final statement that $Z(\mathbb{Z}_\ell)$ has measure 0 follows from Lemma 3.20. □

We next define a double cover $\mathscr{Z}_k^d \to \mathscr{W}^{\circ d}_k$ so that the Dickson invariant is trivial on $\pi_1(\mathscr{Z}_k^d)$.

Definition 3.23 Let $n \geq 1, d \geq 2$, and let k be an integral domain (not necessarily a field) on which $2n$ is invertible. By Lemma 3.19, the Dickson invariant defines a surjective map $\pi_1(\mathscr{W}^{\circ d}_k) \to \mathbb{Z}/2\mathbb{Z}$ and hence corresponds to a finite étale $\mathbb{Z}/2\mathbb{Z}$ cover $\mathscr{Z}_k^d \to \mathscr{W}^{\circ d}_k$. This yields a map $\pi_1(\mathscr{Z}_k^d) \to SO(Q_n^d)$ which is identified with the restriction of $\rho_{n,k}^d$ to the kernel of the Dickson invariant.

In the case k is a field, by abuse of notation, we have a map $\chi_{\mathrm{cyc}} : \pi_1(\mathrm{Spec}\, k) \to (\mathbb{Z}/n\mathbb{Z})^\times$ (induced by the cyclotomic character χ_{cyc} to $\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times$ from Definition 3.12). In the general case where k is just an integral domain, we also obtain a map $\chi_{\mathrm{cyc}} : \pi_1(\mathrm{Spec}\, k) \to (\mathbb{Z}/n\mathbb{Z})^\times$ which can be defined as the unique map making the diagram below commute:

$$\begin{tikzcd}
\pi_1(\mathrm{Frac}(k)) \arrow[rr] \arrow[dr, "\chi_{\mathrm{cyc}}"'] & & \pi_1(\mathrm{Spec}\, k) \arrow[dl, "\chi_{\mathrm{cyc}}"] \\
& (\mathbb{Z}/n\mathbb{Z})^\times &
\end{tikzcd} \tag{3.2}$$

We have a diagram

$$\begin{tikzcd}
\pi_1(\mathscr{X}^d_k) \arrow[rr] \arrow[d] & & SO(Q^d_n) \arrow[dd, "\mathrm{sp}^-_{Q^d_n}"] \\
\pi_1(\mathscr{W}^{\circ d}_k) \arrow[d] & & \\
\pi_1(\operatorname{Spec} k) \arrow[r, "\chi^{d-1}_{\mathrm{cyc}}"] & (\mathbb{Z}/n\mathbb{Z})^\times \arrow[r] & (\mathbb{Z}/n\mathbb{Z})^\times / \left((\mathbb{Z}/n\mathbb{Z})^\times\right)^2 .
\end{tikzcd} \tag{3.3}$$

Lemma 3.24 *The square (3.3) commutes when k is a field of characteristic prime to $2n$.*

Proof Because commutativity of (3.3) is compatible with base change on the integral domain k, it suffices to verify it in the cases that $k = \mathbb{Q}$ and that k is a finite field of characteristic prime to $2n$.

First, we verify the claim when k is a finite field of characteristic prime to $2n$. It suffices to establish the claim for all sufficiently divisible n. Hence, to simplify matters latter, we make the further harmless assumption that $8 \mid n$. Using that $(\mathbb{Z}/n\mathbb{Z})^\times / \left((\mathbb{Z}/n\mathbb{Z})^\times\right)^2$ has even order, it suffices to verify commutativity of (3.3) for all sufficiently large finite fields of characteristic p with $\gcd(p, 2n) = 1$, and odd degree over $\mathbb{F}_p$.

Now, for such sufficiently large finite fields, we only need verify that that for varying $x \in \mathscr{X}(k)$, $\mathrm{sp}^-_{Q^d_n}(\rho^d_{n,k}(\mathrm{Frob}_x))$ is always equal to $\left[q^{d-1}\right]$. By Proposition 3.9, Frobenius elements are equidistributed in a coset of the geometric monodromy group and so it suffices to establish $\mathrm{sp}^-_{Q^d_n}\rho^d_{n,k}(\mathrm{Frob}_x) = \left[q^{d-1}\right]$ for a subset of $x \in \mathscr{W}^{\circ d}_k(k)$ with density in $\mathscr{W}^{\circ d}_k(k)$ tending to 1 as $\#k \to \infty$. Further, we note that the spinor norm is unchanged upon replacing n with n^j for any $j \geq 1$. Note that here we are using the assumption $8 \mid n$, as, for example, $\mathrm{sp}^-_{Q^d_2}$ maps to the trivial group while $\mathrm{sp}^-_{Q^d_4}$ maps to a nontrivial group. By replacing n with a sufficiently large power we can ensure that the density of $g \in \operatorname{im} \rho^d_{n,k}$ with a 0-dimensional 1 eigenspace is arbitrarily close to 1 by Proposition 3.22. Recall that, by the Lang-Weil estimates, if X is a scheme over $\operatorname{Spec} \mathbb{Z}$ with geometrically irreducible fibers and $U \subset X$ a fiberwise dense open subscheme $\lim_{\#k \to \infty} \frac{\#U(k)}{\#X(k)} = 1$. Since $\mathscr{W}^{\boxslash d}_{\operatorname{Spec} \mathbb{Z}[1/2]} \subset \mathscr{W}^{\circ d}_{\operatorname{Spec} \mathbb{Z}[1/2]}$ is a fiberwise dense open subscheme by [28, Lemma 3.14], we find that $\mathscr{W}^{\boxslash d}_k(k)$ has density 1 in $\mathscr{W}^{\circ d}_k(k)$ as $\#k \to \infty$, and so it suffices to verify the above when $x \in \mathscr{W}^{\boxslash d}_k(k)$. Hence, we want to verify commutativity of (3.3) for all $x \in \mathscr{W}^{\boxslash d}_k(k)$ with a 0-dimensional 1 eigenspace, which is the content of Proposition 3.17(2).

So, to finish the proof, it only remains to deal with the case $k = \mathbb{Q}$. Since (3.3) is in fact defined over the integral domain $k = \mathbb{Z}[1/2]$, and is compatible with base change along $\operatorname{Spec} \mathbb{Q} \to \operatorname{Spec} \mathbb{Z}[1/2n]$, it suffices to verify commutativity when

$k = \operatorname{Spec}\mathbb{Z}[1/2n]$. Via the bijection between maps $\pi_1(\mathscr{X}^d_{\mathbb{Z}[1/2n]}) \to G$ and G-covers of $\mathscr{X}^d_{\mathbb{Z}[1/2n]}$, call X and Y the two induced $(\mathbb{Z}/n\mathbb{Z})^\times / \left((\mathbb{Z}/n\mathbb{Z})^\times\right)^2$-covers of $\mathscr{X}^d_{\mathbb{Z}[1/2n]}$ obtained by traversing the diagram (3.3) in the two different paths. We wish to show X and Y are isomorphic. We obtain a $(\mathbb{Z}/n\mathbb{Z})^\times / \left((\mathbb{Z}/n\mathbb{Z})^\times\right)^2$-cover $T \to \mathscr{X}^d_{\mathbb{Z}[1/2n]}$ induced by the "difference" of X and Y; that is, if X and Y correspond to maps $f, g : \pi_1(\mathscr{X}^d_{\mathbb{Z}[1/2n]}) \to (\mathbb{Z}/n\mathbb{Z})^\times / \left((\mathbb{Z}/n\mathbb{Z})^\times\right)^2$ then T corresponds to the homomorphism $t(\alpha) = f(\alpha)g(\alpha^{-1})$. To conclude the proof, it suffices to show T is trivial.

We first verify $T \times_{\operatorname{Spec}\mathbb{Z}[1/2n]} \operatorname{Spec}\mathbb{Q} \to \mathscr{X}^d_{\mathbb{Q}}$ is the pullback of a cover $S \to \operatorname{Spec}\mathbb{Q}$ along the structure map $\mathscr{X}^d_{\mathbb{Q}} \to \operatorname{Spec}\mathbb{Q}$. By the established case of finite fields and compatibility with base change, we know T becomes trivial after base change of $T \to \mathscr{X}^d_{\mathbb{Z}[1/2n]} \to \operatorname{Spec}\mathbb{Z}[1/2n]$ along any closed point $\operatorname{Spec}\mathbb{F}_p \to \operatorname{Spec}\mathbb{Z}[1/2n]$. We now apply [16, Proposition 9.7.8], which states that the number of geometric components of a morphism is constant on some open set, to the map $T \to \operatorname{Spec}\mathbb{Z}[1/2n]$. It follows that the cover $T \to \mathscr{X}^d_{\mathbb{Z}[1/2n]}$ is trivial when restricted to $\operatorname{Spec}\overline{\mathbb{Q}} \to \operatorname{Spec}\mathbb{Z}[1/2n]$. This implies that the composite morphism $\pi_1(\mathscr{X}^d_{\overline{\mathbb{Q}}}) \to \pi_1(\mathscr{X}^d_{\mathbb{Q}}) \to (\mathbb{Z}/n\mathbb{Z})^\times / \left((\mathbb{Z}/n\mathbb{Z})^\times\right)^2$ is trivial. From the exact sequence [17, Exposé IX, Théorème 6.1]

$$0 \longrightarrow \pi_1(\mathscr{X}^d_{\overline{\mathbb{Q}}}) \longrightarrow \pi_1(\mathscr{X}^d_{\mathbb{Q}}) \longrightarrow \pi_1(\operatorname{Spec}\mathbb{Q}) \longrightarrow 0 \tag{3.4}$$

we obtain that the cover $T \times_{\operatorname{Spec}\mathbb{Z}[1/2n]} \operatorname{Spec}\mathbb{Q} \to \mathscr{X}^d_{\mathbb{Q}}$ is the pullback of a cover $S \to \operatorname{Spec}\mathbb{Q}$ along the structure map $\mathscr{X}^d_{\mathbb{Z}} \to \operatorname{Spec}\mathbb{Q}$.

To conclude, we wish to show S is a trivial cover of $\operatorname{Spec}\mathbb{Q}$. By Chebotarev density, it suffices to show that the normalization of $\operatorname{Spec}\mathbb{Z}$ in S is the trivial cover over a density 1 subset of primes. Since S pulls back to $T \times_{\operatorname{Spec}\mathbb{Z}[1/2n]} \operatorname{Spec}\mathbb{Q}$ along the map $\mathscr{X}^d_{\mathbb{Z}[1/2n]} \to \operatorname{Spec}\mathbb{Q}$, it suffices to show that $T \to \mathscr{X}^d_{\mathbb{Z}[1/2n]}$ is the trivial cover over a density 1 subset of primes. Indeed, this triviality holds by the previously established commutativity of (3.3) when $\operatorname{char}(k)$ is positive. □

Recall in Definition 3.23, we defined $\mathscr{X}^d_k$ as the double cover of $\mathscr{W}^{\circ d}_k$ corresponding to the kernel of the Dickson invariant. That is, $\pi_1(\mathscr{X}^d_k) = \ker(\mathrm{D}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}) : \pi_1(\mathscr{W}^{\circ d}_k) \to \mathbb{Z}/2\mathbb{Z}$.

Lemma 3.25 *For a field k of characteristic $p \neq 2$ (allowing $p = 0$) and any height $d \geq 2$, the image of the spinor norm map restricted to* $\ker(D_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}})$

$$sp^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}} \circ \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}|_{\ker(D_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}})} : \pi_1(\mathscr{X}^d_k) \to \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times / \left(\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times\right)^2$$

is identified with the image of the composition

$$\operatorname{Gal}(\overline{k}/k) \xrightarrow{\chi^{d-1}_{\text{cyc}}} \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times \to \left(\widehat{\mathbb{Z}}^{(p)}\right)^\times / \left(\left(\widehat{\mathbb{Z}}^{(p)}\right)^\times\right)^2. \tag{3.5}$$

Remark 3.26 In the case k is algebraically closed or d is odd, Lemma 3.25 says the image of the spinor norm map $\mathrm{sp}^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}} \circ \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}$, when restricted to the kernel of the Dickson invariant, is trivial.

Proof It suffices to establish the claim for all finite n, with no prime factor of n equal to p, in place of $\widehat{\mathbb{Z}}^{(p)}$. The result then follows from Lemma 3.24. □

3.10 Proving Theorem 3.14

Combining the results of the preceding subsections, we are ready to complete our monodromy computation.

Proof of Theorem 3.14 First, by Lemma 3.16, we find $\Omega(Q^d_{\widehat{\mathbb{Z}}^{(p)}}) \subset \operatorname{im} \rho^d_{\widehat{\mathbb{Z}}^{(p)},\overline{k}}$. As

$$\Omega(Q^d_{\widehat{\mathbb{Z}}^{(p)}}) = \ker\left(O\left(Q^d_{\widehat{\mathbb{Z}}^{(p)}}\right) \xrightarrow{(\mathrm{D}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}, \mathrm{sp}^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}})} \left(\prod_{\substack{\text{primes } \ell, \\ \ell \neq p}} \mathbb{Z}/2\mathbb{Z} \right) \times \left(\widehat{\mathbb{Z}}^\times/(\widehat{\mathbb{Z}}^\times)^2\right) \right),$$

determining $\operatorname{im} \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}$ is equivalent to determining the image of $(\mathrm{D}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}, \mathrm{sp}^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}) \circ \operatorname{im} \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}$.

First, because $r_n(O^*_-(Q^d_{\mathbb{Z}})) \subset \rho^d_{n,\overline{k}}$ for every $n \geq 1$ and prime to p, by [28, Theorem 4.4], $\rho^d_{n,\overline{k}}$ does contain elements with trivial spinor norm and nontrivial Dickson invariant. Therefore, since we know the image of the Dickson invariant map is $\Delta_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ by Lemma 3.19, it follows that $\operatorname{im} \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}$ contains $\ker \mathrm{sp}^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}} \cap (\mathrm{D}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}})^{-1}(\Delta_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}))$.

Therefore, the image of the joint map $(\mathrm{D}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}, \mathrm{sp}^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}) \circ \operatorname{im} \rho^d_{\widehat{\mathbb{Z}}^{(p)},k}$ is generated by $\Delta_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{id}$ together with the image of the spinor norm when restricted to the kernel of the Dickson invariant. The latter image is given in the theorem statement by Lemma 3.25. Therefore, the joint map $(\mathrm{D}_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}}, \mathrm{sp}^-_{Q^d_{\widehat{\mathbb{Z}}^{(p)}}})$ has image as claimed in the statement of Theorem 3.14. □

4 The distribution of Sel_ℓ

In this section we will prove the key results towards showing that the BKLPR heuristic agrees with the geometric distribution of Sel_ℓ, for prime ℓ. The psychology of the problem is as follows: one would like to "understand" the distributions by computing numerical invariants such as moments, but the distributions in question are not determined by their moments, since these moments grow too quickly. However, both distributions are the limit as a certain "height" parameter tends to infinity, and at finite height they are distributions on finite sets, hence obviously determined by their moments. We can then verify that the two limiting distributions agree by showing that the "finite height" distributions are very close, which we can then do by computing enough moments.

The key point that makes this computation feasible is that *the moments stabilize very quickly as the height grows*. It was already observed in [28, Theorem 1.2] that the *first* moment (i.e., average) size of Sel_ℓ for height d elliptic curves (in the large q limit) is already equal to its limiting value as soon as the height d is at least 2. In this section we go much further, computing the first $6d-2$ moments for the large q limit of families of elliptic curves with height d (in the large q limit), and showing that they are all already equal to their limiting values. Even computing one fewer moment would be insufficient for our purposes, and it seems that computing one more moment in closed form would be quite difficult, as the next moment is *not* equal to its limiting value!

We caution, however, that the distribution at finite height depends quite delicately on the monodromy group; for example, the large q limit does not literally exist because of small fluctuations among the monodromy groups, but the difference between its $\liminf_{q\to\infty}$ and $\limsup_{q\to\infty}$ will tend to 0 as the height tends to infinity.

We now give an outline of the contents of this section. In Sect. 4.1, we introduce the random kernel model, which is our model for Selmer groups that directly connects to points of the Selmer space. This model will be defined in terms of kernels of random elements of subgroups of an orthogonal group, and so in Sect. 4.2 we compute the probability distributions of the dimensions of these kernels. In Sect. 4.3.5 we show how to determine compute the moments of the above mentioned random kernels, and then how to determine their distribution in terms of these moments, which is used in Sect. 4.4 to bound the total variation distance between the random kernel model and the BKLPR model. We emphasize that these results a priori concern the random kernel model rather than Sel_n, but later in Sect. 6 it will be spelled out how to relate the two.

4.1 The random kernel model

We introduce another probabilistic model which is closely related to the distribution of Selmer elements. We will continue to use the notation introduced earlier, especially from Sect. 3.2.1.

Definition 4.1 (Random 1-eigenspace for an element of H) Let n and d be positive integers. Let $H \subset O(Q_n^d)$ be a subset, where $O(Q_n^d)$ is the orthogonal group for the quadratic form of Definition 3.1. We define $\mathrm{RSel}^H_{V_n^d}$ to be the random variable $\ker(g - \mathrm{id})$, valued in isomorphism classes of $\mathbb{Z}/n\mathbb{Z}$-modules, for g drawn uniformly at random from H.

In this section, we will primarily be concerned with the case of Definition 4.1 where $n = \ell$ is prime, but in Sect. 5, we will crucially use the case that $n = \ell^e$ is a prime power. Now we will define the precise random variable that we end up relating to the distribution of ranks and Selmer groups of elliptic curves for our universal family.

Definition 4.2 (Random kernel model) For $n \in \mathbb{Z}_{\geq 1}$, $d \in \mathbb{Z}_{\geq 2}$ and k a finite field of cardinality q with $\gcd(q, 2n) = 1$, let $[q] \in (\mathbb{Z}/n\mathbb{Z})^\times / \left((\mathbb{Z}/n\mathbb{Z})^\times\right)^2$ denote the class of q. Define

$$H^d_{n,k} := \left(\mathrm{D}_{Q^d_n}\right)^{-1}\left(\Delta_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})\right) \cap \left(\mathrm{sp}^-_{Q^d_n}\right)^{-1}([q^{d-1}]) \subset O\left(Q^d_n\right).$$

Define $\mathrm{RSel}^d_{n,k}$ as the distribution on Ab_n given by

$$\mathrm{Prob}(\mathrm{RSel}^d_{n,k} = G) := \frac{\#\{g \in H^d_{n,k} : \ker(g - \mathrm{id}) \simeq G\}}{\# H^d_{n,k}}.$$

Define $(\mathrm{Rrk}, \mathrm{RSel}_n)^d_k$ as the distribution on $\mathbb{Z}_{\geq 0} \times \mathrm{Ab}_n$ given by

$$\mathrm{Prob}((\mathrm{Rrk}, \mathrm{RSel}_n)^d_k = (r, G)) := \begin{cases} \frac{\#\{g \in SO(Q^d_n) \cap H^d_{n,k} : \ker(g-\mathrm{id}) \simeq G\}}{\# H^d_{n,k}} & \text{if } r = 0, \\ \frac{\#\{g \in \left(O(Q^d_n) - SO(Q^d_n)\right) \cap H^d_{n,k} : \ker(g-\mathrm{id}) \simeq G\}}{\# H^d_{n,k}} & \text{if } r = 1, \\ 0 & \text{if } r \geq 2. \end{cases}$$

Theorem 3.14, adapted to the case of finite fields, gives:

Corollary 4.3 *For q ranging over all prime powers with $\gcd(q, 2n) = 1$ and $d \geq 2$ an integer, the distribution of* $\mathrm{im}\, \rho^d_{n,\mathbb{Z}[1/2n]}(\mathrm{Frob}_x)$ *ranging over $x \in \underline{\mathscr{W}}^{\circ d}_{\mathbb{Z}[1/2]}(\mathbb{F}_q)$, up to an error of $O_{n,d}(q^{-1/2})$, agrees with the distribution $RSel^d_{n,\mathbb{F}_q}$.*

Proof First, by Corollary 3.11 to determine the distribution of Frobenius elements, it makes no difference whether we work with $\underline{\mathscr{W}}^{\circ d}_{\mathbb{Z}[1/2]}$ or $\mathscr{W}^{\circ d}_{\mathbb{Z}[1/2]}$, so we choose to work with the latter. Observe that the monodromy agrees with the geometric monodromy (i.e., $\mathrm{im}\, \rho^d_{n,\mathbb{F}_q} = \mathrm{im}\, \rho^d_{n,\overline{\mathbb{F}}_q}$) when q is a square or d is odd or $n \leq 2$, and has index 2 in the geometric monodromy when q is a square and d is even and $n > 2$ by Theorem 3.14. Therefore, in the former case, it is equidistributed in the monodromy group, which is $H^d_{n,k}$ in this case, up to an error of $O_{n,d}(q^{-1/2})$ by Proposition 3.9. On the other hand, when q is not a square and d is even and $n > 2$, γ_q as in Definition 3.8 is nontrivial since the geometric monodromy is not equal to the monodromy. Hence, by Proposition 3.9, Frob_x is equidistributed in the nontrivial coset of $\rho^d_{n,\mathbb{F}_q} \subset \rho^d_{n,\overline{\mathbb{F}}_q}$, which is precisely $\mathrm{im}\, \rho^d_{n,\mathbb{F}_q} - \mathrm{im}\, \rho^d_{n,\overline{\mathbb{F}}_q} = H^d_{n,k}$.

The statement regarding the concrete characterization of the Dickson invariant and spinor norm is merely a restatement of Theorem 3.14. □

In Sect. 6, we will use the results from Sects. 2.2 and 3.4 to relate the random kernel model to the distribution of Selmer groups. For the rest of this section, we focus on analyzing the random kernel model.

4.2 Distribution of random 1-eigenspaces

We now focus on the case where $n = \ell$ is prime.

4.2.1 Some notation

We will use Theorem 4.9 in conjunction with Lemma 4.5 to deduce the probability generating function for $\ker(g - \mathrm{id})$ for g drawn uniformly at random from a coset of $\Omega(Q_\ell^d) \subset O(Q_\ell^d)$. Now we will take $H \subset O(Q_\ell^d)$ to be a coset of $\Omega(Q_\ell^d)$ in $O(Q_\ell^d)$.

- Note that when $\ell = 2$, the spinor norm is trivial on $O(Q_2^d)$ and hence $\Omega(Q_2^d) = SO(Q_2^d)$ and there are two possibilities for the coset H, determined by the Dickson invariant.
- When ℓ is odd, there are four cosets of $\Omega(Q_\ell^d)$ given by the pair $(\mathrm{sp}^-_{Q_\ell^d}, \mathrm{D}_{Q_\ell^d})$. We label these cosets as in the following table.

$\mathrm{sp}^-_{Q_\ell^d}$ / $\mathrm{D}_{Q_\ell^d}$	trivial	non-trivial
trivial	Ω	A
non-trivial	B	C

For Z a random variable valued in isomorphism classes of finite-dimensional $\mathbb{F}_\ell$-vector spaces, define the *probability generating function* of Z to be the polynomial in t given by

$$G_Z(t) := \mathbb{E}(t^{\dim Z}) = \sum_{i \in \mathbb{N}} \mathrm{Prob}(\dim Z = i) t^i.$$

For a polynomial $f(t) = \sum_{i \in \mathbb{N}} a_i t^i$, introduce the notation $[f(t)]_r := a_r$ to denote the coefficient of t^r in $f(t)$.

4.2.2 The probability generating functions

We will now work towards the proof of:

Theorem 4.4 *Let $\ell > 2$ be an odd prime and $d \geq 1$ a positive integer. Then we have $G_{RSel^B_{V_\ell^d}} = G_{RSel^C_{V_\ell^d}}$ and*

$$G_{RSel^\Omega_{V_\ell^d}} = G_{RSel^A_{V_\ell^d}} + \frac{1}{\#\Omega(Q_\ell^d)} \prod_{i=0}^{6d-3} \left(t^2 - \ell^{2i}\right).$$

4.2.3 Some lemmas

We begin with some preliminary results. For (V, Q) a quadratic space and $k \in \mathbb{Z}_{\geq 0}$, we will abbreviate

$$V^k := \underbrace{V \times V \times \cdots \times V}_{s \text{ times}}$$

and consider the diagonal action of $O(Q)$ on V^k. This induces a diagonal action of the subgroup $\Omega(Q) \subset O(Q)$ on V^k.

Lemma 4.5 *Let $m \in \mathbb{Z}_{\geq 0}$ and let (V, Q) be a nondegenerate quadratic space over a finite field L with $\dim_L V = r$. If $r \geq 2m + 2$, then the orbits of $O(Q)$ and $\Omega(Q)$ on V^m coincide. Hence, the orbits of $O(Q)$ on V^m agree with the orbits of any subgroup $H \supset \Omega(Q)$ on V^m.*

Proof It suffices to show that $\Omega(Q)$ acts transitively on any orbit of $O(Q)$. Fix an arbitrary tuple of vectors $(v_1, \dots, v_m) \in V^m$. Let $W := \operatorname{Span}(v_1, \dots, v_m)$. We claim that if $\dim_L V \geq 2m + 2$, for every $a \in L$, there is some $w \in W^{\perp}$ with $Q(w) = a$.

Assuming this claim, let us show that the orbits of $O(Q)$ and $\Omega(Q)$ coincide. First, we tackle the case $\operatorname{char}(L) \neq 2$. In this case, it suffices to show that for each $(\alpha, \beta) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, there is some $h \in O(Q)$ fixing $(v_1, \dots, v_m)$ with $\operatorname{sp}^-_Q(h) = \alpha$ and $\det(h) = \beta$. To see such an h exists, let w be an element in $W^{\perp}$ with $-Q(w)$ a square in L, and let w' be an element with $-Q(w')$ a non-square in L. Then the four elements id, $r_w, r_{w'}, r_w \circ r_{w'} \in O(Q)$ attain all four possible values of $(\operatorname{sp}^-_Q, \det)$ and fix $(v_1, \dots, v_m)$. This implies that $\Omega(Q)$ acts transitively on the $O(Q)$-orbit of $(v_1, \dots, v_m)$.

The case $\operatorname{char}(L) = 2$ is similar, but easier. To show $\Omega(Q)$ has the same orbits as $O(Q)$, it suffices to exhibit an element of nontrivial Dickson invariant fixing $(v_1, \dots, v_m)$. Indeed, for any $v \in W^{\perp}$, r_v is such an element.

We now conclude the proof by verifying the claim. If (V, Q) is any nondegenerate quadratic space of dimension at least 2 over a finite field L, then for every $a \in L$ there is some $v \in V$ with $Q(v) = a$. Recall that the *rank* of a quadratic space (V, Q) is defined to be $\operatorname{rk}(V, Q) := \dim V - \dim \operatorname{rad}(V, Q)$, where $\operatorname{rad}(V, Q)$ the *radical* of (V, Q), i.e., the set of $x \in V$ with $B_Q(x, y) = 0$ for all $y \in V$. Therefore, it suffices to show that $\operatorname{rk}(Q|_{W^\perp}, W^{\perp}) \geq 2$. Note that $\operatorname{rad}(Q|_{W^\perp}, W^{\perp}) = W \cap W^{\perp}$. Hence

$$\operatorname{rk}(Q|_{W^\perp}, W^{\perp}) = \dim W^{\perp} - \dim(W \cap W^{\perp}). \tag{4.1}$$

Since $\dim V \geq 2 \dim W + 2$, we have $\dim W^{\perp} - \dim(W \cap W^{\perp}) \geq \dim W^{\perp} - \dim W \geq 2$. □

It will also be useful later to have a result on the case when $\dim V = 2m$.

Lemma 4.6 *Let (V, Q) be a nondegenerate quadratic space over a finite field L with $\dim_L V = r$. If $r = 2m$ is even, then the orbits of $O(Q)$ and $\mathrm{SO}(Q)$ on V^m agree except on m-tuples $(v_1, \dots, v_m) \in V^m$ that span a maximal isotropic subspace of V.*

Proof It suffices to exhibit an element of $O(Q) - \mathrm{SO}(Q)$ that stabilizes $(v_1, \dots, v_m)$. Let $W := \operatorname{Span}(v_1, \dots, v_m)$ as in the proof of Lemma 4.5. If we can find $w \in W^{\perp}$ such that $Q(w) \neq 0$, then r_w does the job.

To see that such w exists, it suffices to show that $\operatorname{rk}(Q|_{W^\perp}, W^{\perp}) > 0$. But by (4.1), this holds as long as W is not maximal isotropic. □

Lemma 4.7 *For ℓ a prime and $d \geq 1$, any coset $H \subset O(Q_\ell^d)$ of $\Omega(Q_\ell^d)$, we have*

$$G_{RSel^H_{V_\ell^d}}(\ell^i) = G_{RSel^\Omega_{V_\ell^d}}(\ell^i) \quad \textit{for } i = 0, 1, \ldots, 6d-3.$$

Proof For $g \in G$, let $V^{g=1}$ denote the 1-eigenspace of g acting on V. Let $G' \subset G$ be a subgroup. By definition, we have

$$G_{\mathrm{RSel}^{G'}_{V_\ell^d}}(t) = \frac{1}{\#G'} \sum_{g \in G'} t^{\dim \ker(g - \mathrm{id})}$$

so that

$$G_{\mathrm{RSel}^{G'}_{V_\ell^d}}(\ell^i) = \frac{1}{\#G'} \sum_{g \in G'} (\#V^{g=1})^i. \tag{4.2}$$

Note that $(V^{g=1})^i = (V^i)^{g=1}$ where $g \in G$ acts diagonally on V^i, so that $(\#V^{g=1})^i = \#(V^i)^{g=1}$. Putting this into (4.2) gives

$$G_{\mathrm{RSel}^{G'}_{V_\ell^d}}(\ell^i) = \frac{1}{\#G'} \sum_{g \in G'} (\#V^i)^{g=1}. \tag{4.3}$$

By Burnside's Lemma, we have

$$\sum_{g \in G'} \#(V^i)^{g=1} = \#\{\text{orbits of} G' \text{ on} V^i\}. \tag{4.4}$$

By Lemma 4.5, the right hand side of (4.4) has the same value when we take G' to be any of $\Omega(Q_\ell^d)$, $\ker(\mathrm{sp}^-_{Q_\ell^d})$, $\ker(\mathrm{D}_{Q_\ell^d})$, and $O(Q_\ell^d)$ for $i \leq 6d-3$. Hence we have

$$\begin{aligned} G_{\mathrm{RSel}^\Omega_{V_\ell^d}}(\ell^i) &= G_{\mathrm{RSel}_{V_\ell^d}^{\mathrm{O}^*_-(V_\ell^d)}}(\ell^i) \\ &= G_{\mathrm{RSel}_{V_\ell^d}^{\mathrm{SO}(V_\ell^d)}}(\ell^i) = G_{\mathrm{RSel}_{V_\ell^d}^{\mathrm{O}(V_\ell^d)}}(\ell^i), \quad i = 1, \ldots, 6d-3. \end{aligned}$$

We then obtain the result by noting that any coset can be expressed in terms of differences of the above subgroups. For example, we can obtain the result for $H = B$ by writing

$$G_{\mathrm{RSel}_{V_\ell^d}^{\mathrm{SO}(V_\ell^d)}}(\ell^i) = \frac{1}{2} G_{\mathrm{RSel}^\Omega_{V_\ell^d}}(\ell^i) + \frac{1}{2} G_{\mathrm{RSel}^B_{V_\ell^d}}(\ell^i).$$

□

Proof of Theorem 4.4 Recall that the Dickson invariant of any element $g \in O(Q_n^d)$ agrees with the dimension of its 1-eigenspace $\mod 2$. Indeed, in general, the Dickson invariant of g agrees with $\dim \operatorname{im}(1-g)$, by [39, p. 160], where the notation $[V, f]$ is used for $\operatorname{im}(1-f)$. Since $\dim V_n^d$ is even, it follows that $\dim \ker(1-g) \equiv \dim \operatorname{im}(1-g) \mod 2$.

Because of this, only *odd* powers of t can appear in $G_{\mathrm{RSel}^B_{V^d_\ell}}(t)$ and $G_{\mathrm{RSel}^C_{V^d_\ell}}(t)$. Furthermore, they have degree at most $12d-5$ since $\dim V = 12d-4$. By Lemma 4.7, these functions agree at the $6d-2$ points $1, \ell, \ldots, \ell^{6d-3}$. Since they are both odd functions, they must agree as well at $0, -1, -\ell, \ldots, -\ell^{6d-3}$. But two polynomials of degree at most $12d-5$ agreeing at $12d-3$ points must be the same.

Similarly, $G_{\mathrm{RSel}^\Omega_{V^d_\ell}}(t)$ and $G_{\mathrm{RSel}^A_{V^d_\ell}}$ are *even* polynomials of degree at most $12d-4$, and they agree at the $12d-4$ points $\pm 1, \pm\ell, \ldots, \pm\ell^{6d-3}$. The difference $G_{\mathrm{RSel}^\Omega_{V^d_\ell}}(t) - G_{\mathrm{RSel}^A_{V^d_\ell}}(t)$ must therefore be proportional to $\prod_{i=1}^{6d-3}(t^2-\ell^{2i})$. To find the constant of proportionality, note that the coefficient of t^{12d-4} in $G_{\mathrm{RSel}^H_{V^d_\ell}}(t)$ is the probability that $g \in H$ fixes all of V, i.e. is the identity. This happens with probability $\frac{1}{\#\Omega(Q_\ell^d)}$ for $H = \Omega(Q_\ell^d)$, and probability 0 for any other coset. This completes the proof. □

4.2.4 Formulas for the generating functions

Let $O(12d-4, \mathbb{F}_\ell)$ denote the orthogonal group associated to the standard quadratic form $\sum_{i=1}^{6d-2} x_{2i-1}x_{2i}$ on a $12d-4$ dimensional vector space over $\mathbb{F}_\ell$.

Lemma 4.8 *The group $O(12d-4, \mathbb{F}_\ell)$ is isomorphic to $O(Q_\ell^d)$.*

Proof We begin by showing the quadratic form Q_n^d has discriminant 1 over $\mathbb{Z}/n\mathbb{Z}$. Indeed, it is the reduction $\mod n$ of a quadratic form $Q_{\mathbb{Z}}^d$ over $\mathbb{Z}$ which has discriminant 1 over $\mathbb{Z}$ by [28, Theorem 4.4 and Remark 4.5]. Indeed, [28, Remark 4.5] explains that $Q_{\mathbb{Z}}^d = U^{\oplus(2d-2)} \bigoplus (-E_8)^{\oplus d}$, where U denotes the hyperbolic plane and $-E_8$ denotes the quadratic form associated to the E_8 lattice with negative its usual pairing. Since U has discriminant -1 while $-E_8$ has discriminant 1, the discriminant of $Q_{\mathbb{Z}}^d$ is $(-1)^{2d-2} \cdot 1^d = 1$. We deduce that, $O(Q_\ell^d) = O(12d-4, \mathbb{F}_\ell)$ has rank $12d-4$ and discriminant 1. When $\ell > 2$, there is a unique orthogonal group over $\mathbb{F}_\ell$ of discriminant 1 [43, 3.4.6], and so $O(Q_\ell^d) \simeq O(12d-4, \mathbb{F}_\ell)$ in this case. When $\ell = 2$, there are two nonisomorphic quadratic forms of discriminant 1 and rank $12d-4$, but $O(12d-4, \mathbb{F}_\ell)$ is the unique hyperbolic such quadratic form, so we only need check $O(Q_\ell^d)$ is hyperbolic. To this end, it suffices to check the quadratic form associated to E_8 is hyperbolic when reduced modulo 2. A nondegenerate even dimensional quadratic form over a field is hyperbolic if and only if it contains an isotropic subspace of half the dimension of the quadratic space [31, III, Lemma 1.2]. For the E_8 lattice, one can explicitly construct such a subspace, such as the space spanned by the first, third, sixth and eighth basis vectors, when the E_8 lattice is written as in [20, Chapter 14, 0.3(iii)]. □

By Lemma 4.8, the generating function $\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}$ agrees with the generating function $\mathrm{RSel}_{V_\ell^d}^{H}$ from Definition 4.1 with $H = O(12d-4, \mathbb{F}_\ell)$ the full orthogonal group, so we may use these notations interchangeably. The following theorem, which completely characterizes $\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}$, is proved in an unpublished manuscript of Rudvalis–Shinoda, cf. [15]. We will give an independent proof of this theorem in Sect. 4.3.1.

For Z a random variable we let $\mathbb{E}(Z^m)$ denote the m**th moment** of Z, which is the expected value of the random variable Z^m.

Theorem 4.9 *(Rudvalis-Shinoda, [15, Theorem 2.5 and 4.7]) We have*

$$\mathrm{Prob}(\dim RSel_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)} = v)$$
$$= \begin{cases} \frac{\ell^z}{2|\mathrm{GL}_z(\mathbb{F}_{\ell^2})|} \sum_{i=0}^{6d-2-z} \frac{(-1)^i}{\ell^{(2z-1)i}(\ell^{2i}-1)\cdots(\ell^4-1)(\ell^2-1)} \\ \quad + \frac{1}{2} \frac{(-1)^{6d-2-z}}{\ell^{2z(6d-2-z)}|\mathrm{GL}_z(\mathbb{F}_{\ell^2})|(\ell^{2(6d-2-z)}-1)\cdots(\ell^4-1)(\ell^2-1)} & \textit{if } v = 2z \\ \frac{1}{2\ell^z|\mathrm{GL}_z(\mathbb{F}_{\ell^2})|} \sum_{i=0}^{6d-2-z} \frac{(-1)^i}{\ell^{i^2+2(z+1)i}(1-q^{-2})(1-q^{-4})\cdots(1-q^{-2i})} & \textit{if } v = 2z+1. \end{cases}$$

Furthermore, we have

$$\lim_{d\to\infty} \left(\mathrm{Prob}(\dim RSel_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)} = v) \right) = \prod_{j\geq 0} \left(1 + \ell^{-j}\right)^{-1}$$
$$\frac{1}{\ell^{(v^2-v)/2}\left(1-\ell^{-1}\right)\left(1-\ell^{-2}\right)\cdots\left(1-\ell^{-v}\right)}. \tag{4.5}$$

Additionally, for $0 \leq m \leq 6d-2$, *the moments of* $\#RSel_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}$ *are computed as*

$$\mathbb{E}(\#RSel_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)})^m = \prod_{i=1}^{m} \left(\ell^i + 1\right).$$

From Theorems 4.9 and 4.4, it is fairly straightforward to deduce explicit formulas for the probability generating functions $G_{\mathrm{RSel}_{V_\ell^d}^{\Omega}}(t)$, $G_{\mathrm{RSel}_{V_\ell^d}^{A}}(t)$, $G_{\mathrm{RSel}_{V_\ell^d}^{B}}(t)$, $G_{\mathrm{RSel}_{V_\ell^d}^{C}}(t)$. However, we omit the answers as we will not need them.

4.3 Direct computation of the moments

In this subsection we give an alternate computation of the moments of $\dim\ker(g-\mathrm{id})$ for $g \in O(Q)$, for Q a quadratic form over $\mathbb{F}_\ell$ of sufficiently large rank without using the unpublished results of Rudvalis and Shinoda. We will explain that this gives an alternate proof of Theorem 4.9. In addition, the analysis here is used later to get better control on the convergence of the random kernel model.

As already mentioned above, [15] computed an explicit formula for the moments of $\dim \ker(g - \mathrm{id})$ for $g \in O(Q)$, using the probability distribution obtained in unpublished work of Rudvalis–Shinoda. The calculation of Rudvalis–Shinoda rests on intricate combinatorial analysis. We learned of this work after we had already found an independent computation of the probability distribution, which we will explain in this subsection. Our logic in this subsection runs in the opposite direction: we directly compute the moments, and deduce the probability distribution from it. (The advantage of this approach is that it also gives the distribution for g drawn from subgroups of $O(Q)$, such as Ω.)

Theorem 4.10 *Fix $m \in \mathbb{Z}_{\geq 0}$, let n be squarefree, and let (V, Q) be a nondegenerate quadratic space over $\mathbb{Z}/n\mathbb{Z}$. For $\mathrm{rk}_{\mathbb{Z}/n\mathbb{Z}} V \geq 2m + 2$, then:*

(1) The number of orbits of $O(Q)$ acting diagonally on V^m is

$$\prod_{\ell \text{ prime } | n} (1+\ell)(1+\ell^2)\cdots(1+\ell^m). \tag{4.6}$$

(2) The orbits of $\Omega(Q)$ acting diagonally on V^m coincide with those of $O(Q)$ acting diagonally on V^m.

For the next part (which is about getting slightly sharper results in the "edge case" $r = 2m$), we let $n = \ell$ be prime and ask that (V, Q) be a split[4] quadratic space of dimension r over $\mathbb{F}_\ell$.

(3) For $r = 2m$, the number of orbits of $O(Q)$ acting diagonally on V^m is also given by (4.6).

(4) For $r = 2m$,

$$\#\{\textit{orbits of } \mathrm{SO}(Q) \textit{ on } V^m\} = \#\{\textit{orbits of } O(Q) \textit{ on } V^m\} + 1.$$

4.3.1 Proof of Theorem 4.9, assuming Theorem 4.10

Let $\widetilde{G}(t)$ be the generating function of the distribution in Theorem 4.9. This is a polynomial of degree $12d - 4$; write

$$\widetilde{G}(t) = \widetilde{G}^{\mathrm{odd}}(t) + \widetilde{G}^{\mathrm{even}}(t)$$

where $\widetilde{G}^{\mathrm{odd}}(t)$ is an odd polynomial and $\widetilde{G}^{\mathrm{even}}(t)$ is an even polynomial. The computation in [15] shows that the moments of the even and odd parts of the distributions coincide, so that

$$\widetilde{G}^{\mathrm{odd}}(\ell^m) = \widetilde{G}^{\mathrm{even}}(\ell^m), \quad 0 \leq m \leq 6d - 3.$$

As explained Lemma 4.7, the orbit counts in Theorem 4.10 are the moments of $\#\mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}$, so Theorem 4.10 shows that the mth moment of $\#\mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}$

[4] For the definition of this, see [31, I, Sect. 6].

is as claimed in Theorem 4.9 for $0 \le m \le 6d - 3$. Writing

$$G_{\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}}(t) = G^{\mathrm{odd}}_{\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}}(t) + G^{\mathrm{even}}_{\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}}(t)$$

for the decomposition into odd and even parts, Lemma 4.7 implies also that

$$G^{\mathrm{odd}}_{\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}}(\ell^m) = G^{\mathrm{even}}_{\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}}(\ell^m), \quad \text{for } 0 \le m \le 6d - 3.$$

Hence $\widetilde{G}^{\mathrm{odd}}(\ell^m) = G^{\mathrm{odd}}_{\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}}(\ell^m)$ for $0 \le m \le 6d - 2$. Since they are both odd polynomials, they also agree at $-\ell^m$ for $0 \le m \le 6d - 3$. But since they both have degree at most $12d - 5$, and they agree at $12d - 4$ points, they must be equal.

Similarly, $\widetilde{G}^{\mathrm{even}}(\ell^m) = G^{\mathrm{even}}_{\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}}(\ell^m)$ for $0 \le m \le 6d - 2$. Since they are both odd polynomials, they also agree at $-\ell^m$ for $0 \le m \le 6d - 2$. Hence there difference is a polynomial of degree at most $12d - 4$ vanishing at the $12d - 4$ points $\pm\ell^m$ for $0 \le m \le 6d - 3$, and must therefore a multiple of $\prod_{m=0}^{6d-2}(t^2 - \ell^{2m})$. But the coefficients of t^{12d-4} in both $\widetilde{G}^{\mathrm{even}}(t)$ and $G^{\mathrm{even}}_{\mathrm{RSel}_{V_\ell^d}^{O(12d-4,\mathbb{F}_\ell)}}(t)$ are both $\frac{2}{\#\mathrm{O}(12d-4,\mathbb{F}_\ell)}$, so the constant of proportionality must be 0. □

The rest of this subsection is devoted towards proving Theorem 4.10.

4.3.2 Counting orbits of independent vectors

Recall that a quadratic space is *hyperbolic* if it has the form $W \oplus W^\vee$ with form $Q(w, \lambda) = \lambda(w)$; over a field, this is equivalent to the condition that it be *metabolic*, i.e., that it is nondegenerate and contains an isotropic subspace of half the dimension [31, III, Lemma 1.2].

Lemma 4.11 *Let (V, Q) be a metabolic quadratic space over a field. Then any (possibly degenerate) quadratic space (W, Q') of dimension $\dim(W) \le \dim(V)/2$ embeds isometrically in V.*

Proof If $\dim(W) < \dim(V)/2$, we can always enlarge W by taking the direct sum with a trivial quadratic space of dimension $\dim(V)/2 - \dim(W)$, so we may as well assume that $\dim(W) = \dim(V)/2$. Let Q'' be the quadratic form on $W \oplus W^*$ given by $Q''(w, \lambda) = Q'(w) + \lambda(w)$. Then (W, Q') embeds isometrically in the metabolic (thus hyperbolic) quadratic space $(W \oplus W^*, Q'')$. Since two hyperbolic quadratic spaces of the same dimension are isomorphic, there is an isometry $(W \oplus W^*, Q'') \cong (V, Q)$, and thus (W, Q') embeds in (V, Q) as required. □

Corollary 4.12 *Let (V, Q) be a nondegenerate quadratic space over a finite field. Then any (possibly degenerate) quadratic space (W, Q') of dimension $\dim(W) \le (\dim(V) - 2)/2$ embeds isometrically in (V, Q).*

Proof Any nondegenerate quadratic space over a finite field is isomorphic to the direct sum of a hyperbolic quadratic space and a nondegenerate quadratic space of dimension at most 2, and Lemma 4.11 shows that (W, Q') embeds in the former. □

The key technical ingredient in the proof of Theorem 4.10 is the following Proposition.

Proposition 4.13 *Fix $m \in \mathbb{Z}_{\geq 0}$ and let (V, Q) be a nondegenerate quadratic space over $\mathbb{F}_\ell$ of dimension $r \geq 2m+2$. Then, the number of orbits of $O(Q)$ in V^m consisting of a tuple of independent vectors $(x_1, \dots, x_m)$ is $\ell^{m(m+1)/2}$. More precisely, the orbits consisting of independent vectors are in bijection with $\mathbb{F}_\ell^{m(m+1)/2}$ via the map sending*

$$(x_1, \dots, x_m) \mapsto (Q(x_1), \dots, Q(x_m), B_Q(x_i, x_j) : 1 \leq i < j \leq m). \tag{4.7}$$

If (V, Q) is metabolic, then the result still holds if $r = 2m$.

Proof of Proposition 4.13 First we argue that (4.7) is injective. If $(x_1, \dots, x_m)$ and $(x'_1, \dots, x'_m)$ have the same image under (4.7), $\mathrm{Span}(x_1, \dots, x_m)$ is isomorphic as a quadratic subspace of (V, Q) to $\mathrm{Span}(x'_1, \dots, x'_m)$ by the map sending $x_i \mapsto x'_i$. Therefore, by Witt's theorem [8, I.4.1, p. 80], there is an element of $O(Q)$ sending $x_i \mapsto x'_i$. Hence, if $(x_1, \dots, x_m)$ and $(x'_1, \dots, x'_m)$ have the same image under (4.7), they lie in the same $O(Q)$ orbit.

It remains to show that (4.7) is surjective. Suppose $(c_1, \dots, c_m, c_{ij} : 1 \leq i < j \leq m) \subset \mathbb{F}_\ell^{m(m+1)/2}$ are arbitrary. Let (W, Q') be the quadratic space on basis vectors $(y_1, \dots, y_m)$ with $Q'(y_i) = c_i$ and $B_{Q'}(y_i, y_j) = c_{ij}$. The surjectivity amounts to showing that we can find an embedding $(W, Q') \to (V, Q)$ which is an isometry onto its image. But this is exactly the content of Corollary 4.12 if $r \geq 2m + 2$, and Lemma 4.11 if $r \geq 2m$ and (V, Q) is metabolic. □

4.3.3 Orbits of dependent vectors

We aim to explain how to determine the orbits of tuples of vectors that are linearly dependent inductively using Proposition 4.13. The following lemma is key to counting these dependent orbits.

Lemma 4.14 *Let (V, Q) be a nondegenerate quadratic space over $\mathbb{F}_\ell$ and let $O(Q)$ act on V^m. Fix $(x_1, \dots, x_{m-1}) \in V^{m-1}$ and let $W := \mathrm{Span}\,(x_1, \dots, x_{m-1})$. The number of orbits of vectors of the form $(x_1, \dots, x_{m-1}, y) \in V^m$ under the action of $O(Q)$ with $y \in \mathrm{Span}(x_1, \dots, x_{m-1})$ is $\ell^{\dim W}$.*

Proof Suppose that $(x_{i_1}, \dots, x_{i_t})$ is a basis for W, so $\dim W = t$. Then for any $g \in O(Q)$, $g \cdot (x_1, \dots, x_{m-1}, y)$ is uniquely determined by $g \cdot (x_{i_1}, \dots, x_{i_t})$.

To count the number of orbits, we can express y uniquely as

$$y = \sum_{j=1}^{t} a_j x_{i_j}.$$

Then the orbit of $(x_1, \ldots, x_{m-1}, y)$ is uniquely determined by the scalars $(a_i \in \mathbb{F}_\ell)_{1 \le i \le t}$, and so there are $\ell^{\dim W}$ such orbits. □

4.3.4 A recursive formula

Definition 4.15 Fix a quadratic space (V, Q) over a finite field k. Let $f(n, i)$ be the number of orbits of V^n under the action of $O(Q)$ such that $\dim_k \operatorname{Span}(x_1, \ldots, x_n) = i$.

We next explain a recursive formula for the $f(n, i)$.

Lemma 4.16 *The functions $f(n, i)$ satisfy the recursion*

$$f(n, i) = f(n-1, i-1)\ell^i + f(n-1, i)\ell^i. \tag{4.8}$$

Proof Fix a tuple $(x_1, \ldots, x_{n-1}) \in V^{n-1}$. We will count the number of orbits of the form $(x_1, \ldots, x_{n-1}, y) \in V^n$, by conditioning on whether or not $y \in \operatorname{Span}(x_1, \ldots, x_{n-1})$.

- If $y \in \operatorname{Span}(x_1, \ldots, x_{n-1})$, each choice of y yields a different orbit and there are ℓ^i possible such orbits by Lemma 4.14.
- If $y \notin \operatorname{Span}(x_1, \ldots, x_{n-1})$, let $\left(x_{s_1}, \ldots, x_{s_{i-1}}\right)$ be a basis for $\operatorname{Span}(x_1, \ldots, x_{n-1})$. Proposition 4.13 shows that there are $\ell^{i(i+1)/2-(i-1)i/2} = \ell^i$ orbits of the form $(x_1, \ldots, x_{n-1}, y)$, parameterized by the possible values of the pairings

$$B_Q(y, x_{s_1}), \ldots, B_Q(y, x_{s_{i-1}}), Q(y, y).$$

Adding these two contributions over varying vectors $(x_1, \ldots, x_{n-1}) \in V^{n-1}$ yields the result. □

Remark 4.17 We have the initial condition $f(0, i) = 1$ for all $i \ge 0$. This together with the recursion of Lemma 4.16 determine the $f(n, i)$ uniquely. We extend $f(n, i)$ by 0 to a function on $\mathbb{Z} \times \mathbb{Z}$.

Definition 4.18 For every $j \in \mathbb{Z}_{\ge 0}$, define

$$\Sigma^{(s)}(m) := \sum_{i \in \mathbb{Z}} f(m, i)\ell^{is}.$$

Remark 4.19 From the definitions, it follows that the total number of orbits of $O(Q)$ on V^m is $\Sigma^{(0)}(m) = \sum_{i \in \mathbb{Z}} f(m, i)$. Also observe that for any j, $\Sigma^{(j)}(0) = 1$ by definition, since $f(0, i) = 0$ unless $i = 0$.

By Remark 4.19, we want to calculate $\Sigma^{(0)}(m)$. The following lemma relates this to $\Sigma^{(m)}(0)$.

Lemma 4.20 *For $m > 0$ and $s \ge 0$, We have*

$$\Sigma^{(s)}(m) = (1 + \ell^{s+1})\Sigma^{(s+1)}(m-1).$$

Proof By Lemma 4.16, we have

$$\begin{aligned}\Sigma^{(s)}(m) &= \sum_{i\in\mathbb{Z}} f(m-1,i-1)\ell^{i+is} + \sum_{i\in\mathbb{Z}} f(m-1,i)\ell^{i+is}\\ &= \ell^{s+1}\sum_{i\in\mathbb{Z}} f(m-1,i-1)\ell^{(i-1)(s+1)} + \sum_{i\in\mathbb{Z}} f(m-1,i)\ell^{i(s+1)}\\ &= \ell^{s+1}\sum_{i\in\mathbb{Z}} f(m-1,i)\ell^{i(s+1)} + \sum_{i\in\mathbb{Z}} f(m-1,i)\ell^{i(s+1)}\\ &= (\ell^{s+1}+1)\Sigma^{(s+1)}(m-1).\end{aligned}$$

□

Using Lemma 4.20, we can compute $\Sigma^{(0)}(m)$, and hence prove Theorem 4.10.

4.3.5 Proof of Theorem 4.10

First we focus on the situation in parts (1) and (2), where $\mathrm{rk}_{\mathbb{Z}/n\mathbb{Z}} V \geq 2m+2$. Since n is squarefree, we may reduce to the case $n = \ell$ is a prime by the Chinese remainder theorem. Once the statement for $O(Q)$ is established, the statement for $\Omega(Q)$ follows from Lemma 4.5. By Remark 4.19, we just need to show that

$$\Sigma^{(0)}(m) = (1+\ell)(1+\ell^2)\cdots(1+\ell^m).$$

Indeed, using Lemma 4.20, we find

$$\begin{aligned}\Sigma^{(0)}(m) &= (1+\ell)\Sigma^{(1)}(m-1)\\ &= (1+\ell)(1+\ell^2)\Sigma^{(2)}(m-2)\\ &\ \ \vdots\\ &= (1+\ell)(1+\ell^2)\cdots(1+\ell^m)\Sigma^{(m)}(0)\\ &= (1+\ell)(1+\ell^2)\cdots(1+\ell^m).\end{aligned}$$

□

This completes the proof of parts (1) and (2). Now we move onto parts (3) and (4). The argument for part (3) is the same as for the proof of Theorem 4.10. For Part (4), we note by Lemma 4.6 that the orbits coincide except on vectors $(x_1,\ldots,x_m) \in V^m$ that span a maximal isotropic subspace of V. In this case there is only one orbit of such vectors under $O(Q)$, but two orbits under $\mathrm{SO}(Q)$ [7, Corollary T.3.4].

4.4 Bounding the TV distance

We use the moment computations in Sect. 4.3 to obtain certain useful expressions for the probability generating functions.

In this section, let (V_r, Q_r) be the *split* orthogonal space over $\mathbb{F}_\ell$ of rank r (hence discriminant 1). We denote $O_r = O(V_r, Q_r)$, $\mathrm{SO}_r = \mathrm{SO}(V_r, Q_r)$, $\Omega_r = \Omega(V_r, Q_r)$, etc.

Let $H_{2r} \subset O_{2r}$ denote the kernel of the Dickson invariant, i.e., $H_{2r} = \mathrm{SO}_{2r}$ when ℓ is odd, and $H_{2r} = \Omega_{2r}$ when ℓ is even. For $j \geq 0$, let M_j be the limit as $r \to \infty$ of the jth moment of $\mathrm{RSel}^{\mathrm{SO}}_{V_r}$, which by Theorem 4.9 is $\prod_{i=1}^{j}(\ell^i + 1)$.

Lemma 4.21 *We have the following values for the moments of* $\#\ker(g-1)$ *for* g *drawn from* H_{2r} *and its complement:*

$$\begin{aligned}
\mathbb{E}_{g\in H_{2r}}(\#\ker(g-1)^j) &= M_j, 0 \leq j < r\\
\mathbb{E}_{g\in H_{2r}}(\#\ker(g-1)^r) &= M_r + 1\\
\mathbb{E}_{g\notin H_{2r}}(\#\ker(g-1)^j) &= M_j, 0 \leq j < r\\
\mathbb{E}_{g\notin H_{2r}}(\#\ker(g-1)^r) &= M_r - 1.
\end{aligned}$$

Proof The claims for $j < r$ follow from Lemma 4.5 plus Theorem 4.10. The claims for $j = r$ follow from Lemma 4.6 plus Theorem 4.10 □

Let $P_r(t)$ be the unique even polynomial of degree $2r$ such that $P_r(\ell^j) = M_j$ for all $0 \leq j \leq r$, and let $P'_r(t)$ be the unique odd polynomial of degree $2r-1$ such that $P'_r(\ell^j) = M_j$ for $0 \leq j < r$ (not to be confused with the derivative of P_r).

Define

$$G_r(t) := \mathbb{E}_{g\in H_{2r}}[t^{\dim\ker(g-1)}]$$

to be the probability generating function for 1-eigenspaces of elements drawn randomly from H_{2r}, and

$$G'_r(t) := \mathbb{E}_{g\in O_{2r}-H_{2r}}[t^{\dim\ker(g-1)}].$$

Lemma 4.22 *We have identities*

$$G_r(t) = P_{r-1}(t) + \frac{1}{\#H_{2r}} \prod_{0\leq j<r}(t^2 - \ell^{2j}), \tag{4.9}$$

$$G_r(t) = P_r(t) + \prod_{0\leq j<r} \frac{t^2 - \ell^{2j}}{\ell^{2r} - \ell^{2j}}, \tag{4.10}$$

$$G'_{r+1}(t) = P'_r(t) + \ell^{-r} t \prod_{0\leq j<r} \frac{t^2 - \ell^{2j}}{\ell^{2r} - \ell^{2j}}, \tag{4.11}$$

$$G'_{r+1}(t) = P'_{r+1}(t). \tag{4.12}$$

Proof First, we check (4.9). By Lemma 4.21, $G_r(t) - P_{r-1}(t)$ vanishes at $t = \pm\ell^j$ for $0 \leq j \leq r-1$, and is of degree $2r$, hence is proportional to $\prod_{0\leq j<r}(t^2 - \ell^{2j})$.

Therefore, we can determine $G_r(t)$ completely by examining the coefficient of t^{2r}, which is $\#H_{2r}^{-1}$ because that is the probability of drawing the identity element.

We next check (4.10) Similarly, $G_r(t) - P_r(t)$ is proportional to $\prod_{0 \leq j < r}(t^2 - \ell^{2j})$, and it can be determined by evaluating at ℓ^r, where the value is 1 by Lemma 4.21.

Next, (4.12) holds because both $G'_{r+1}(t)$ and $P'_{r+1}(t)$ are polynomials of degree $2r + 1$ vanishing at the $2r + 3$ values $0, \pm 1, \pm \ell, \dots, \pm \ell^r$.

Finally, we show (4.11). By (4.12) and Lemma 4.21, we see $P'_r(\ell^r) = M_r - 1$ while $G'_{r+1}(\ell^r) = M_r$. Therefore, $G'_{r+1}(t) - P'_r(t)$ is a degree $2r+1$ polynomial vanishing at the $2r + 1$ values $0, \pm 1, \pm \ell, \dots \pm \ell^r$, and hence is determined up to a constant. We can then determine its constant value by plugging in $t = \ell^r$, using $P'_r(\ell^r) = M_r - 1$ and $G'_{r+1}(\ell^r) = M_r$. □

Recall that the *Total Variation distance* (TV) between two probability distributions P and P' is

$$d_{\mathrm{TV}}(P, P') = \sup_{\text{events } A} |P(A) - P'(A)|.$$

When P and P' are defined on a countable discrete probability space X, as shown in [30, Proposition 4.2] we can write this as

$$d_{\mathrm{TV}}(P, P') := \frac{1}{2} \sum_{x \in X} |P(x) - P'(x)|. \tag{4.13}$$

In other words, conflating P and P' with functions on X, this is (up to the normalization factor $1/2$) the L^1-norm. Clearly, convergence in TV distance implies convergence as distributions (which is pointwise convergence in the case of distributions on a discrete space). We define the TV distance between two random variables to be the TV distance between their induced probability distributions.

Theorem 4.23 *For ℓ a prime, $d \geq 2$, and q ranging over prime powers with $\gcd(q, 2\ell) = 1$ We have*

$$\limsup_{\substack{q \to \infty \\ \gcd(q,2n)=1}} d_{TV}(\dim RSel^d_{\ell,\mathbb{F}_q}, \lim_{d \to \infty} \dim RSel^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}) = O(\ell^{-(6d-2)^2}),$$

where the implicit constants are absolute in both cases.

Proof We write the proof in the case where ℓ is odd; the case where $\ell = 2$ is even easier, as the analysis of the cosets simplifies because there are fewer cosets (cf. the discussion in Sect. 4.2.4).

We first compare the TV distance between $\dim \mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}$ and $\dim \mathrm{RSel}^d_{\ell,\mathbb{F}_q}$. We have

$$G_{\mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}}(t) = \frac{1}{4} G_{\mathrm{RSel}^{\Omega}_{V^d_\ell}}(t) + \frac{1}{4} G_{\mathrm{RSel}^{A}_{V^d_\ell}}(t) + \frac{1}{4} G_{\mathrm{RSel}^{B}_{V^d_\ell}}(t) + \frac{1}{4} G_{\mathrm{RSel}^{C}_{V^d_\ell}}(t)$$

and

$$G_{\mathrm{RSel}^d_{\ell,\mathbb{F}_q}}(t) = \frac{1}{2}G_{\mathrm{RSel}^{\Omega}_{V^d_\ell}}(t) + \frac{1}{2}G_{\mathrm{RSel}^{B}_{V^d_\ell}}(t) \text{ or } \frac{1}{2}G_{\mathrm{RSel}^{A}_{V^d_\ell}}(t) + \frac{1}{2}G_{\mathrm{RSel}^{C}_{V^d_\ell}}(t).$$

Note that the TV distance between random variables Z and Z' has a clean formulation in terms of the probability generating functions $G_Z(t)$ and $G_Z(t')$: it is half the sum of the absolute values of the differences of the coefficients, as follows from (4.13). Using this observation together with Theorem 4.4, we have

$$\begin{aligned} d_{\mathrm{TV}}(\dim \mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}, \dim \mathrm{RSel}^d_{\ell,\mathbb{F}_q}) &\leq \frac{1}{4}d_{\mathrm{TV}}(\dim \mathrm{RSel}^{\Omega}_{V^d_\ell}, \dim \mathrm{RSel}^{A}_{V^d_\ell}) \\ &= \frac{1}{8}\cdot\frac{1}{\#\Omega(Q^d_\ell)}\prod_{i=0}^{6d-3}(1+\ell^{2i}). \end{aligned}$$

By examining the dimension of the orthogonal group, we find

$$\#\Omega(Q^d_\ell) = \frac{1}{4}\#O(Q^d_\ell) \asymp \ell^{(12d-4)(12d-5)/2}.$$

On the other hand, we have

$$\prod_{i=0}^{6d-3}(1+\ell^{2i}) \asymp \ell^{(6d-2)(6d-3)}.$$

Hence[5]

$$d_{\mathrm{TV}}(\dim \mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}, \dim \mathrm{RSel}^d_{\ell,\mathbb{F}_q}) \ll \ell^{-(6d-2)^2}.$$

Next, we estimate $d_{\mathrm{TV}}(\mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}, \lim_{r\to\infty}\mathrm{RSel}^{O(12r-4,\mathbb{F}_\ell)}_{V^r_\ell})$. It suffices to show that

$$d_{\mathrm{TV}}(\dim \mathrm{RSel}^{O_{2r}}_{V^{2r}_\ell}, \dim \mathrm{RSel}^{O_{2r+2}}_{V^{2r+2}_\ell}) \ll \ell^{-r^2}.$$

We compare the even and odd parts of their generating functions, using the computations of the preceding section. For the even part, using Lemma 4.22 gives that the sum of the absolute values of the coefficients of $G_r(t) - G_{r-1}(t)$ is

$$\ll \ell^{-r}\prod_{0\leq j<r}\frac{1+\ell^{2j}}{\ell^{2r}-\ell^{2j}} = \ell^{-r}\ell^{-r^2+r}\prod_{0\leq j<r}\frac{1+\ell^{-2j}}{1-\ell^{2j-2r}} \ll \ell^{-r^2}.$$

[5] The notation $A(d) \ll B(d)$ means $A(d) = O(B(d))$ as $d\to\infty$, where the implicit constant is absolute.

This shows

$$\limsup_{q\to\infty} d_{\mathrm{TV}}(\dim \mathrm{RSel}^d_{\ell,\mathbb{F}_q}, \lim_{d\to\infty} \mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}) = O(\ell^{-(6d-2)^2}).$$

□

Corollary 4.24 *Fix a prime ℓ, an integer $d \geq 2$, and consider a sequence of prime powers $\{q_1, q_2, \ldots\}$ with $\gcd(q_i, 2\ell) = 1$, so that the q_i lie in a fixed residue class mod ℓ if ℓ is odd, and lie in a fixed residue class mod 8 if $\ell = 2$. Then, the TV distance between the BKLPR heuristic and $\lim_{i\to\infty} \dim RSel^d_{\ell,\mathbb{F}_{q_i}}$ is $O(\ell^{-(6d-2)^2})$.*

Proof First, we impose the assumption that the the q_i lie in a fixed residue class mod ℓ if ℓ is odd, and lie in a fixed residue class mod 8 if $\ell = 2$, so that the distribution in Theorem 3.14 is independent of the choice of q_i in this sequence, since im χ^{d-1} is independent of the choice of q_i. Hence, $\lim_{i\to\infty} \dim \mathrm{RSel}^d_{\ell,\mathbb{F}_{q_i}}$ exists.

Note that in the case where ℓ is prime, which we are currently considering, the "BKLPR heuristic" first appeared as the "Poonen-Rains heuristic" [33], whose explicit formula is given by [33, Conjecture 1.1(a)]. By inspection, this agrees with the distribution of $\lim_{d\to\infty} \mathrm{RSel}^{O(12d-4,\mathbb{F}_\ell)}_{V^d_\ell}$ calculated in Theorem 4.9. Hence the result follows from Theorem 4.23. □

5 Markov properties

In this section, we establish Markov properties satisfied by both the random kernel model and the BKLPR model, which will be used to identify their distributions for prime power order Selmer groups. In Sect. 5.1 we state the Markov property satisfied by the random kernel model, which we prove in Sect. 5.2. We then recall the BKLPR model in Sect. 5.3 and demonstrate the Markov property satisfied by the BKLPR model in Sect. 5.4.

5.1 Markov property for random 1-eigenspaces

Let (V, Q) be a nondegenerate quadratic space of rank rm over $\mathbb{Z}/\ell^e\mathbb{Z}$. Recalling from Definition 4.1, that for a subset $H \subset O(V, Q)$ we let RSel^H_V be the random variable $\ker(g - \mathrm{id})$, valued in isomorphism classes of finite abelian ℓ-groups, for g drawn uniformly at random from H.

In this section only, we will use the notation $O(V, Q)$, $\Omega(V, Q)$, and $SO(V, Q)$ for various subgroups of orthogonal groups, because we will consider various coefficient changes and wish to emphasize this in the notation. Noting that H acts on $V[\ell^j]$, we let H_j be the image of H in $O(V[\ell^j], Q|_{V[\ell^j]})$.

Theorem 5.1 *Let (V, Q) be a nondegenerate quadratic space of rank $2m$ over $\mathbb{Z}/\ell^e\mathbb{Z}$. For $j \leq e$, write $d_j(H) := \dim_{\mathbb{F}_\ell}(\ell^{j-1} RSel^{H_j}_{V[\ell^j]})$.*

If H is a non-empty union of cosets of $\Omega(V, Q)$ in $O(V, Q)$, then the sequence of random variables $d_1(H), d_2(H), \ldots, d_e(H)$ is Markov. If ℓ is odd or $d_i \neq 2m$, then *the distribution of $d_{i+1}(H)$ given $d_i(H)$ is the same as the dimension of the kernel of a uniform random alternating form on $\mathbb{F}_\ell^{d_i(H)}$.*

Corollary 5.2 *For n a prime power, $d \geq 2$ and k a finite field, the statement of Theorem 5.1 holds with $H := \operatorname{im} \rho^d_{n,k} \cap \operatorname{mult}^{-1}(\operatorname{mult} \gamma_q)$.*

Proof By definition, $\operatorname{im} \rho^d_{n,k} \cap \operatorname{mult}^{-1}(\operatorname{mult} \gamma_q)$ is a coset of the geometric monodromy group in the monodromy group. By Theorem 3.14, the geometric monodromy group contains $\Omega(V^d_n, Q^d_n)$ and the monodromy group is contained in $O(V^d_n, Q^d_n)$. Hence $(\operatorname{im} \rho^d_{n,k})^{\operatorname{mult} \gamma_q}$ is a union of cosets of $\Omega(V^d_n, Q^d_n)$ in $O(V^d_n, Q^d_n)$, and we can apply Theorem 5.1 to each of the cosets. □

We next reduce Theorem 5.1 to Theorem 5.4 below. For any $1 \leq j \leq e$, consider $\ell^{e-j} V = V[\ell^j]$, which is a nondegenerate quadratic space of rank $2m$ over $\mathbb{Z}/\ell^j\mathbb{Z}$. The action of $g \in O(V, Q)$ on $V[\ell^j]$ factors through the quotient $O(V, Q) \twoheadrightarrow O(V[\ell^j], Q|_{V[\ell^j]})$. Let H be any coset of $\Omega(V, Q)$. If g is drawn uniformly at random in $O(V, Q)$, its image in $O(V[\ell^j], Q|_{V[\ell^j]})$ will also be uniform in a coset of $\Omega(V_{\mathbb{Z}/\ell^j\mathbb{Z}}, Q_{\mathbb{Z}/\ell^j\mathbb{Z}})$. We now naturally generalize Definition 4.1 to the setting of quadratic space over $\mathbb{Z}_\ell$.

Definition 5.3 Let (V, Q) be a quadratic space over $\mathbb{Z}_\ell$, and let $H \subset O(V, Q)$ be a subset which is a union of cosets of $\Omega(V, Q)$ in $O(V, Q)$. Define the random variable $\mathrm{RSel}^H_{V\otimes\mathbb{Q}_\ell/\mathbb{Z}_\ell}$ to be given by $\ker(g - \mathrm{id}\, |_{V\otimes\mathbb{Q}_\ell/\mathbb{Z}_\ell})$ for $g \in H$ drawn from the Haar measure (normalized to be a probability measure) of Lemma 3.20.

By the compatibility with reduction modulo ℓ^j discussed above, Theorem 5.1 then follows from:

Theorem 5.4 *Let (V, Q) be a nondegenerate quadratic space of rank $2m$ over $\mathbb{Z}_\ell$. Let $H \subset O(V, Q)$ be a union of cosets of $\Omega(V, Q)$. Define the random variable*

$$d_j(H) := \dim_{\mathbb{F}_\ell}(\ell^{j-1} RSel^H_{V\otimes\frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}[\ell^j]}).$$

Then the sequence $d_1(H), d_2(H), \dots$ is Markov, and for ℓ odd or $d_i \neq 2m$, the distribution of $d_{i+1}(H)$ given $d_i(H)$ is the same as the dimension of the kernel of a uniform random alternating form on $\mathbb{F}_\ell^{d_i(H)}$.

We prove Theorem 5.4 in Sect. 5.2.

Remark 5.5 Another way to think about the numbers $d_j(H)$ is as follows. Decomposing

$$\mathrm{RSel}^H_V := (\mathbb{Z}/\ell\mathbb{Z})^{r_1(H)} \oplus (\mathbb{Z}/\ell^2\mathbb{Z})^{r_2(H)} \oplus (\mathbb{Z}/\ell^3\mathbb{Z})^{r_3(H)} \oplus \dots$$

where the $r_i(H)$ are random variables, we have

$$d_1(H) = r_1(H) + r_2(H) + r_3(H) + \dots$$

$$\begin{aligned} d_2(H) &= r_2(H) + r_3(H) + \dots \\ d_3(H) &= r_3(H) + \dots \\ &\vdots \end{aligned}$$

5.2 Proving Theorem 5.4

We now embark on the proof of Theorem 5.4. The proof encompasses this entire subsection, and notation is built cumulatively throughout the section.

We begin by giving one more interpretation of the sequences $d_j(H)$. Referring to notation of Theorem 5.4, let V_j^H be the random variable[6], valued in isomorphism classes of $\mathbb{F}_\ell$-vector spaces, given by

$$(\ker(g - \mathrm{id})|_{V/\ell^j V} + \ell V)/\ell V \subset V \otimes \mathbb{F}_\ell,$$

for g drawn from the Haar measure on H. For a fixed $g \in O(V, Q)$ we write

$$V_j^g := \ker((g - \mathrm{id})|_{V/\ell^j V}).$$

Lemma 5.6 *For a fixed $g \in O(V, Q)$, the isomorphism $V \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell \xrightarrow{\sim} V \otimes_{\mathbb{Z}_\ell} \frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}(\ell)$ identifies*

$$V_j^g \xrightarrow{\sim} \ell^{j-1} \ker\left(g - \mathrm{id}\,|_{V \otimes_{\mathbb{Z}_\ell} \frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}[\ell^j]}\right).$$

Hence dim V_j^H *coincides with the random variable $d_j(H)$.*

Proof This is a straightforward verification which follows from commutativity of

$$\begin{tikzcd} (V \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)[\ell^j] \arrow[r, "\times \ell^j", "\sim"'] \arrow[d, "\times \ell^{j-1}"] & V \otimes \mathbb{Z}/\ell^j\mathbb{Z} \arrow[d, "\bmod \ell"] \\ (V \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)[\ell] \arrow[r, "\times \ell", "\sim"'] & V \otimes \mathbb{F}_\ell \end{tikzcd} \tag{5.1}$$

□

We set $V_0^H := V \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell$ by convention. We claim that the sequence $V_1^H, V_2^H, \dots$ of random subspaces is Markov, and more precisely that if ℓ is odd or $V_j^H \neq V_0^H$, then V_{j+1}^H is the kernel of a uniformly distributed alternating form on V_j^H. In view of Lemma 5.6, this will complete the proof of Theorem 5.4.

Lemma 5.7 *The orthogonal complement of $V_j^g \subset V \otimes \mathbb{F}_\ell$ with respect to the quadratic form induced by Q is $(\ell^{1-j}(\mathrm{im}(g - \mathrm{id}) \cap \ell^{j-1} V))/\ell V \subset V \otimes \mathbb{F}_\ell$.*

[6] We apologize for the similarity to the notation V_n^d; at least, the latter notation will not appear in this section.

Proof Inside $V/\ell^j V$, we have $\ker((g-\mathrm{id})|_{V/\ell^j V})^\perp = \mathrm{im}((g-\mathrm{id})|_{V/\ell^j V})$, hence

$$(\mathrm{im}((g-\mathrm{id})|_{V/\ell^j V}) \cap \ell^{j-1}V/\ell^j V)^\perp = \ker((g-\mathrm{id})|_{V/\ell^j V}) + \ell V.$$

This immediately induces the claim about orthogonal complements inside $V \otimes \mathbb{F}_\ell$. □

Given j and g, for $v \in V_j^g$, we use $\widetilde{v}$ to denote any choice of lift to V.

Lemma 5.8 *Keep the notation of the preceding discussion. The following are equivalent:*

(i) $v \in V_{j+1}^g$,
(ii) $\ell^{-j}(g-\mathrm{id})\tilde{v} \in (\ell^{1-j}(\mathrm{im}(g-\mathrm{id}) \cap \ell^{j-1}V))/\ell V = (V_j^g)^\perp$,
(iii) $B(\ell^{-j}(g-\mathrm{id})\tilde{v}, w) = 0$ *for all* $w \in V_j^g$, *where B is the bilinear form associated to the quadratic form Q on V.*

Proof Given $v \in V_j^g$, we want to know when it is in V_{j+1}^g. The condition that $v \in V_j^g$ is equivalent to there being a lift $\tilde{v}$ of v to V such that $(g-\mathrm{id})\tilde{v} \in \ell^j V$. Fixing such a lift $\widetilde{v}$, the question is whether we can modify it to another lift $\widetilde{v}'$ such that $(g-\mathrm{id})\tilde{v}' \in \ell^{j+1}V$. The freedom for modification is that we can replace $\widetilde{v}$ by $\widetilde{v} + \ell\delta$ for some $\delta \in V$. So we want to know if δ can be chosen so that

$$(g-\mathrm{id})(\widetilde{v} + \ell\delta) \in \ell^{j+1}V,$$

or equivalently, so that

$$(g-\mathrm{id})\widetilde{v} \equiv \ell(g-\mathrm{id})\delta \mod \ell^{j+1}V.$$

Since we know that $(g-\mathrm{id})\widetilde{v} \in \ell^j V$ by assumption, we can rewrite this as

$$\ell^{-j}(g-\mathrm{id})\widetilde{v} = \ell^{1-j}(g-\mathrm{id})\delta \in V \otimes \mathbb{F}_\ell$$

for δ such that $(g-\mathrm{id})\delta \in \ell^{j-1}V$. This establishes the equivalence of (i) and (ii).

The equivalence of (ii) and (iii) then follows from Lemma 5.7. □

The $\mathbb{F}_\ell$-linear functional $w \mapsto B(\ell^{-j}(g-\mathrm{id})\tilde{v}, w)$ on V_j^g depends only on v, and expresses V_{j+1}^g as the kernel of a linear transformation $V_j^g \to (V_j^g)^\vee$, or equivalently as the radical of a bilinear form.

Lemma 5.9 *Keep the notation of the preceding discussion. Define the bilinear form on V_j^g:*

$$\langle v, w\rangle_j := B(\ell^{-j}(g-\mathrm{id})\tilde{v}, w).$$

Then

(i) V_{j+1}^g *is the radical of* $\langle\cdot,\cdot\rangle_j$.

(ii) $\langle\cdot,\cdot\rangle_j$ *is alternating.*

Proof Part (i) follows from Lemma 5.8. For (ii), we need to show that

$$B((g-\mathrm{id})\tilde{v},\tilde{v}) \in \ell^{j+1}\mathbb{Z}_\ell.$$

But this follows by observing:

$$\begin{aligned} B((g-\mathrm{id})\tilde{v},\tilde{v}) &= Q(g\tilde{v}) - Q((g-\mathrm{id})\tilde{v}) - Q(\tilde{v}) \\ &= -Q((g-\mathrm{id})\tilde{v}) \\ &= -\ell^{2j}Q(\ell^{-j}(g-\mathrm{id})\tilde{v}) \in \ell^{2j}\mathbb{Z}_\ell. \end{aligned}$$ □

We thus find that V^g_{j+1} is the kernel of an alternating form on V^g_j, so it remains only to show that as g varies over elements with fixed sequence $(V^g_1,\dots,V^g_j)$, this alternating form is uniformly distributed. It suffices to show this when g merely varies over elements of a fixed coset of $\Omega(V,Q)\subset O(V,Q)$. Let $\Omega_j\subset\Omega(V,Q)$ be the subgroup consisting of elements which are $1 \mod \ell^j$. We will show that the uniform distribution holds already when drawing uniformly from the coset $H=\Omega_j g$. For fixed v, changing $g\mapsto hg$ with $h\in\Omega_j$ changes the linear functional by

$$w\mapsto B(\ell^{-j}(h-1)g\tilde{v},w) = B(\delta_h gv,w) = B(\delta_h v, g^{-1}w),$$

where $\delta_h=\ell^{-j}(h-1)$. We view its reduction modulo as an element of the Lie algebra of the special fiber of $O(V,Q)$: $\overline{\delta_h}\in\mathrm{Lie}(O(V,Q)_{\mathbb{F}_\ell})$. To get equidistribution, it suffices for the induced homomorphism from Ω_j/Ω_{j+1} to the space $\wedge^2(V^g_j)^\vee$ of alternating forms on V^g_j, sending h to the restriction of $\overline{\delta}_h$, to be surjective.

5.2.1 The case $\ell>2$

If ℓ is odd, then Ω_1 is a pro-ℓ-group, and thus the spinor

norm vanishes on Ω_1. It immediately follows that the logarithm induces an isomorphism $\Omega_j/\Omega_{j+1}\xrightarrow{\sim}\mathrm{Lie}(O(V,Q)_{\mathbb{F}_\ell})\cong\wedge^2(V\otimes\mathbb{F}_\ell)^\vee$, hence the further projection map to $\wedge^2(V^g_j)^\vee$ is surjective.

5.2.2 The case $\ell=2$

For $\ell=2$, it may not be the case that Ω_j surjects on Lie $O(V,Q)$. However, $\Omega(V,Q)$ contains the commutator subgroup of $O(V,Q)$, and the image of the commutator subgroup in $\mathrm{Lie}(O(V,Q)_{\mathbb{F}_\ell})$ contains the image of $\mathrm{Ad}\,g-\mathrm{Id}$ for all $g\in O(V,Q)$. In particular, the image of Ω_j contains

$$(\mathrm{Ad}\,g-\mathrm{Id})\cdot\alpha = \alpha\mapsto g\alpha g^t-\alpha$$

for any $g\in O(V,Q)$ and any alternating form $\alpha\in\wedge^2(V\otimes\mathbb{F}_\ell)^\vee$.

Take g to be any lift of the reflection in a nonisotropic vector $v \in V_{\mathbb{F}_\ell}$ (i.e., a vector with $Q(v) \neq 0$). Denoting $v^* = B(v, \bullet) \in V^\vee$, $g \in V^\vee_{\mathbb{F}_\ell} \otimes V_{\mathbb{F}_\ell}$ can be represented by $\mathrm{Id} + \frac{v^*}{Q(v)} v$ (the unusual expression because we are in characteristic 2). Then

$$g\alpha g^t - \alpha = \frac{1}{Q(v)}(v^* \otimes v \cdot \alpha + \alpha \cdot v^* \otimes v) - \frac{1}{Q(v)^2}(v^* \otimes v)\alpha(v^* \otimes v).$$

A computation shows all $w^* \otimes v^*$ with $B(v, w) = 0$ are in the space generated by such expressions [7]

Since for any w, $\langle w \rangle^\perp$ is spanned by nonisotropic vectors, the space $\log(\Omega_j)$ in fact contains

$$\{v^* \wedge w^* : B(v, w) = 0\}, \tag{5.2}$$

and thus has codimension at most 1. The full Lie algebra Lie $O(V, Q)$ is generated over this space by any single element $v^* \wedge w^*$ with $B(v, w) \neq 0$. If W is any proper subspace of V, then we can pick $v \in W^\perp$ and $w \in V$ such that $B(v, w) \neq 0$. The image of $v^* \wedge w^*$ in $\wedge^2 W^\vee$ is zero, hence the restriction map from (5.2) to $\wedge^2(W^\vee)$ is surjective for any proper subspace $W \subset V$. Thus the only case in which the alternating form may not be equidistributed is when $V_j = V_0$. This completes the proof of Theorem 5.4. □

5.3 The BKLPR heuristic

We summarize the model for the Selmer group described in [1, Sect. 1.2].

5.3.1 The ℓ^∞ rank and Selmer distribution from BKLPR

Let $m \in \mathbb{Z}$ and $V = \mathbb{Z}_\ell^{2m}$, with the quadratic form $Q: V \to \mathbb{Z}_\ell$ given by

$$Q(x_1, \ldots, x_m, y_1, \ldots, y_m) = \sum_{i=1}^{m} x_i y_i.$$

A $\mathbb{Z}_\ell$-submodule $Z \subset V$ is called *isotropic* if $Q|_Z = 0$. Let $\mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$ be the set of maximal isotropic *summands* of V, hence each $Z \in \mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$ is a free $\mathbb{Z}_\ell$-module of rank m.

There is a probability measure on $\mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$ such that the distribution of $Z/\ell^e Z$ in $V/\ell^e V$ for each $e \geq 1$ is uniform [1, Sects. 1.2, 2, 4]. We define $\mathcal{Q}_{2m,\ell}$ (notated

[7] We spell out this computation in more detail. Let x be such that $B(x, v) = 1$. Take α to be represented by $x^* \otimes w \in V^*_{\mathbb{F}_\ell} \otimes V_{\mathbb{F}_\ell}$, where we have used B to identify V with V^*. Then $g\alpha g^t - \alpha$ is represented by

$$\underbrace{(v^* \otimes v)(x^* \otimes w)}_{v^* \otimes w} + \underbrace{(x^* \otimes w)(v^* \otimes v)}_{0} + \underbrace{(v^* \otimes v)(x^* \otimes w)(v^* \otimes v)}_{0}.$$

in [1] as $\mathscr{Q}_{2m}$) to be the distribution associated to the random variable S, valued in isomorphism classes of abelian groups, where S obtained by drawing Z and W from $\mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$ independently from this measure, and forming

$$S := \left(Z \otimes \frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}\right) \cap \left(W \otimes \frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}\right).$$

Remark 5.10 In [1], $\mathscr{Q}_{2m,\ell}$ and related distributions were defined on symplectic abelian groups, which are abelian groups together with a nondegenerate alternating pairing to $\mathbb{Q}/\mathbb{Z}$. Since two symplectic abelian groups are isomorphic *if and only if* their underlying abelian groups are isomorphic [1, §3.2], their distribution can be regarded as a distribution on abelian groups (which takes probability 0 on any abelian group not admitting a symplectic structure).

As $m \to \infty$ the distributions $\mathscr{Q}_{2m,\ell}$ converge to a discrete probability distribution $\mathscr{Q}_\ell$ [1, Theorem 1.2], which is conjectured in [1, Conjecture 1.3] to determine the asymptotic distribution of ℓ^∞-Selmer groups of elliptic curves ordered by height.

Furthermore, S fits naturally into a short exact sequence

$$0 \to R \to S \to T \to 0$$

where $R := (Z \cap W) \otimes \frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}$ and T is torsion. It is further conjectured that the joint distribution of (R, S, T) models the joint distribution of the rank of the elliptic curve (i.e., $R = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^r$ for r modeling the rank), the ℓ^∞-fSelmer group, and the ℓ-primary part of the Tate–Shafarevich group, respectively [1, Conjecture 1.3]. For example, the following proposition expresses the compatibility of these predictions with the Katz-Sarnak philosophy [27] that 50% of elliptic curves should have rank 0 and 50% should have rank 1.

Proposition 5.11 *([1, Proposition 5.6]) Let notation be as above. Fix* $W \in \mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$*. If* Z *is chosen randomly from* $\mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$ *(according to the above measure), then* $Z \cap W$ *has rank* 0 *with probability 1/2 and rank* 1 *with probability 1/2.*

5.3.2 The ℓ^∞ Selmer distribution from BKLPR conditioned on rank

Let $\mathscr{T}_{2m,r,\ell}$ be the distribution on finite abelian ℓ-groups, (notated in [1] as $\mathscr{T}_{2m,r}$) given by the above process in Sect. 5.3.1 *conditioned* on the assumption $\mathrm{rk}(Z \cap W) = r$. By [1, Theorem 1.6], these distributions converge as $m \to \infty$ to a discrete distribution $\mathscr{T}_{r,\ell}$, (notated in [1] as $\mathscr{T}_r$) which agrees with Delaunay's conjecture for the distribution of Ш$[\ell^\infty]$ of rank r elliptic curves over $\mathbb{Q}$ [1, p. 278].

There is another characterization of the distribution $\mathscr{T}_{r,\ell}$. For non-negative integers m, r with $m - r \in 2\mathbb{Z}_{\geq 0}$, let A be drawn randomly from the Haar probability measure on the set of *alternating* $m \times m$-matrices over $\mathbb{Z}_\ell$ having rank $m - r$, and $\mathscr{A}_{m,r,\ell}$ be the distribution of $(\mathrm{coker}\, A)_{\mathrm{tors}}$. According to [1, Theorem 1.10], as $m \to \infty$ through integers with $m - r \in 2\mathbb{Z}_{\geq 0}$, the distributions $\mathscr{A}_{m,r,\ell}$ converge to a limit $\mathscr{A}_{r,\ell}$, which coincides with $\mathscr{T}_{r,\ell}$.

Finally, [1, Sect. 5.6] predicts that, conditioned on elliptic curves having rank r, Ш is distributed as the direct sum over all primes ℓ of a finite abelian group drawn from $\mathscr{T}_{r,\ell}$.

5.3.3 The BKLPR *n*-Selmer distribution

We next review the model for n-Selmer elements described at the beginning of [1, Sect. 5.7]. Let $\mathscr{T}_{r,\ell}$ denote the random variable defined on isomorphism classes of finite abelian ℓ groups (notated $\mathscr{T}_r$ in [1]) defined in [1, Theorem 1.6] and reviewed in Sect. 5.3.2. For G an abelian group, we let $G[n]$ denote the n torsion of G. For $n \in \mathbb{Z}_{\geq 1}$ with prime factorization $n = \prod_{\ell \mid n} \ell^{a_\ell}$, define a distribution $\mathscr{T}_{r,\mathbb{Z}/n\mathbb{Z}}$ on finitely generated $\mathbb{Z}/n\mathbb{Z}$ modules by choosing a collection of abelian groups $\{T_\ell\}_{\ell \mid n}$, with T_ℓ drawn from $\mathscr{T}_{r,\ell}$, and defining the probability $\mathscr{T}_{r,\mathbb{Z}/n\mathbb{Z}} = G$ to be the probability that $\oplus_{\ell \mid n} T_\ell[n] \simeq G$.

Given the above predicted distribution for the n-Selmer group of elliptic curves of rank r, the heuristic that 50% of elliptic curves have rank 0 and 50% have rank 1 leads to the following predicted joint distribution of the n-Selmer group and rank:

Definition 5.12 Let $(\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}})$ be the joint distribution on $\mathbb{Z}_{\geq 0} \times \mathrm{Ab}_n$ defined by

$$\mathrm{Prob}((\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}}) = (r, G)) = \begin{cases} \frac{1}{2}\mathscr{T}_{r,\mathbb{Z}/n\mathbb{Z}} & \text{if } r \leq 1 \\ 0 & \text{if } r \geq 2. \end{cases}$$

5.4 Markov property for the BKLPR model

Fix $Z, W \in \mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$ and set $S = (Z \otimes \frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}) \cap (W \otimes \frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell})$. Define

$$S_j := \left(\underbrace{W/\ell^j \cap Z/\ell^j}_{\subset V/\ell^j} + \frac{\ell V}{\ell^j V} \right) / \ell V, \tag{5.3}$$

which are the analogues of the V_j in Lemma 5.6. Although S_j depends on Z and W, and will be viewed as a random variable in the future, we suppress this dependence for notational convenience. The main result of this subsection is the following Theorem 5.13, and the proof encompasses the remainder of this subsection.

Theorem 5.13 *Let V, Z, and W be as in Sect. 5.3. Define random variables, valued in isomorphism classes of finite-dimensional $\mathbb{F}_\ell$-vector spaces, by $S_0 := V \otimes \mathbb{F}_\ell$, and $S_1, S_2, \ldots, S_j, \ldots$ as in (5.3). Then, the sequence $S_1, S_2, \ldots$ is Markov, and the distribution of* $\dim S_{i+1}$ *given S_i coincides with the distribution of the dimension of the kernel of a uniformly random alternating form on S_i.*

We omit the proof of the following lemma, which is similar to that of Lemma 5.6.

Lemma 5.14 *Keep the notation above. Under the identification*

$$\left(V \otimes \frac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell}\right)[\ell] \xrightarrow{\sim} V \otimes \mathbb{F}_\ell,$$

we have

$$\ell^{j-1} \cdot S[\ell^j] \xrightarrow{\sim} S_j.$$

The non-degenerate bilinear form B on V induces a non-degenerate bilinear form on $V \otimes \mathbb{F}_\ell$, that we denote by $\overline{B}$. We may sometimes abbreviate notation by using $\overline{B}(v, x)$, with $v \in V$ and $x \in V \otimes \mathbb{F}_\ell$, to denote $\overline{B}(v \pmod{\ell}, x)$.

We will construct the sequence of alternating forms (one for each S_j, whose radical is S_{j+1}) referenced in Theorem 5.13.

Lemma 5.15 *Identifying* $\ell^{1-j}(\ell^{j-1}V/\ell^j V) \xrightarrow{\sim} V \otimes \mathbb{F}_\ell$*, the orthogonal complement of* S_j *in* $V \otimes \mathbb{F}_\ell$ *is* $\ell^{1-j}\left((Z/\ell^j + W/\ell^j) \cap \ell^{j-1}V/\ell^j V\right)$.

Proof Inside $V/\ell^j V$, we have

$$\begin{aligned}\left(Z/\ell^j \cap W/\ell^j\right)^\perp &= Z^\perp/\ell^j + W^\perp/\ell^j \\ &= Z/\ell^j + W/\ell^j\end{aligned}$$

using that Z and W are maximal isotropic. Therefore,

$$\begin{aligned}\left((Z/\ell^j \cap W/\ell^j) + \ell V/\ell^j\right)^\perp &= (Z/\ell^j \cap W/\ell^j)^\perp \cap (\ell V/\ell^j)^\perp \\ &= (Z/\ell^j + W/\ell^j) \cap \ell^{j-1}V/\ell^j.\end{aligned}$$

The result then follows by tensoring with $\mathbb{F}_\ell$. □

Next, given $v \in S_j$, we seek to characterize when $v \in S_{j+1}$. By definition, $v \in S_j$ is equivalent to the existence of a representative $\widetilde{v} \in W/\ell^j \cap Z/\ell^j$ reducing to v mod ℓ, and lifts w_v of $\widetilde{v}$ to W and z_v of $\widetilde{v}$ to Z such that $w_v \equiv z_v \pmod{\ell^j V}$. Hence $w_v - z_v = \ell^j \epsilon$ for some $\epsilon \in V$.

Lemma 5.16 *With notation above,* $v \in S_j$ *lies in* S_{j+1} *if and only if the associated* ϵ *as above satisfies* $\epsilon \in \ell^{1-j}\left((Z/\ell^j + W/\ell^j) \cap \ell^{j-1}V/\ell^j V\right)$.

Proof For $v \in S_{j+1}$, if we can find other lifts $\widetilde{v}'$, w_v', z_v' satisfying the same conditions, but such that $w_v' \equiv z_v' \pmod{\ell^{j+1}}$. Such modifications are exactly of the form $w_v' = w_v + \ell\delta_W$ with $\delta_W \in W$ and $z_v' = z_v + \ell\delta_Z$ with $\delta_Z \in Z$. Hence $v \in S_{j+1}$ if and only if we can choose δ_W, δ_Z such that

$$w_v + \ell\delta_W \overset{?}{=} z_v + \ell\delta_Z + \ell^{j+1}\epsilon'.$$

Since $w_v = z_v + \ell^j\epsilon$, this is equivalent to solving

$$\ell^{j-1}\epsilon \equiv \delta_W - \delta_Z \pmod{\ell^j} \quad \text{for some } \delta_W \in W/\ell^j, \delta_Z \in Z/\ell^j.$$

which is equivalent to

$$\epsilon \in \ell^{1-j}\left((Z/\ell^j + W/\ell^j) \cap \ell^{j-1}V/\ell^j V\right). \qquad \square$$

Lemma 5.17 *There is a well defined bilinear form*

$$A_j : S_j \times S_j \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$$

given by

$$A_j(v, x) := \overline{B}(\epsilon, x) = \overline{B}(\ell^{-j}(w_v - z_v), x). \tag{5.4}$$

Proof We need to check that the value

$$\overline{B}(\epsilon, x) = \overline{B}(\ell^{-j}(w_v - z_v), x) \mod \ell. \tag{5.5}$$

is independent of the choices of $\widetilde{v}$, w_v, and z_v. Indeed, any other allowable w'_v differs from w_v by an element of $\ell^j W$, say $\ell^j\delta$ with $\delta \in W$. But since W/ℓ is isotropic and x lies in $S_j \subset W/\ell \subset V/\ell$, we have $B(\delta, x) \equiv 0 \pmod{\ell}$. Similarly, replacing z_v with any other allowable z'_v will not alter (5.5). □

Lemma 5.18 *Keep the notation of the preceding discussion.*

(i) The radical of A_j is S_{j+1}.
(ii) A_j is alternating.

Proof By definition, $v \in S_j$ is in the radical of A_j if and only if (following the notation above) $\epsilon_v := \ell^{-j}(w_v - z_v)$ lies in $S_j^\perp$. But by Lemma 5.15, $\epsilon \in S_j^\perp$ if and only if $\epsilon_v \in \ell^{1-j}\left((Z/\ell^j + W/\ell^j) \cap \ell^{j-1}V/\ell^j V\right)$, which, as we proved in Lemma 5.16, occurs if and only if $\epsilon \in S_{j+1}$.

For (ii), since we can take z_v as a lift of v to V, it suffices to check $B(w_v - z_v, z_v) \in \ell^{j+1}\mathbb{Z}_\ell$. For this, write $w_v - z_v = \ell^j\epsilon$ and observe that Z and W are isotropic for Q, we have

$$\begin{aligned} B(w_v - z_v, z_v) &= Q(w_v) - Q(w_v - z_v) - Q(z_v) \\ &= Q(w_v - z_v) \\ &= Q(\ell^j\epsilon) \\ &= \ell^{2j}Q(\epsilon) \in \ell^{j+1}\mathbb{Z}_\ell. \end{aligned} \qquad \square$$

As in Sect. 5.1, it suffices to show that as Z and W are drawn from the canonical measure on $\mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$, the alternating form A_j is uniformly distributed.

Lemma 5.19 *$O(V, Q)$ acts transitively on* $\mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$.

Proof Fix $W, Z \in \mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$. Then we have a scheme

$$\mathrm{Isom}(W, Z) = \{g \in O(V, Q): gW = Z\} \subset O(V, Q)$$

over $\mathbb{Z}_\ell$. This is evidently a torsor for the parabolic subgroup $\mathrm{Isom}(W, W) \subset O(V, Q)$. Moreover, Witt's theorem implies that $\mathrm{Isom}(W, Z)$ has a point over $\mathbb{F}_\ell$, which lifts to a $\mathbb{Z}_\ell$-point because $\mathrm{Isom}(W, Z)$ is smooth (being a torsor for a smooth group scheme). □

It will suffice to show that conditioning on a fixed W, the distribution of A_j is already uniform. The distribution of Z conditioned on a fixed W coincides with the orbit measure on $\mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$ induced by the Haar measure on $O(V, Q)$, since $O(V, Q)$ acts transitively on $\mathrm{OGr}_{(V,Q)}(\mathbb{Z}_\ell)$ by Lemma 5.19. As in Sect. 5.1, it suffices to show that the distribution of A_j is already uniform as Z varies over an orbit of a coset of the principal congruence subgroup

$$\Gamma(\ell^j) := \{g \in O(V, Q): g \equiv \mathrm{Id} \pmod{\ell^j}\}.$$

For fixed Z^0, which induces the alternating form

$$A_j(v, x) = \overline{B}(\ell^{-j}(w_v - z_v^0), x),$$

the alternating form associated to γZ^0 for $\gamma \in \Gamma(\ell^j)$ is

$$\overline{B}(\ell^{-j}(w_v - \gamma z_v^0), x)$$

which changes the functional by

$$x \mapsto \overline{B}(\ell^{-j}(1 - \gamma)z_v^0, x).$$

Now, since the map $\gamma \mapsto 1 - \gamma$ induces an isomorphism $\Gamma(\ell^j)/\Gamma(\ell^{j+1}) \xrightarrow{\sim} \mathrm{Lie}\, O(V_{\mathbb{F}_\ell}, Q)$, the resulting alternating form A_j is uniformly distributed, so we are done. □

Remark 5.20 Note that unlike in the case of the random kernel model, where we had additional complications to deal with associated to $\ell = 2$ in Sect. 5.2.2, there are no additional complications here for $\ell = 2$ in the proof of Theorem 5.13, because here we are working with the full congruence subgroup $\Gamma(\ell^j)$, instead of a subgroup which may have index 2, as was the case in Sect. 5.2.

6 Proofs of the main theorems

We conclude the paper by proving our main theorems. In Sect. 6.1 we connect the actual Selmer distribution to the random kernel model, while in Sect. 6.2 we connect the random kernel model to the BKLPR distribution. Combining these gives us a proof of our main theorem, Theorem 1.1. Finally, in Sect. 6.3 we prove Corollaries 1.6 and 1.7.

6.1 Comparing the Selmer distribution with the random kernel model

To start, we state one of our main theorems, which compares the distribution of Selmer groups of elliptic curves to the random kernel model. We prove this at the end of the subsection.

Theorem 6.1 *Fix integers $d \geq 2$ and $n \geq 1$. For q ranging over prime powers, with $\gcd(q, 2n) = 1$ and $(r, G) \in \mathbb{Z}_{\geq 0} \times Ab_n$, we have*

$$\operatorname{Prob}(\operatorname{Sel}_n^d / \mathbb{F}_q(t) \simeq G) = \operatorname{Prob}(RSel_{n,\mathbb{F}_q}^d = G) + O_{n,d}(q^{-1/2}) \tag{6.1}$$

and

$$\begin{aligned}\operatorname{Prob}((rk, Sel_n)_{\mathbb{F}_q}^d = (r, G)) &= \operatorname{Prob}((rk^{an}, Sel_n)_{\mathbb{F}_q}^d = (r, G)) + O_{n,d}(q^{\frac{-1}{216d^2-162d+31}}) \\ &= \operatorname{Prob}((Rrk, RSel_n)_{\mathbb{F}_q}^d = (r, G)) + O_{n,d}(q^{\frac{-1}{216d^2-162d+31}}).\end{aligned} \tag{6.2}$$

In particular,

$$\limsup_{\substack{q\to\infty \\ \gcd(q,2n)=1}} (rk^{an}, Sel_n)_{\mathbb{F}_q}^d = \limsup_{\substack{q\to\infty \\ \gcd(q,2n)=1}} (rk, Sel_n)_{\mathbb{F}_q}^d = \limsup_{q\to\infty} (Rrk, RSel_n)_{\mathbb{F}_q}^d \tag{6.3}$$

$$\liminf_{\substack{q\to\infty \\ \gcd(q,2n)=1}} (rk^{an}, Sel_n)_{\mathbb{F}_q}^d = \liminf_{\substack{q\to\infty \\ \gcd(q,2n)=1}} (rk, Sel_n)_{\mathbb{F}_q}^d = \liminf_{q\to\infty} (Rrk, RSel_n)_{\mathbb{F}_q}^d, \tag{6.4}$$

The values of (6.3) and (6.4) agree when d is odd or $n \leq 2$, but differ when d is even and $n > 2$.

We are nearly ready to prove Theorem 6.1, but first we will need to establish two preliminary results. The first preliminary result relates the Selmer group of an elliptic curve to the 1-eigenspace of Frobenius.

Lemma 6.2 *For $n \geq 1, d \geq 2$ and $[E_x] = x \in \mathscr{W}^{\circ d}_{\mathbb{Z}[1/2n]}(\mathbb{F}_q)$, we have*

$$\operatorname{Sel}_n(E_x) = \ker\left(\rho^d_{n,\mathbb{Z}[1/2n]}(\operatorname{Frob}_x) - \operatorname{id}|_{\left(\underline{\mathscr{W}}^{\circ d}_{k}\right)_x}\right).$$

Proof Notate the geometric fiber of $\underline{\mathscr{W}}^{\circ d}_{k}$ over x by $\left(\underline{\operatorname{Sel}}^{\circ d}_{n,k}\right)_{\overline{x}}$, and the fiber by $\left(\underline{\operatorname{Sel}}^{\circ d}_{n,k}\right)_{x}$. Since $\left(\underline{\mathscr{W}}^{\circ d}_{k}\right)_x$ is a finite étale $\mathbb{F}_q$-scheme, we have

$$\left(\underline{\operatorname{Sel}}^{\circ d}_{n,k}\right)_{x}(\mathbb{F}_q) = \ker\left(\rho^d_{n,\mathbb{Z}[1/2n]}(\operatorname{Frob}_x) - \operatorname{id}|_{\left(\underline{\mathscr{W}}^{\circ d}_{k}\right)_{\overline{x}}}\right).$$

Hence, combining this with Lemma 2.3, we obtain that for $[E_x] = x \in \underline{\mathscr{W}}^{\circ d}_{k}$,

$$\ker\left(\rho^d_{n,\mathbb{Z}[1/2n]}(\operatorname{Frob}_x) - \operatorname{id}|_{\left(\underline{\mathscr{W}}^{\circ d}_{k}\right)_{\overline{x}}}\right) = \operatorname{Sel}_n(E_x).$$

Here we are using that there is an isomorphism $(\underline{\mathrm{Sel}}^{\circ d}_{n,k})_x \simeq (\mathrm{Sel}^{\circ d}_{n,k})_{x'}$ for $x' \in \mathscr{W}^{\circ d}_{k}$ mapping to x, coming from the definition of $\underline{\mathrm{Sel}}^{\circ d}_{n,k}$ and $\underline{\mathscr{W}}^{\circ d}_{k}$ as quotients of $\mathrm{Sel}^{\circ d}_{n,k}$ and $\mathscr{W}^{\circ d}_{k}$ by a compatible group action. □

Our second preliminary result relates the rank of an elliptic curve $[E_x] \in \mathscr{W}^{\circ d}_{k}(\mathbb{F}_q)$ to the Dickson invariant of $\rho^{d}_{\mathbb{Z}_\ell,k}(\mathrm{Frob}_x)$.

Recall from Definition 3.1 that $(Q^d_{\mathbb{Z}}, V^d_{\mathbb{Z}})$ denotes the quadratic space over $\mathbb{Z}$, whose reduction mod n is (Q^d_n, V^d_n) on which the monodromy representation $\rho^d_{n,k}$ acts. Let $(Q^d_{\mathbb{Z}_\ell}, V^d_{\mathbb{Z}_\ell}) := (Q^d_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell, V^d_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)$ denote the base change to $\mathbb{Z}_\ell$.

Proposition 6.3 *Let $d \geq 2$, and let ℓ be a prime. For q a prime power with* $\gcd(q, 2\ell) = 1$*, define*

$$\mathcal{W}^{d,\mathrm{rk}^{an}\leq 1}_{\ell,q} := \left\{[E_x] = x \in \mathscr{W}^{\boxslash d}_{\mathbb{Z}[1/2\ell]}(\mathbb{F}_q) : \mathrm{rk}^{an}(E_x) \leq 1\right\}.$$

(1) For q ranging over prime powers with $\gcd(q, 2\ell) = 1$*, we have*

$$\frac{\#\mathcal{W}^{d,\mathrm{rk}^{an}\leq 1}_{\ell,q}}{\#\mathscr{W}^{\boxslash d}_{\mathbb{Z}[1/2\ell]}(\mathbb{F}_q)} = 1 + O_d\left(q^{\frac{-1}{216d^2-162d+31}}\right).$$

(2) For all $x \in \mathcal{W}^{d,\mathrm{rk}^{an}\leq 1}_{\ell,q} \subset \mathscr{W}^{\boxslash d}_{\mathbb{Z}[1/2\ell]}(\mathbb{F}_q)$, we have

$$\begin{aligned}&\mathrm{rk}\ker\left(\rho^d_{\mathbb{Z}_\ell,\mathbb{Z}[1/2\ell]}(\mathrm{Frob}_x) - \mathrm{id}\right)\\ &\quad= \begin{cases} 0 & \iff \rho^d_{\mathbb{Z}_\ell,\mathbb{Z}[1/2\ell]}(\mathrm{Frob}_x) \in SO(Q^d_{\mathbb{Z}_\ell}) \\ 1 & \iff \rho^d_{\mathbb{Z}_\ell,\mathbb{Z}[1/2\ell]}(\mathrm{Frob}_x) \notin SO(Q^d_{\mathbb{Z}_\ell}).\end{cases}\end{aligned}$$

(3) The above statements are true with analytic rank replaced by algebraic rank.

Proof To start, observe that (2) follows directly from Lemma 3.18 and Proposition 3.22

We next demonstrate (1). By Lemma 3.18, whenever $x \in \mathscr{W}^{\boxslash d}_{\mathbb{Z}}[1/2\ell]$, the analytic rank of E_x is equal to the rank of the 1-generalized eigenspace of $\rho^d_{\mathbb{Z}_\ell,\mathbb{Z}[1/2\ell]}(\mathrm{Frob}_x) - \mathrm{id}$.

By Proposition 3.22, whenever $x \notin \mathcal{W}^{d,\mathrm{rk}^{\mathrm{an}}\leq 1}_{\ell,q}$, there is a particular Zariski closed hypersurface Z in the algebraic group $O(Q^d_{\mathbb{Z}_\ell})$, i.e., the hypersurface parameterizing elements with a two or more dimensional generalized 1-eigenspace, such that $\rho^d_{\mathbb{Z}_\ell,\mathbb{Z}[1/2\ell]}(\mathrm{Frob}_x) \in Z(\mathbb{Z}_\ell)$. By Lemma 3.20, for any positive integer e, we have

$$\begin{aligned}&\mathrm{im}(Z(\mathbb{Z}/\ell^e\mathbb{Z}) \to O(Q^d_{\mathbb{Z}_\ell})(\mathbb{Z}/\ell^e\mathbb{Z}))\\ &\quad= O_Z\left(\ell^{e(\dim O(Q^d_{\mathbb{Z}_\ell})-1)}\right)\end{aligned}$$

$$= O_{\ell,d}\left(\ell^{e(\dim O(Q^d_{\mathbb{Z}_\ell})-1)}\right).$$

By Theorem 3.14, we know $\operatorname{im}\rho^d_{\ell^e,\mathbb{Z}[1/2\ell]}$ has index at most 2 in $O(Q^d_{\mathbb{Z}_\ell})$, and hence has size within a constant factor of $\ell^{e\dim O(Q^d_{\mathbb{Z}_\ell})}$. Therefore, it follows from Proposition 3.9 that

$$\begin{aligned}
&\frac{\#\left(\mathscr{W}^{\boxslash d}_{\mathbb{Z}[1/2\ell]}(\mathbb{F}_q) - \mathcal{W}^{d,\mathrm{rk}^{\mathrm{an}}\le 1}_{\ell,q}\right)}{\#\mathscr{W}^{\boxslash d}_{\mathbb{Z}[1/2\ell]}(\mathbb{F}_q)} \\
&\quad = \frac{\#\operatorname{im}(Z(\mathbb{Z}/\ell^e\mathbb{Z}) \to O(Q^d_{\mathbb{Z}_\ell}))}{\#\operatorname{im}\rho^d_{\ell^e,\mathbb{Z}[1/2\ell]}} \\
&\qquad + O_d\left(\#\operatorname{im}\rho^d_{\ell^e,\mathbb{Z}[1/2\ell]}\sqrt{\frac{\#\operatorname{im}(Z(\mathbb{Z}/\ell^e\mathbb{Z}) \to O(Q^d_{\mathbb{Z}_\ell}))}{q}}\right) \\
&\quad = O_{\ell,d}\left(\frac{\ell^{e(\dim O(Q^d_{\mathbb{Z}_\ell})-1)}}{\ell^{e\dim O(Q^d_{\mathbb{Z}_\ell})}} + q^{-1/2}\ell^{e\dim O(Q^d_{\mathbb{Z}_\ell})}\ell^{\frac{1}{2}e(\dim O(Q^d_{\mathbb{Z}_\ell})-1)}\right) \\
&\quad = O_{\ell,d}\left(\ell^{-e} + q^{-1/2}(\ell^e)^{(\frac{3}{2}\dim O(Q^d_{\mathbb{Z}_\ell})-\frac{1}{2})}\right).
\end{aligned} \tag{6.5}$$

Crucially, the above constant does not depend on e, and so we may freely choose e to minimize the above error term. Indeed, we may take e to be the least positive integer so that $q \le (\ell^e)^{(1+3\dim O(Q^d_{\mathbb{Z}_\ell}))}$, or equivalently $q^{\frac{1}{1+3\dim O(Q^d_{\mathbb{Z}_\ell})}} \le \ell^e$. Then, so long as $q > \ell$, replacing q by $(\ell^e)^{(1+3\dim O(Q^d_{\mathbb{Z}_\ell}))}$ will introduce at most a factor of ℓ, and so

$$\begin{aligned}
O_{\ell,d}(\ell^{-e}) &= O_{\ell,d}(q^{\frac{-1}{1+3\dim O(Q^d_{\mathbb{Z}_\ell}))}}) \\
O_{\ell,d}(q^{-1/2}(\ell^e)^{(\frac{3}{2}\dim O(Q^d_{\mathbb{Z}_\ell})-\frac{1}{2})}) &= O_{\ell,d}\left(q^{-\frac{1}{2}+\frac{\frac{3}{2}\dim O(Q^d_{\mathbb{Z}_\ell})-\frac{1}{2}}{1+3\dim O(Q^d_{\mathbb{Z}_\ell})}}\right) = O_{\ell,d}\left(q^{\frac{-1}{1+3\dim O(Q^d_{\mathbb{Z}_\ell})}}\right).
\end{aligned} \tag{6.6}$$

Further, for the finitely many $q < \ell$, we can adjust the constants so that the above still holds with no dependence on q.

Combining (6.5) and (6.6), we find

$$\frac{\#\left(\mathscr{W}^{\boxslash d}_{\mathbb{Z}[1/2\ell]}(\mathbb{F}_q) - \mathcal{W}^{d,\mathrm{rk}^{\mathrm{an}}\le 1}_{\ell,q}\right)}{\#\mathscr{W}^{\boxslash d}_{\mathbb{Z}[1/2\ell]}(\mathbb{F}_q)} = O_{\ell,d}\left(q^{\frac{-1}{1+3\dim O(Q^d_{\mathbb{Z}_\ell}))}}\right).$$

Further, the constant above does not depend on ℓ because the analytic rank, and hence the subset $\mathcal{W}^{d,\mathrm{rk}^{\mathrm{an}}\le 1}_{\ell,q} \subset \mathscr{W}^{\boxslash d}_{\mathbb{Z}[1/2\ell]}(\mathbb{F}_q)$ is independent of the auxiliary choice of ℓ.

Now, (1) follows because

$$\frac{-1}{1+3\dim O(Q^d_{\mathbb{Z}_\ell}))} = \frac{-1}{1+\frac{3(12d-4)(12d-5)}{2}}$$
$$= \frac{-1}{1+3(6d-2)(12d-5)} = \frac{-1}{216d^2-162d+31}.$$

Part (3) follows from the proceeding ones and fact that, for elliptic curves of rank at most 1 over $\mathbb{F}_q$ of characteristic ≥ 3, we know on a full density (as $q \to \infty$) subset that algebraic rank equals analytic rank. For char $\mathbb{F}_q > 3$ the statement holds for every elliptic curve of rank at most 1, as explained in [40, Sect. 3.8], using the analogue of the Gross-Zagier formula in [41, Theorem 1.2]. If char $\mathbb{F}_q = 3$, it follows by combining [40, Sect. 3.8] with the Gross-Zagier formula for everywhere semistable elliptic curves in [44, Remark 1.5]. Note that there is an open subscheme $\mathscr{W}^{\boxslash d}_B \subset \mathscr{W}^{\circ d}_B$ parameterizing those elliptic surfaces which have squarefree discriminant, so are everywhere semistable. This is fiberwise dense over B by [28, Lemma 3.14], so that in the large q limit, a density 1 subset of $\mathscr{W}'^d_B(\mathbb{F}_q)$ corresponds to elliptic curves with everywhere semistable reduction. □

Proof of Theorem 6.1 We will explain how the distribution of $(\mathrm{rk}^{\mathrm{an}}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ and $(\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$, up to an error of $O_{n,d}(q^{\frac{-1}{216d^2-162d+31}})$, are determined by the distributions of Frob_x for $x \in \mathcal{W}^{d,\mathrm{rk}^{\mathrm{an}}\leq 1}_{\ell,q} \subset \underline{\mathscr{W}}^{\boxslash^{\mathbb{F}_q}}_d(\mathbb{F}_q)$, as defined in Proposition 6.3. By definition, these distributions are determined by Frob_x for $x \in \underline{\mathscr{W}}'^d_{\mathbb{F}_q}(\mathbb{F}_q)$, so we only need justify why there are $O_{n,d}(q^{\frac{-1}{216d^2-162d+31}})$ points in $\underline{\mathscr{W}}^{\boxslash^{\mathbb{F}_q}}_d(\mathbb{F}_q) - \mathcal{W}^{d,\mathrm{rk}^{\mathrm{an}}\leq 1}_{\ell,q}$,

To start, we explain why $(\mathrm{rk}^{\mathrm{an}}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ and $(\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ agree with their restrictions from $\underline{\mathscr{W}}'^d_{\mathbb{F}_q}(\mathbb{F}_q)$ to $\underline{\mathscr{W}}^{\boxslash^{\mathbb{F}_q}}_d(\mathbb{F}_q)$, up to an error of $O_{n,d}(q^{-1/2})$. The argument here is analogous to that in Remark 1.4. Indeed, the closed substack $\underline{\mathscr{W}}^{\boxslash^{\mathbb{F}_q}}_d - \underline{\mathscr{W}}'^d_{\mathbb{F}_q} \subset \underline{\mathscr{W}}'^d_{\mathbb{F}_q}$ has positive codimension. Hence, contributes at most $O_{n,d}(q^{-1/2})$ to the distributions $(\mathrm{rk}^{\mathrm{an}}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ and $(\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$, as can be deduced from the Lang-Weil estimate and [28, Lemma 5.3].

We next explain how to relate the distribution of $\rho^d_{n,\mathbb{Z}[1/2]}(\mathrm{Frob}_x)$ over $x \in \underline{\mathscr{W}}^{\boxslash^{\mathbb{F}_q}}_d(\mathbb{F}_q)$ to $(\mathrm{rk}^{\mathrm{an}}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ and $(\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$. The key will be the following two results shown above.

(i) By Lemma 6.2, we have $\mathrm{Sel}_n(E_x) = \ker\left(\rho^d_{n,\mathbb{Z}[1/2n]}(\mathrm{Frob}_x) - \mathrm{id}\,|_{\left(\underline{\mathscr{W}}^{\circ d}_{\mathbb{F}_q}\right)_x}\right)$.

(ii) By Proposition 6.3, there is a subset $\mathcal{W}^{d,\mathrm{rk}^{\mathrm{an}}\leq 1}_{\ell,q} \subset \underline{\mathscr{W}}^{\boxslash^{\mathbb{F}_q}}_d(\mathbb{F}_q)$ whose density is $1 + O_d(q^{\frac{-1}{216d^2-162d+31}})$ for q ranging over prime powers with $\gcd(q, 2\ell) = 1$ such that

$$\mathrm{rk}(E_x) = \mathrm{rk}^{\mathrm{an}}(E_x) = \delta_{\rho^d_{n,\mathbb{Z}[1/2n]}(\mathrm{Frob}_x)\notin SO(Q^d_n)},$$

where $\delta_{a \notin B} = 1$ if $a \notin B$ and 0 if $a \in B$.

The observation (i) then establishes (6.1). Combining (i) and (ii) with the preceding discussion, we have explained how the distribution of Frobenius elements determines the joint distributions $(\mathrm{rk}^{\mathrm{an}}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ and $(\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$, up to an error of $O_{n,d}(q^{\frac{-1}{216d^2-162d+31}})$. By Corollaries 4.3 and 3.11, up to an error of $O_{n,d}(q^{-1/2})$, the elements $\rho^d_{n,\mathbb{Z}[1/2n]}(\mathrm{Frob}_x)$ are equidistributed between the two cosets of $\Omega(Q^d_n)$ given by

$$\left(\mathrm{D}_{Q^d_n}, \mathrm{sp}^-_{Q^d_n}\right) \in \left\{\left((0, \ldots, 0), [q^{d-1}]\right), \left((1, \ldots, 1), [q^{d-1}]\right)\right\}.$$

This describes the distribution $(\mathrm{Rrk}, \mathrm{RSel}_n)^d_{\mathbb{F}_q}$ and hence yields (6.2), (6.3) and (6.4).

To conclude the proof we need justify the values of (6.3) and (6.4) agree when d is odd or $n \le 2$ but differ when d is even and $n > 2$. Because these limits approach $(\mathrm{Rrk}, \mathrm{RSel}_n)^d_{\mathbb{F}_q}$, it suffices to show $(\mathrm{Rrk}, \mathrm{RSel}_n)^d_{\mathbb{F}_q}$ is independent of q when d is odd or $n \le 2$ but depends on q when d is even. When d is odd, this follows from Definition 4.2 because the square class of q^{d-1} is always trivial, hence independent of q. Also, when $n \le 2$, this holds again by Definition 4.2 because the spinor norm is trivial. However, when d is even and $n > 2$, the spinor norm is nontrivial, and $(\mathrm{Rrk}, \mathrm{RSel}_n)^d_{\mathbb{F}_q}$ will change depending on whether q is a square or nonsquare. Indeed, when q is a square, $\mathrm{Prob}(\mathrm{RSel}^d_{n,\mathbb{F}_q} = (\mathbb{Z}/n\mathbb{Z})^{12d-4}) > 0$, corresponding to the case that $g = \mathrm{id}$ in Definition 4.2, while when q is not a square, $\mathrm{Prob}(\mathrm{RSel}^d_{n,\mathbb{F}_q} = (\mathbb{Z}/n\mathbb{Z})^{12d-4}) = 0$. □

6.2 Comparing the random kernel model with the BKLPR heuristic

We now prove:

Theorem 6.4 *The TV distance between the BKLPR heuristic and* $\limsup_{q\to\infty}(Rrk, RSel_n)^d_{\mathbb{F}_q}$ *is* $O(2^{-(6d-2)^2})$, *where the implicit constant is absolute, and similarly for the TV distance between the BKLPR heuristic and* $\liminf_{q\to\infty}(Rrk, RSel_n)^d_{\mathbb{F}_q}$

In particular, we have

$$\begin{aligned}(rk^{BKLPR}, Sel_n^{BKLPR}) &= \lim_{d\to\infty} \limsup_{q\to\infty}(Rrk, RSel_n)^d_{\mathbb{F}_q} \\ &= \lim_{d\to\infty} \liminf_{q\to\infty}(Rrk, RSel_n)^d_{\mathbb{F}_q}.\end{aligned}$$

Proof By Definition 4.2, with probability one the rank is 0 or 1, and determined by whether the random g in the random kernel model has Dickson invariant 0 or 1, respectively. Hence the rank component of these distributions is completely determined by the Selmer component, we can focus our attention on the Selmer component.

Thanks to Corollary 4.24, we know that the TV distance between $\liminf_{q\to\infty}$ $\dim \mathrm{RSel}^d_{\ell,\mathbb{F}_q}$ and the BKLPR heuristic for Sel_ℓ is $O(\ell^{-(6d-2)^2})$, and similarly for

$\limsup_{q\to\infty}$ in place of $\liminf_{q\to\infty}$. The Markov properties Theorem 5.1 and Corollary 5.2 and Theorem 5.13 imply that for $\ell > 2$, the two distributions for Sel_{ℓ^e} agree conditioned upon them agreeing for Sel_ℓ. For $\ell = 2$, the same is true as long as $d_1 < 12d - 4$ where the notation d_1 is as in Theorem 5.1, which only fails if g reduces to the identity element in $\mathrm{O}(12d-4, \mathbb{F}_\ell)$. This happens with probability $1/\#\mathrm{O}(12d-4, \mathbb{F}_\ell)$, which is negligible compared to the error term we seek. We conclude that the TV distance between the two distributions for Sel_{ℓ^e} is also $O(\ell^{-(6d-2)^2})$.

Finally, we consider general n. For $n = \prod \ell^{a_\ell}$, the prime factorization of n, we have

$$\mathrm{Sel}_n \cong \oplus_\ell \mathrm{Sel}_{\ell^{a_\ell}}.$$

The BKLPR heuristic predicts that the distributions of the $\mathrm{Sel}_{\ell^{a_\ell}}$ are independent after conditioning on the rank. If (V, Q) is a quadratic form over $\mathbb{Z}/n\mathbb{Z}$ then note that $\Omega(Q) \simeq \prod_{\text{prime } \ell | n} \Omega(Q|_{\mathbb{Z}/\ell^{a_\ell}\mathbb{Z}})$. Therefore, conditioned on each coset of Ω in $H^{d,i}_{\ell,k}$ the distributions $(\mathrm{RSel}^{\mathrm{kernel}}_{\ell^{a_\ell}})^d_{\mathbb{F}_q}$ are independent.

Since the TV distance of two product distributions is the sum of the TV distance of the factors, the TV distance between the BKLPR heuristic and $\limsup_{q\to\infty}(\mathrm{Rrk}, \mathrm{RSel}_n)^d_{\mathbb{F}_q}$ is

$$\ll \sum_{\text{prime } \ell | n} \ell^{-(6d-2)^2} \ll \zeta((6d-2)^2) - 1 \ll 2^{-(6d-2)^2}.$$

□

We can now complete the proof of Theorem 1.1.

Proof of Theorem 1.1 This follows immediately from combining Theorems 6.1 and 6.4. □

6.3 Remaining results

We conclude by proving two remaining results, promised in the introduction. First, we prove Corollary 6.5, which is a version of Corollary 1.5 with more precise error terms, and then we prove Corollary 6.6 which is a version of Corollary 1.6 with more precise error terms.

Corollary 6.5 *(Large q analog of [33, Conjecture 1.2]) For fixed integers $d \geq 2$ and $n \geq 1$, and q ranging over prime powers with* $\gcd(q, 2n) = 1$, *we have*

$$\mathrm{Prob}(\mathrm{rk}^d/\mathbb{F}_q(t) = r) = \begin{cases} 1/2 + O_d(q^{\frac{-1}{216d^2-162d+31}}) & \text{if } r \leq 1, \\ O_d(q^{\frac{-1}{216d^2-162d+31}}) & \text{if } r \geq 2. \end{cases} \qquad (6.7)$$

Furthermore,

$$\mathbb{E}[\mathrm{rk}^d/\mathbb{F}_q(t)] = 1/2 + O_d(q^{\frac{-1}{216d^2-162d+31}}).$$

Proof The first statement follows immediately from (6.2) by summing over the set of possible groups G which can appear. For the statement regarding average rank, we also need to know that there is a uniform bound on the rank of elliptic curves of height d over $\mathbb{F}_q(t)$, only depending on d. This holds because the rank is bounded by the size of the Selmer group, which is uniformly bounded in q among all elliptic curves of height d, as follows from [28, Corollary 3.27], since the Selmer space $\mathrm{Sel}'^{d}_{n,\mathbb{F}_q}$ is quasi-compact and quasi-finite over $\mathscr{W}'^{d}_{\mathbb{F}_q}$ and hence has uniformly bounded fiber degree. □

Theorem 6.6 *(Large q analog of [33, Conjecture 1.4]) Let n be a squarefree positive integer, $d \geq 2$, and $\omega(n)$ be the number of prime factors of n.*

(1) Fix $c_\ell \in \mathbb{Z}_{\geq 0}$ for each prime $\ell \mid n$. Then

$$\begin{aligned}
&\lim_{d\to\infty} \limsup_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \mathrm{Prob}\left(\mathrm{Sel}_n^d / \mathbb{F}_q(t) \simeq \prod_{\ell \mid n} (\mathbb{Z}/\ell\mathbb{Z})^{c_\ell}\right) \\
&= \lim_{d\to\infty} \liminf_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \mathrm{Prob}\left(\mathrm{Sel}_n^d / \mathbb{F}_q(t) \simeq \prod_{\ell \mid n} (\mathbb{Z}/\ell\mathbb{Z})^{c_\ell}\right) \qquad (6.8) \\
&= \begin{cases} 2^{\omega(n)-1} \prod_{\ell \mid n} \left(\left(\prod_{j\geq 0} \left(1-\ell^{-j}\right)^{-1}\right)\left(\prod_{j=1}^{c_\ell} \frac{\ell}{\ell^j-1}\right)\right) & \textit{if all } c_\ell \textit{ have the same parity,} \\ 0 & \textit{otherwise.} \end{cases}
\end{aligned}$$

(2) For q ranging over prime powers with $\gcd(q, 2n) = 1$*, we have*

$$\mathbb{E}[\#\,\mathrm{Sel}_n^d / \mathbb{F}_q(t)] = \sigma(n) + O_{n,d}(q^{-1/2}) := \sum_{s \mid n} s + O_{n,d}(q^{-1/2}).$$

(3) For $m \leq 6d-3$ the mth moment of $\mathrm{Sel}_n^d / \mathbb{F}_q(t)$ *is*

$$\mathbb{E}[(\#\,\mathrm{Sel}_n^d / \mathbb{F}_q(t))^m] = \prod_{\textit{prime } \ell \mid n} \prod_{i=1}^{m} \left(\ell^i + 1\right) + O_{n,d,m}(q^{-1/2}).$$

Proof The first part follows from Theorem 1.1 once we establish that $\mathrm{Sel}_n^{\mathrm{BKLPR}}$ has distribution as predicted in the bottom line of (6.8). To see this, note that, by definition, the model $\mathrm{Sel}_n^{\mathrm{BKLPR}}$ is determined by the models for $\mathrm{Sel}_\ell^{\mathrm{BKLPR}}$ with $\ell \mid n$ which are independent, except for the constraint that the parities of their $\mathbb{Z}/\ell\mathbb{Z}$ ranks are all equal. Hence, it suffices to establish the first part in the case $n = \ell$ is prime. Note that the model $\mathrm{Sel}_\ell^{\mathrm{BKLPR}}$ agrees with the model for ℓ-Selmer groups defined in [33, Definition 2.9] by [33, Theorem 2.19(f)]. Therefore, in the case $n = \ell$ is prime, $\mathrm{Sel}_\ell^{\mathrm{BKLPR}}$ has distribution as predicted in the bottom line of (6.8) by [33, Proposition 2.6(d) and (f)].

Note that (2) is the special case of (3) with $m = 1$, so it suffices to prove (3). To simplify notation in the ensuing proof, we use $\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}$ to denote $\underbrace{\mathrm{Sel}^{\circ d}_{n,\mathbb{F}_q} \times_{\mathscr{W}^{\circ d}_{\mathbb{F}_q}} \cdots \times_{\mathscr{W}^{\circ d}_{\mathbb{F}_q}} \mathrm{Sel}^{\circ d}_{n,\mathbb{F}_q}}_{m \text{ times}}$ and $\mathrm{Sel}'^{d,m}_{n,\mathbb{F}_q}$ to denote

$\underbrace{\mathrm{Sel}'^{d}_{n,\mathbb{F}_q} \times_{\mathscr{W}'^{d}_{\mathbb{F}_q}} \cdots \times_{\mathscr{W}'^{d}_{\mathbb{F}_q}} \mathrm{Sel}'^{d}_{n,\mathbb{F}_q}}_{m \text{ times}}$ To establish parts (2) and (3), we claim it is equivalent to show $\lim_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \frac{\#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}(\mathbb{F}_q)}{\#\mathscr{W}^{\circ d}_{\mathbb{F}_q}(\mathbb{F}_q)}$ has values as given by the right hand sides of (2) and (3). To show this is the case, it is enough to show that both $\#\mathscr{W}^{\circ d}_{\mathbb{F}_q}(\mathbb{F}_q)$ is within a factor of $1 + O_{n,d,m}(q^{-1/2})$ of the total number of height d elliptic curves and $\#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}(\mathbb{F}_q)$ is within a factor of $1 + O_{n,d,m}(q^{-1/2})$ of the sum of $\#\,\mathrm{Sel}_n(E)^m$ over all height d elliptic curves. First, $\#\mathscr{W}^{\circ d}_{\mathbb{F}_q}(\mathbb{F}_q)$ certainly furnishes a lower bound for the size of the set of all elliptic curves of height d, while $\mathscr{W}'^{d}_{\mathbb{F}_q}(\mathbb{F}_q)$ furnishes an upper bound (it is only an upper bound because it includes non-minimal smooth elliptic curves). Next, using Lemma 2.3 to compare $\#\,\mathrm{Sel}_n(E)$ to $\#H^1(\mathbb{P}^1, \mathscr{E}^0[n])$, for E with smooth Weierstrass model, we find that $\#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}(\mathbb{F}_q)$ indeed furnishes a lower bound for the sum of $\#\,\mathrm{Sel}_n(E)^m$ over all height d elliptic curves.

Finally, to reduce to computing $\lim_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \frac{\#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}(\mathbb{F}_q)}{\#\mathscr{W}^{\circ d}_{\mathbb{F}_q}(\mathbb{F}_q)}$ for (3), we wish to show that up to a factor of $1 + O_{n,d,m}(q^{-1/2})$, $\#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}(\mathbb{F}_q)$ also furnishes an upper bound for the sum of $\#\,\mathrm{Sel}_n(E)^m$ over all height d elliptic curves. Since $\mathrm{Sel}'^{d}_{n,\mathbb{F}_q} \to \mathscr{W}'^{d}_{\mathbb{F}_q}$ is étale and quasi-finite, and $\mathrm{Sel}^{\circ d}_{n,\mathbb{F}_q}$ constitutes a dense open in $\mathrm{Sel}'^{d}_{n,\mathbb{F}_q}$, it follows that $\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}$ constitutes a dense open in the maximal dimensional components of $\mathrm{Sel}'^{d,m}_{n,\mathbb{F}_q}$. Therefore, $\#\mathrm{Sel}'^{d,m}_{n,\mathbb{F}_q}(\mathbb{F}_q) - \#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}$ is bounded by $O_{n,d,m}(q^{-1/2})$, using the Lang-Weil estimates. The difference $\#\mathrm{Sel}'^{d,m}_{n,\mathbb{F}_q}(\mathbb{F}_q) - \#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}$ is not necessarily an upper bound for the sum of $\#\,\mathrm{Sel}_n(E)^m$. However, as shown in [28, Corollary 3.27], it is an upper bound for the sum over all height d elliptic curves of $\#(n^2 \cdot \mathrm{Sel}_n(E))^m$.

To conclude, it remains to determine $\lim_{\substack{q\to\infty \\ \gcd(q,2n)=1}} \frac{\#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}(\mathbb{F}_q)}{\#\mathscr{W}^{\circ d}_{\mathbb{F}_q}(\mathbb{F}_q)}$. Using the Lang-Weil estimates as in [28, Lemma 5.1], it is enough to compute the number of geometrically irreducible components of $\#\mathrm{Sel}^{\circ d,m}_{n,\mathbb{F}_q}$. Now, Part (3) follows from Burnside's lemma for the action of $\operatorname{im} \rho^d_{n,k}$ acting diagonally on $(V^d_n)^m$, which we claim has a total of $\prod_{\ell \mid n} \prod_{i=1}^m \left(\ell^i + 1\right)$ orbits. Note that $\Omega(Q^d_n) \subset \operatorname{im} \rho^d_{n,k} \subset O(Q^d_n)$, so it suffices to show both $\Omega(Q^d_n)$ and $O(Q^d_n)$ have $\prod_{\ell \mid n} \prod_{i=1}^m \left(\ell^i + 1\right)$ orbits on $(V^d_n)^m$. This follows from Theorem 4.9 and Lemma 4.5, together with the Chinese remainder theorem to bootstrap this latter result from primes to squarefree integers. □

Acknowledgements It is our pleasure to thank Ravi Vakil for organizing the "What's on My Mind" seminar, which led to the genesis of this paper. We thank Johan de Jong, Chao Li, Bjorn Poonen, Arul Shankar, Doug Ulmer, and Melanie Matchett Wood for helpful discussions. We thank Lisa Sauermann for help translating [24]. We also thank David Zureick-Brown and Jackson Morrow for help with writing and running MAGMA code. The first author was supported by a Stanford ARCS Fellowship and an NSF Postdoctoral Fellowship under Grant No. 1902927, and the second author was supported by the National Science Foundation Graduate Research Fellowship Program under Grant No. DGE-1656518.

Funding Open Access funding provided by the MIT Libraries

Data availibility Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest On behalf of all authors, Aaron Landesman states that there is no conflict of interest.

References

1. Manjul, B., Daniel, M.K., Hendrik, W.L., Jr., Bjorn, P., Eric, R.: Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. Camb. J. Math. **3**(3), 275–321 (2015)
2. Bosch, S., Lütkebohmert, W., Raynaud, M.: Néron Models. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). [Results in Mathematics and Related Areas (3)], vol. 21. Springer, Berlin (1990)
3. Bhargava, M., Shankar, A.: The average number of elements in the 4-selmer groups of elliptic curves is 7. arXiv:1312.7333v1 (arXiv preprint) (2013)
4. Bhargava, M., Shankar, A.: The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. arXiv:1312.7859v1 (arXiv preprint) (2013)
5. Bhargava, M., Shankar, A.: Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. Ann. Math. (2) **181**(1), 191–242 (2015)
6. Manjul, B., Arul, S.: Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. Ann. Math. (2) **181**(2), 587–621 (2015)
7. Conrad, B., Feng, T.: Algebraic groups II, notes, v3. *AMS Open Math Notes* (2017)
8. Chevalley, C.: The Algebraic Theory of Spinors and Clifford Algebras. Collected Works. Vol. 2, Edited and with a Foreword by Pierre Cartier and Catherine Chevalley, With a Postface by J.-P. Bourguignon. Springer, Berlin (1997)
9. Conrad, B.: Reductive group schemes. In: *Autour des Schémas en Groupes. Vol. I*, Volume 42/43 of *Panor. Synthèses*, pp. 93–444. Soc. Math. France, Paris (2014)
10. de Jong, A.J.: Counting elliptic surfaces over finite fields. Mosc. Math. J. **2**(2), 281–311 (2002). (Dedicated to Yuri I. Manin on the occasion of his 65th birthday)
11. de Jong, A.J., Robert, F.: On the geometry of principal homogeneous spaces. Am. J. Math. **133**(3), 753–796 (2011)
12. Ekedahl, T.: An effective version of Hilbert's irreducibility theorem. In: Séminaire de Théorie des Nombres. Paris 1988–1989, Volume 91 of Progress in Mathematics, pp. 241–249. Birkhäuser, Boston (1990)
13. Jordan, S.E., Akshay, V., Craig, W.: Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields. Ann. Math. (2) **183**(3), 729–786 (2016)
14. Freitag, E., Kiehl, R.: Étale Cohomology and the Weil Conjecture, Volume 13 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné. Springer, Berlin (1988)
15. Fulman, J., Stanton, D.: On the distribution of the number of fixed vectors for the finite classical groups. NN. Comb. **20**(4), 755–773 (2016)
16. Grothendieck, A.: Éléments de géométrie algébrique. Inst. Hautes Études Sci. Publ. Math. IV. Étude locale des schémas et des morphismes de schémas. III **28**, 255 (1966)
17. Grothendieck, A.: Revêtements étales et Groupe Fondamental (SGA 1). Lecture notes in mathematics, vol. 224. Springer, Berlin (1971)

18. Hall, C.: Big symplectic or orthogonal monodromy modulo l. Duke Math. J. **141**(1), 179–203 (2008)
19. Hô, Q.P., LêHùng, V.B.: BC Ngô,: Average size of 2-Selmer groups of elliptic curves over function fields. Math. Res. Lett. **21**(6), 1305–1339 (2014)
20. Huybrechts, D.: Lectures on K3 Surfaces. Cambridge Studies in Advanced Mathematics, vol. 158. Cambridge University Press, Cambridge (2016)
21. Illusie, L.: Théorie de Brauer et caractéristique d'Euler-Poincaré (d'après P. Deligne). In: The Euler-Poincaré characteristic (French). volume 82 of Astérisque, pp. 161–172. Soc. Math. France, Paris (1981)
22. Katz, N.M.: Twisted L-Functions and Monodromy. Annals of Mathematics Studies, vol. 150. Princeton University Press, Princeton (2002)
23. Katz, N.M.: Moments, Monodromy, and Perversity: A Diophantine Perspective. Annals of Mathematics Studies, vol. 159. Princeton University Press, Princeton (2005)
24. Kneser, M.: Erzeugung ganzzahliger orthogonaler gruppen durch spiegelungen. Math. Ann. **255**(4), 453–462 (1984)
25. Kowalski, E.: The large sieve, monodromy and zeta functions of curves. J. Reine Angew. Math. **601**, 29–69 (2006)
26. Kowalski, E.: On the rank of quadratic twists of elliptic curves over function fields. Int. J. Number Theory **2**(2), 267–288 (2006)
27. Katz, N.M., Sarnak, P.: Random Matrices, Frobenius Eigenvalues, and Monodromy. American Mathematical Society Colloquium Publications, vol. 45. American Mathematical Society, Providence (1999)
28. Landesman, A.: The geometric average size of Selmer groups over function fields. Algebra Number Theory **15**(3), 673–709 (2021)
29. Laumon, G.: Semi-continuité du Conducteur de Swan (d'après P. Deligne). In: The Euler-Poincaré Characteristic (French). Volume 83 of Astérisque, pp. 173–219. Mathematical Society of France, Paris (1981)
30. Levin, D.A., Peres, Y., Elizabeth, L.W.: Markov Chains and Mixing Times. American Mathematical Society, Providence: (With a chapter by James G. Propp and David B, Wilson) (2009)
31. Milnor, J., Husemoller, D.: Symmetric Bilinear Forms. Springer, New York (1973). (Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73 Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73)
32. Jennifer, P., Bjorn, P., John, V., Melanie, M.W.: A heuristic for boundedness of ranks of elliptic curves. J. Eur. Math. Soc. **21**(9), 2859–2903 (2019)
33. Poonen, B., Rains, E.: Random maximal isotropic subspaces and Selmer groups. J. Am. Math. Soc. **25**(1), 245–269 (2012)
34. Park, S.W., Wang, N.: Average size of Selmer group in large q limit. arXiv:2102.00549v2 (arXiv preprint) (2021)
35. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Inst. Hautes Études Sci. Publ. Math. **54**, 323–401 (1981)
36. Serre, J.-P.: Lectures on the Mordell-Weil Theorem. Aspects of Mathematics. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre, 3rd edn. Friedr. Vieweg & Sohn, Braunschweig (1997)
37. Silverman, J.H.: Advanced topics in the arithmetic of elliptic curves. 151:xiv+525 (1994)
38. Silverman, J.H.: The Arithmetic of Elliptic Curves, Volume 106 of Graduate Texts in Mathematics, 2nd edn. Springer, Dordrecht (2009)
39. Taylor, D.E.: The Geometry of the Classical Groups. Sigma Series in Pure Mathematics, vol. 9. Heldermann Verlag, Berlin (1992)
40. Ulmer, D.: Elliptic curves and analogies between number fields and function fields. In: Heegner Points and Rankin L-Series, Volume 49 of Math. Sci. Res. Inst. Publ., pp. 285–315. Cambridge University Press, Cambridge (2004)
41. Ulmer, D.: Geometric non-vanishing. Invent. Math. **159**(1), 133–186 (2005)
42. Verdier, J.-L: A duality theorem in the etale cohomology of schemes. In: Proceedings of Conference on Local Fields (Driebergen, 1966). Springer, Berlin, pp 184–198 (1967)
43. Wilson, R.A.: The Finite Simple Groups. Graduate Texts in Mathematics, vol. 251. Springer, London (2009)
44. Yun, Z., Zhang, W.: Shtukas and the Taylor expansion of L-functions (II). Ann. Math. (2) **189**(2), 393–526 (2019)
45. Zassenhaus, H.: On the spinor norm. Arch. Math. **13**, 434–451 (1962)

46. Zywina, D.: The inverse Galois problem for orthogonal groups. arXiv:1409.1151v1 (arXiv preprint) (2014)