Math. Res. Lett.
Volume 26, Number 4, 1217–1250, 2019

The distribution of Selmer ranks of quadratic twists of Jacobians of hyperelliptic curves

Myungjun Yu

Let C be an odd degree hyperelliptic curve over a number field K and J be its Jacobian. Let J^χ be the quadratic twist of J by a quadratic character $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$. For every non-negative integer r, we show the probability that $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^\chi/K)) = r$ for a certain family of quadratic twists can be given explicitly conditional on some heuristic hypothesis.

1. Introduction

Let E be an elliptic curve over a number field K. Let $\mathrm{Sel}_2(E/K)$ denote the 2-Selmer group of E over K. We write E^χ for the quadratic twist of E by a quadratic character $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$. Define

$$d_2(E/K) := \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E/K)) - \dim_{\mathbf{F}_2}(E(K)[2]),$$

where $E(K)[2]$ is the group of K-rational 2-torsion elements of E. Let $\mathrm{Prob}(\star)$ denote the probability of an event $\star$. Let E_1 denote the elliptic curve $y^2 = x^3 - x$. Heath-Brown [5] proved that

$$\mathrm{Prob}(d_2(E_1^\chi/\mathbf{Q})) = d) = \frac{f_d}{2} := \frac{1}{2}\prod_{j\geq 1}(1+2^{-j})^{-1}\prod_{j=1}^{d}\frac{2}{2^j-1}. \tag{1}$$

Swinnerton-Dyer [13] and Kane [6] generalized this by obtaining the same distribution for the family of quadratic twists of any E over $\mathbf{Q}$ with $E[2] \subset E(\mathbf{Q})$ with no rational cyclic 4-isogeny.

Remark 1.1. There are infinitely many quadratic characters. Therefore, in order for the notation $\mathrm{Prob}(d_2(E^\chi/\mathbf{Q})) = d)$ to make sense, we need to fix an ordering of quadratic characters χ. We may order χ by the conductor or by the discriminant. We could also order χ by the largest prime at which χ is ramified. In this case, if $\chi_1, \chi_2, \ldots, \chi_n$ have the same largest ramified prime, we order them arbitrarily. This ordering is first studied by Klagsbrun, Mazur and Rubin [7]. It seems to be believed that the distribution in (1) holds for an arbitrary elliptic curve E over $\mathbf{Q}$ with "any reasonable ordering" of quadratic characters.

Poonen and Rains [12] noticed that the 2-Selmer groups (in fact the p-Selmer groups) can be viewed as an intersection of two *maximal isotropic subspaces* (or *Lagrangian subspaces*) A and B in a (infinite dimensional) *metabolic space* and showed that the probability of two maximal isotropic subspaces having the intersection of dimension r is equal to $f_d/2$. In other words, if one believes that A and B appear randomly in the set of maximal isotropic subspaces, one will get the same distribution as in (1) for the family of all elliptic curves over a general number field K. In a similar fashion to this, Bhargava, Kane, Lenstra, Poonen, and Rains [3] found plausible models for Mordell-Weil groups, Selmer groups, and Shafarevich-Tate groups of elliptic curves in terms of random maximal isotropic subspaces.

When we restrict the family of all elliptic curves over K to the family of quadratic twists however, it requires a little bit more care. For an elliptic curve E over K, there could be a bias in the parity of Selmer ranks in the family of quadratic twists. For example, Dokchitser-Dokchitser [4] showed that $d_2(E^\chi/K)$ has a *constant parity* for any quadratic twists E^χ if and only if K has no real embedding and E acquires everywhere good reduction over an abelian extension of K. Klagsbrun, Mazur and Rubin [7] were able to quantify this bias and called it the *disparity*. Yu [14] generalized this to the case of Jacobians of odd degree hyperelliptic curves over K.

Theorem 1.2 (Klagsbrun-Mazur-Rubin, Yu). *Let C be an odd degree hyperelliptic curve and J be its Jacobian. Then we have*

$$\mathrm{Prob}\left(\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^\chi/K)) \text{ is even}\right) = \frac{1}{2} + \delta(J/K),$$

where $\delta(J/K)$ is defined in Definition 8.11.

Remark 1.3. In [7] and [14], the disparity constant is defined by $2\delta(J/K)$; we follow the definition in [8].

Remark 1.4. Theorem 1.2 has been recently generalized further to the case of principally polarised abelian varieties by Morgan [10].

It seems that 2-Selmer groups of Jacobians of (odd degree) hyperelliptic curves of fixed genus $g \geq 2$ behave (statistically) similarly to those of elliptic curves. For example, Bhargava and Gross [2] showed that when odd degree hyperelliptic curves of fixed genus $g \geq 1$ (elliptic curves if $g = 1$) over $\mathbf{Q}$ are ordered by *height*, the average size of the 2-Selmer groups of their Jacobians is 3. As a corollary, it follows that the average of the 2-Selmer ranks of Jacobians of odd degree hyperelliptic curves of genus g is bounded above by 3/2. For the Jacobians of odd degree hyperelliptic curves, there is a conjecture ([12, Conjecture 1.7]) that predicts the same distribution as in (1). For the Jacobians of even degree hyperelliptic curves, due to the presence of a nontrivial *torsor*, which contributes systematically on the 2-Selmer groups, we have a conjecture with different numbers. See [12, Conjecture 1.8] and [12, Example 4.20].

For the distribution of 2-Selmer ranks of elliptic curves in the family of quadratic twists, Klagsbrun-Mazur-Rubin showed the following [8]:

Theorem 1.5 (Klagsbrun-Mazur-Rubin). *Let E be elliptic curve over a number field K with*

$$\mathrm{Gal}(K(E[2])/K) \cong S_3$$

For every $m \geq 0$ and $X > 0$ let $m \mapsto \mathcal{B}_m(X) = \cup_k \mathcal{B}_{m,k,X}$ be the 'fan-structure' of collections of quadratic characters of K. Then for every $n \geq 0$,

$$\lim_{m\to\infty} \lim_{X\to\infty} \frac{|\{\chi \in \mathcal{B}_m(X) : \dim_{\mathbf{F}_2} \mathrm{Sel}_2(E^\chi/K) = n\}|}{|\mathcal{B}_m(X)|} = \begin{cases} (\frac{1}{2} + \delta(E/K))f_n & \text{if } n \text{ is even,} \\ (\frac{1}{2} - \delta(E/K))f_n & \text{if } n \text{ is odd,} \end{cases}$$

where $\delta(E/K)$ is given by Definition 8.11.

Remark 1.6. In the statement of [8, Theorem A], there is a misprint. The words "even" and "odd" should be switched as in the equality of Theorem 1.5.

They proved Theorem 1.5 by finding a certain *Markov model* for 2-Selmer ranks of elliptic curves in the family of quadratic twists and showing the density of 2-Selmer ranks is given by the equilibrium distribution.

The main goal of this paper is to give an evidence that the distribution of 2-Selmer ranks of Jacobians of (odd degree) hyperelliptic curves in the family of quadratic twists should be the same as that of elliptic curves in the family of quadratic twists. In fact, assuming an *"equidistribution"* condition (see Definition 5.8) on certain families of Lagrangian subspaces, we prove Theorem 1.5 holds for Jacobians of odd degree hyperelliptic curves. Namely, we prove

Theorem 1.7. *Let $C : y^2 = f(x)$ be an hyperelliptic curve of degree $2g+1$ over a number field K and let J be the Jacobian of C. Suppose that*

$$\mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}.$$

Suppose that C has UDRL (see Definition 5.8). For every $m \geq 0$ and $X > 0$ let $m \mapsto \mathcal{B}_m(X) = \cup_k \mathcal{B}_{m,k,X}$ be the 'fan-structure' of collections of quadratic

characters of K as in Definition 8.9. Then for every $n \geq 0$,

$$\lim_{m\to\infty}\lim_{X\to\infty}\frac{|\{\chi \in \mathcal{B}_m(X) : \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^\chi/K)) = n\}|}{|\mathcal{B}_m(X)|} = \begin{cases} (\frac{1}{2} + \delta(J/K))f_n & \text{if } n \text{ is even,} \\ (\frac{1}{2} - \delta(J/K))f_n & \text{if } n \text{ is odd,} \end{cases}$$

where $\delta(J/K)$ is given by Definition 8.11.

Since an elliptic curve satisfying $\mathrm{Gal}(K(E[2])/K) \cong S_3$ has UDRL (see Remark 5.11), this theorem can be regarded as a generalization of Theorem 1.5. As in [8] for elliptic curves, a direct application of Theorem 1.7 is

Corollary 1.8. *Suppose that all conditions of Theorem 1.7 hold. With notation as in Theorem 1.7, the average Mordell-Weil rank of the quadratic twists of J satisfies*

$$\lim_{m\to\infty}\lim_{X\to\infty}\frac{\sum_{\chi\in\mathcal{B}_m(X)}\mathrm{rk}(J^\chi(K))}{|\mathcal{B}_m(X)|} < 1.2646 + 0.1211\cdot\delta(J/K) < 1.3252,$$

where $\mathrm{rk}(J^\chi(K))$ denotes the Mordell-Weil rank of J^χ over K.

We rely heavily on the theory built in [8], so we keep notation consistent with [8] for the convenience of the reader.

2. Metabolic spaces and Lagrangian subspaces

For this section, fix a finite dimensional $\mathbf{F}_p$-vector space V.

Definition 2.1. A *quadratic form* on V is a function $Q : V \to \mathbf{F}_p$ such that

- $Q(av) = a^2Q(v)$ for every $a \in \mathbf{F}_p$ and $v \in V$,
- the map $(v, w)_Q := Q(v + w) - Q(v) - Q(w)$ is a bilinear form.

We say that X is a *Lagrangian subspace* or *maximal isotropic subspace* of V if $Q(X) = 0$ and $X = X^\perp$, where $X^\perp$ denotes the orthogonal complement of X in the bilinear form $(,)_Q$.

A *metabolic space* (V, Q) is a vector space such that $(,)_Q$ is nondegenerate and V contains a Lagrangian subspace. When Q is understood or not important, we just call V a metabolic space. Note that if X is a Lagrangian subspace of a metabolic space V, then $\dim_{\mathbf{F}_p}(V) = 2\dim_{\mathbf{F}_p}(X)$.

Lemma 2.2. *Suppose that (V, Q) is a metabolic space, and let X, Y, Z are Lagrangian subspaces of V. Then the following statements are true.*

(i) *Suppose that W is contained in a Lagrangian subspace of V. Then $W + W^{\perp} \cap X$ is a Lagrangian subspace of V. In particular, $(W + W^{\perp} \cap X)/W$ is a Lagrangian subspace of the metabolic space $W^{\perp}/W$ with the quadratic form induced by Q.*

(ii) $\dim_{\mathbf{F}_p}((X+Y)\cap Z) \equiv \dim_{\mathbf{F}_p}(X\cap Z + Y\cap Z) \pmod 2$,

(iii) $\dim_{\mathbf{F}_p}(X/(X\cap Y)) \equiv \dim_{\mathbf{F}_p}(Y/(Y\cap Z)) + \dim_{\mathbf{F}_p}(Z/(Z\cap X)) \pmod 2$.

Proof. (i) already appeared in [12, Remark 2.4(b)] and is not difficult to prove. See [7, Lemma 2.3] and [7, Corollary 2.5] for (ii) and (iii), respectively. □

Fix a finite dimensional $\mathbf{F}_p$-vector space T with a continuous action of G_K such that there exists a bilinear, alternating, nondegenerate and G_K-equivariant pairing

$$T \times T \to \mu_p,$$

where μ_p is the multiplicative group of p-th roots of unity. For every place v of K, the cup product induces a pairing

$$H^1(K_v, T) \times H^1(K_v, T) \xrightarrow{\cup} H^2(K_v, T \otimes T) \longrightarrow H^2(K_v, \boldsymbol{\mu}_p).$$

For every v, there is a canonical inclusion $H^2(K_v, \boldsymbol{\mu}_p) \hookrightarrow \mathbf{F}_p$ that is an isomorphism if v is nonarchimedean. The local Tate pairing is the composition

$$\langle\ ,\ \rangle_v : H^1(K_v, T) \times H^1(K_v, T) \longrightarrow \mathbf{F}_p. \tag{2}$$

Definition 2.3. Suppose v is a place of K. We say that Q is a *Tate quadratic form* on $H^1(K_v, T)$ if the bilinear form induced by Q (see Definition 2.1) is $\langle\ ,\ \rangle_v$ in (2).

For the rest of the paper, we fix a hyperelliptic curve $C : y^2 = f(x)$ with $\deg(f) = 2g + 1$ and $\mathrm{Gal}(f) \cong S_{2g+1}$. Let J be the Jacobian of C. Our main interest is when $T = J[2]$, the group of 2-torsion elements of J. In such a case, there is a canonical way to construct a Tate quadratic form q_v on $H^1(K_v, J[2])$ for every place v of K. This quadratic form q_v is induced by the *Heisenberg group* (see [14, Definition 5.5]).

We recall for every abelian variety A/K_v and $\psi \in \mathrm{Hom}(G_{K_v}, \{\pm 1\})$, there is a canonical isomorphism $A^\psi[2] \cong A[2]$ and the Kummer map

$$A(K_v)/2A(K_v) \hookrightarrow H^1(K_v, A[2]).$$

Lemma 2.4. *For every place v and $\psi \in \mathcal{C}(K_v)$, the space*

$$\mathrm{Im}(J^\psi(K_v)/2J^\psi(K_v) \to H^1(K_v, J^\psi[2]) \cong H^1(K_v, J[2]))$$

is a Lagrangian subspace of $(H^1(K_v, J[2]), q_v)$.

Proof. The lemma follows from [12, Proposition 4.11] and [14, Theorem 5.10]. □

3. Counting Lagrangian subspaces

In this section, we count the number of Lagrangian subspaces of a metabolic space under various conditions, which will turn out to be crucial in our heuristic model. For this section, we fix a metabolic space V of dimension $2n$ over $\mathbf{F}_p$.

Definition 3.1. Define

$$L_V := \{\text{Lagrangian subspaces of } V\}.$$

Definition 3.2. Let A and B be Lagrangian subspaces of V such that $\dim_{\mathbf{F}_p}(A \cap B) = i$. Let

$$b_{n,i}(j) := \#\{C \in L_V : \dim_{\mathbf{F}_p}(C \cap B) = 0 \text{ and } \dim_{\mathbf{F}_p}(C \cap A) = j\}.$$

Remark 3.3. By Definition 3.2, if $i + j > n$, then $b_{n,i}(j) = 0$.

Remark 3.4. Suppose Y is contained in a Lagrangian subspace of V. Then $Y^\perp/Y$ is a metabolic space (with quadratic form induced by that attached to V). Note that there is a map (Lemma 2.2(i))

$$\Phi_Y : L_V \longrightarrow L_{Y^\perp/Y}$$

by sending W to $(W \cap Y^\perp + Y)/Y$. The following lemma compute $b_{n,i}(j)$ by investigating the map Φ_Y.

Lemma 3.5. *We have*

(i) *If* $i \geq 1$, $b_{n,i}(j) = p^{n-1} b_{n-1,i-1}(j)$.

(ii) *If* $i \geq 1$, $b_{n,i}(j) = p^{ni - \frac{i(i+1)}{2}} b_{n-i,0}(j)$.

(iii) *If* $j \geq 1, b_{n,0}(j) = b_{n-j,0}(0) \prod_{k=1}^{j} \frac{p^{n-k+1}-1}{p^k-1} = b_{n-j,0}(0) \prod_{k=1}^{n-j} \frac{p^{n-k+1}-1}{p^k-1}$.

(iv) $\sum_{k=0}^{n} b_{n,0}(k) = p^{n(n-1)/2}$.

(v) *If* $n \not\equiv i + j \pmod 2$, *then* $b_{n,i}(j) = 0$.

(vi) $b_{2n,0}(0) = p^{(2n)(2n-1)/2} - \sum_{k=1}^{n} (b_{2n-2k,0}(0) \prod_{i=1}^{2k} \frac{p^{2n+1-i}-1}{p^{2k+1-i}-1})$.

(vii) $b_{2n,0}(0) = \prod_{k=1}^{n} (p^{2k-1} - 1) p^{2k-2}$.

Proof. Choose two Lagrangian subspaces A and B of V so that $\dim_{\mathbf{F}_p}(A \cap B) = i$. Suppose that

$$A \text{ has a basis } \{a_1, a_2, \cdots, a_i, a_{i+1}, \cdots, a_n\},$$
$$B \text{ has a basis } \{a_1, a_2, \cdots, a_i, a_{n+1}, \cdots, a_{2n-i}\}.$$

Let (a_1) denote the subspace generated by a_1. Consider the map (Remark 3.4)

$$\Phi_{(a_1)} : L_V \longrightarrow L_{(a_1)^\perp/(a_1)}.$$

Put $A' = A/(a_1)$ and $B' = B/(a_1)$. Note that $\dim_{\mathbf{F}_p}(A' \cap B') = i - 1$. If

$$D \in \{C \in L_V \mid \dim_{\mathbf{F}_p}(C \cap B) = 0 \text{ and } \dim_{\mathbf{F}_p}(C \cap A) = j\},$$

then $\Phi_{(a_1)}(D)$ is a Lagrangian subspace of $(a_1)^\perp/(a_1)$, $\dim_{\mathbf{F}_p}(\Phi_{(a_1)}(D) \cap B') = 0$, and $\dim_{\mathbf{F}_p}(\Phi_{(a_1)}(D) \cap A') = j$. Conversely, for $C' \in L_{(a_1)^\perp/(a_1)}$ such that

$$\dim_{\mathbf{F}_p}(C' \cap B') = 0 \quad \text{and} \quad \dim_{\mathbf{F}_p}(C' \cap A') = j,$$

there are $p^{n-1} + 1$ elements in the fiber of C' in the map

$$\Phi_{(a_1)} : L_V \longrightarrow L_{(a_1)^\perp/(a_1)}$$

by [12, Proposition 2.6(a)]. Every Lagrangian subspace F in the fiber satisfies $\dim_{\mathbf{F}_p}(F \cap B) = 0$ and $\dim_{\mathbf{F}_p}(F \cap A) = j$ except only one that contains a_1. In other words, there is a p^{n-1}-to-one correspondence between the following

two sets:

$$\{C \in L_V : \dim_{\mathbf{F}_p}(C \cap B) = 0 \text{ and } \dim_{\mathbf{F}_p}(C \cap A) = j\}, \text{ and}$$
$$\{C' \in L_{(a_1)^\perp/(a_1)} : \dim_{\mathbf{F}_p}(C' \cap B') = 0 \text{ and } \dim_{\mathbf{F}_p}(C' \cap A') = j\}.$$

Therefore, (i) follows. (ii) follows easily from (i).

Now we show (iii). We suppose A and B are Lagrangian subspaces of V such that $A \cap B = \{0\}$. Note that

$$\left|\{M \subseteq \mathbf{F}_p^n : \dim_{\mathbf{F}_p}(M) = j\}\right| = \prod_{k=1}^{j} \frac{p^{n-k+1}-1}{p^k-1}.$$

Fix a dimension j subspace D of A. Put $A'' = A/D$ and $B'' = (B \cap D^\perp + D)/D$. The map

$$\Phi_D : L_V \longrightarrow L_{D^\perp/D}$$

takes a Lagrangian subspace C (of V) such that $C \cap B = \{0\}$ and $C \cap A = D$ to a Lagrangian subspace $\Phi_D(C)$ of $D^\perp/D$ such that $\Phi_D(C) \cap B'' = \{0\}$ and $\Phi_D(C) \cap A'' = \{0\}$. Conversely, it is easy to see that a Lagrangian space W of $D^\perp/D$ such that $W \cap A'' = \{0\}$ and $W \cap B'' = \{0\}$ has a unique element C_W in the fiber of W satisfying $C_W \cap B = \{0\}$ and $C_W \cap A = D$. In other words, there is an one-to-one correspondence between the following two sets:

$$\{C \in L_V : C \cap A = D \text{ and } C \cap B = \{0\}\}, \text{ and}$$
$$\{C'' \in L_{D^\perp/D} : C'' \cap A'' = \{0\} \text{ and } C'' \cap B'' = \{0\}\}.$$

Therefore (iii) follows. To see (iv), combine Proposition 2.6 (b) and (e) in [12]. (v) follows from Lemma 2.2(ii). We obtain (vi) by combining (iii), (iv), and (v). Finally Lemma 3.8 implies (vii). □

To prove Lemma 3.8, we recall some equalities from *q-binomial coefficients*.

Definition 3.6. Define $(a)_n := (a;q)_n := (1-a)(1-aq)\cdots(1-aq^{n-1})$,

$$\begin{bmatrix} n \\ m \end{bmatrix} := \begin{cases} (q)_n (q)_m^{-1} (q)_{n-m}^{-1} & \text{if } 0 \leqq m \leqq n \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 3.7. *We have*

(i)
$$\sum_{j=0}^{m} (-1)^j \begin{bmatrix} m \\ j \end{bmatrix} = \begin{cases} (q;q^2)_n & \text{if } m = 2n \\ 0 & \text{if } m \text{ is odd.} \end{cases}$$

(ii) $\begin{bmatrix} 2n-j \\ k \end{bmatrix}\begin{bmatrix} 2n \\ j \end{bmatrix} = \begin{bmatrix} j+k \\ j \end{bmatrix}\begin{bmatrix} 2n \\ j+k \end{bmatrix}$.

(iii) $(1)_N = 0$ *if* $N > 0$ *and* $(1)_0 = 1$.

(iv) $(z)_N = \sum_{j=0}^{N} \begin{bmatrix} N \\ j \end{bmatrix}(-1)^j z^j q^{j(j-1)/2}$.

Proof. (ii) and (iii) are easy to prove by the definition. (i) follows from [1, Theorem 2.3.4] and (iv) follows from [1, Theorem 2.3.3]. □

Lemma 3.8. *Let* $d_0 = 0$. *Then* $d_{2n} = \prod_{k=1}^{n}(p^{2k-1}-1)p^{2k-2}$ *for all* $n \geq 1$ *if and only if*

$$d_{2n} = p^{2n(2n-1)/2} - \sum_{k=1}^{n}\left(d_{2n-2k}\prod_{i=1}^{2k}\frac{p^{2n+1-i}-1}{p^{2k+1-i}-1}\right) \text{ for all } n \geq 1.$$

Proof. This proof was suggested by Dennis Eichhorn. In the proof, we take $q = 1/p$. Assuming $d_{2n} = \prod_{k=1}^{n}(p^{2k-1}-1)p^{2k-2}$, we show that

$$d_{2n} = p^{\frac{2n(2n-1)}{2}} - \sum_{k=1}^{n} d_{2n-2k}\frac{(p^{2n}-1)(p^{2n-1}-1)\cdots(p^{2n-2k+1}-1)}{(p^{2k}-1)(p^{2k-1}-1)\cdots(p^1-1)},$$

and the converse follows by induction. If we put $e_{2n} = d_{2n}/p^{2n(2n-1)/2}$, it is equivalent to proving

$$e_{2n} = 1 - \sum_{k=1}^{n} e_{2n-2k}\begin{bmatrix} 2n \\ 2k \end{bmatrix}(1/p)^{2k(2k-1)/2}.$$

Note that $e_{2k} = (1/p; 1/p^2)_k$. Letting $e_{2k-1} = 0$, it is equivalent to proving

$$1 = \sum_{j=0}^{2n} e_{2n-j}\begin{bmatrix} 2n \\ j \end{bmatrix}(1/p)^{j(j-1)/2} = \sum_{j=0}^{2n}\sum_{k=0}^{2n-j}(-1)^k\begin{bmatrix} 2n-j \\ k \end{bmatrix}\begin{bmatrix} 2n \\ j \end{bmatrix}(1/p)^{j(j-1)/2}$$
$$= \sum_{j=0}^{2n}\sum_{k=0}^{2n-j}(-1)^k\begin{bmatrix} j+k \\ j \end{bmatrix}\begin{bmatrix} 2n \\ j+k \end{bmatrix}(1/p)^{j(j-1)/2}.$$

Let the last summation be $[D]$. The second equality comes from (i) of Lemma 3.7. The third equlity follows from (ii) of Lemma 3.7. Putting

$m = j + k$, we re-index the double sum so that

$$[D] = \sum_{m=0}^{2n} (-1)^m \begin{bmatrix} 2n \\ m \end{bmatrix} \sum_{j=0}^{m} (-1)^j \begin{bmatrix} m \\ j \end{bmatrix} (1/p)^{j(j-1)/2}.$$

Thus, by (iii) and (iv) of Lemma 3.7, the inner sum of $[D]$ vanishes unless $m = 0$, in which case the inner sum $= 1$. Therefore $[D] = 1$. □

4. Local conditions induced by local characters and Selmer groups

Let $C : y^2 = f(x)$ be a hyperelliptic curve over a number field K of degree $2g + 1$ and let J be its Jacobian. We write ∞ for the point at infinity of the affine model $y^2 = f(x)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_{2g+1}$ be the roots of $f(x)$. Then the 2-torsion group $J[2]$ has a basis $\{(\alpha_1, 0) - \infty, (\alpha_2, 0) - \infty, \ldots, (\alpha_{2g}, 0) - \infty\}$, and $(\alpha_{2g+1}, 0) - \infty = \sum_{i=1}^{2g}((\alpha_i, 0) - \infty)$ in J. The action of $\mathrm{Gal}(\overline{K}/K)$ on the roots of f induces that on $J[2]$. Then we can identify $\mathrm{Gal}(K(J[2])/K)$ with $\mathrm{Gal}(f)$.

We fix a finite set Σ of places of K containing all primes where J has bad reduction, all primes above 2, and all archimedean places. For the rest of the paper, we assume that $\mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}$, where S_{2g+1} denotes the symmetric group with $2g + 1$ letters. By Hilbert's irreducibility theorem, most hyperelliptic curves of degree $2g + 1$ satisfy this assumption.

Definition 4.1. Let L be either a local field or a global field. Define

$$\mathcal{C}(L) := \mathrm{Hom}(G_L, \{\pm 1\}),$$

where G_L denotes the absolute Galois group of L. If L is a local field, we often identify $\mathcal{C}(L)$ with $\mathrm{Hom}(L^\times, \{\pm 1\})$ via the local reciprocity map. We let $\mathcal{C}_{\mathrm{ram}}(L)$ denote the set of ramified quadratic characters.

Definition 4.2. Let $\mathfrak{q}$ denote a prime of K. We write $\mathbf{N}(\mathfrak{q})$ for the *norm* of $\mathfrak{q}$. Define

$$\begin{aligned} \mathcal{P}_n &:= \{\mathfrak{q} : \mathfrak{q} \notin \Sigma \text{ and } \dim_{\mathbf{F}_2}(J(K_\mathfrak{q})[2]) = n\} \quad \text{for } 0 \le n \le 2g, \\ \mathcal{P} &:= \mathcal{P}_0 \coprod \mathcal{P}_1 \coprod \mathcal{P}_2 \coprod \cdots \coprod \mathcal{P}_{2g} = \{\mathfrak{q} : \mathfrak{q} \notin \Sigma\}, \\ \mathcal{P}_n(X) &:= \{\mathfrak{q} : \mathfrak{q} \in \mathcal{P}_n \text{ and } \mathbf{N}(\mathfrak{q}) < X\}. \end{aligned}$$

Define the *width* function $w : \mathcal{P} \to \{0, 1, 2, \cdots, 2g\}$ by $w(\mathfrak{q}) := n$ if $\mathfrak{q} \in \mathcal{P}_n$.

Remark 4.3. In the definition of $\mathcal{P}_n$, the condition $\dim_{\mathbf{F}_2}(J(K_\mathfrak{q})[2]) = n$ is equivalent to $\dim_{\mathbf{F}_2}(J(K_\mathfrak{q})/2J(K_\mathfrak{q})) = n$ by [14, Lemma 2.11(i)].

Let v be a place of K. Recall that we attach a canonical Tate quadratic form q_v to $H^1(K_v, J[2])$. See the paragraph after Definition 2.3.

Definition 4.4. Let v be a place of K. Let K_v^{ur} denote the maximal unramified extension of K_v. Define

$$\mathcal{H}(q_v) := \{\text{Lagrangian subspaces of } (H^1(K_v, J[2]), q_v)\},$$

and if $v \notin \Sigma$, let

$$H^1_{\mathrm{ur}}(K_v, J[2]) := \ker(H^1(K_v, J[2]) \to H^1(K_v^{\mathrm{ur}}, J[2])),$$

and

$$\mathcal{H}_{\mathrm{ram}}(q_v) := \{X \in \mathcal{H}(q_v) : X \cap H^1_{\mathrm{ur}}(K_v, J[2]) = \{0\}\}.$$

Definition 4.5. For every place v of K, define

$$\alpha_v : \mathcal{C}(K_v) \longrightarrow \mathcal{H}(q_v)$$

sending $\psi \in \mathcal{C}(K_v)$ to

$$\mathrm{Im}(J^\psi(K_v)/2J^\psi(K_v) \to H^1(K_v, J^\psi[2]) \cong H^1(K_v, J[2])),$$

where the last isomorphism is induced by the canonical isomorphism $J^\psi[2] \cong J[2]$. The map α_v is well-defined by Lemma 2.4.

Lemma 4.6. *Suppose J has good reduction at v and $\psi \in \mathcal{C}(K_v)$. If $\psi \in \mathcal{C}(K_v)$ is unramified, then $\alpha_v(\psi) = H^1_{\mathrm{ur}}(K_v, J[2])$. If $\psi \in \mathcal{C}_{\mathrm{ram}}(K_v)$, then $\alpha_v(\psi) \in \mathcal{H}_{\mathrm{ram}}(q_v)$.*

Proof. It is well known that if J has good reduction at v, then we have $\alpha_v(1_v) = H^1_{\mathrm{ur}}(K_v, J[2])$. The first assertion follows from [14, Lemma 2.15]. The second assertion follows from [14, Lemma 2.16]. □

Remark 4.7. If $v \in \mathcal{P}_1$, then $|\mathcal{H}_{\mathrm{ram}}(q_v)| = 1$ by Lemma 3.5(iv). Therefore if $v \in \mathcal{P}_1$, the map α_v sends every element in $\mathcal{C}_{\mathrm{ram}}(K_v)$ to the single element in $\mathcal{H}_{\mathrm{ram}}(q_v)$. If C is an elliptic curve and $v \in \mathcal{P}_2$, then the map α_v gives a bijection $\mathcal{C}_{\mathrm{ram}}(K_v) \to \mathcal{H}_{\mathrm{ram}}(q_v)$ by [7, Proposition 5.8].

Definition 4.8. Let

$$\mathcal{D} := \{\text{squarefree products of primes } \mathfrak{q} \in \mathcal{P}_1 \cup \mathcal{P}_2 \cup \cdots \cup \mathcal{P}_{2g}\},$$

and if $\mathfrak{d} \in \mathcal{D}$ let $\mathfrak{d}_i$ be the product of all primes dividing $\mathfrak{d}$ that lie in $\mathcal{P}_i$, so $\mathfrak{d} = \mathfrak{d}_1\mathfrak{d}_2\cdots\mathfrak{d}_{2g}$. For every $\mathfrak{d} \in \mathcal{D}$, define

- $w(\mathfrak{d}) := \sum_{\mathfrak{q}|\mathfrak{d}} w(\mathfrak{q}) = \sum_{n=1}^{2g} n|\{\mathfrak{q} : \mathfrak{q} \mid \mathfrak{d}_n\}|$, the *width* of $\mathfrak{d}$,
- $\Sigma(\mathfrak{d}) := \Sigma \cup \{\mathfrak{q} : \mathfrak{q} \mid \mathfrak{d}\} \subset \Sigma \cup \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_{2g}$,
- $\Omega_{\mathfrak{d}} := \prod_{v\in\Sigma} \mathcal{C}(K_v) \times \prod_{\mathfrak{q}|\mathfrak{d}} \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$,
- $\Omega_{\mathfrak{d}}^S := S \times \prod_{\mathfrak{q}|\mathfrak{d}} \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$ for every subset $S \subset \Omega_1 = \prod_{v\in\Sigma} \mathcal{C}(K_v)$,
- $\eta_{\mathfrak{d},\mathfrak{q}} : \Omega_{\mathfrak{d}\mathfrak{q}}^S \to \Omega_{\mathfrak{d}}^S$ the projection map, if $\mathfrak{d}\mathfrak{q} \in \mathcal{D}$.

Definition 4.9. For every $\mathfrak{d} \in \mathcal{D}$ and $\omega = (\omega_v)_v \in \Omega_{\mathfrak{d}}$, we define the *Selmer group* $\mathrm{Sel}_2(J,\omega)$ as follows. Let α_v is as in Definition 4.5. Define

$$\mathrm{Sel}_2(J,\omega) := \{x \in H^1(K, J[2]) : \mathrm{res}_v(x) \in \alpha_v(\omega_v) \text{ if } v \in \Sigma(\mathfrak{d}), \text{ and } \mathrm{res}_v(x) \in H^1_{\mathrm{ur}}(K_v, J[2]) \text{ otherwise}\},$$

where $\mathrm{res}_v : H^1(K, J[2]) \to H^1(K_v, J[2])$ is the restriction map. We also define

$$\mathrm{rk}(\omega) := \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J,\omega)).$$

Definition 4.10. Define

$$\mathrm{Sel}_2(J,\omega)^{(\mathfrak{q})} := \ker\left(H^1(K, J[2]) \xrightarrow{\oplus \mathrm{res}_v} \bigoplus_{v\neq\mathfrak{q}} H^1(K_v, J[2])/\alpha_v(\omega_v)\right),$$
$$\mathrm{Sel}_2(J,\omega)_{(\mathfrak{q})} := \ker\left(\mathrm{Sel}_2(J,\omega) \xrightarrow{\mathrm{res}_{\mathfrak{q}}} H^1(K_{\mathfrak{q}}, J[2])\right).$$

Lemma 4.11. *Let $\mathfrak{q} \in \mathcal{P}_n$. Then we have*

$$\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J,\omega)^{(\mathfrak{q})}) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J,\omega)_{(\mathfrak{q})}) = n.$$

Proof. The assertion follows from the *Poitou-Tate duality*. For example, see [9, Theorem 2.3.4]. □

It follows from Lemma 4.11 that if $\omega' \in \eta_{\mathfrak{d},\mathfrak{q}}^{-1}(\omega)$ for $\mathfrak{q} \in \mathcal{P}_n$ and $\omega \in \Omega_{\mathfrak{d}}$, then $|\mathrm{rk}(\omega) - \mathrm{rk}(\omega')| \leq n$. If we let $\eta_1 : \Omega_{\mathfrak{d}} \to \Omega_1$ be the projection, we have

$$\mathrm{rk}(\omega) \leq \mathrm{rk}(\eta_1(\omega)) + w(\mathfrak{d})$$

by induction. Therefore we have

Proposition 4.12. *Let $\mathfrak{d} \in \mathcal{D}$ and $\omega \in \Omega_{\mathfrak{d}}$. Then*

$$\mathrm{rk}(\omega) \leq w(\mathfrak{d}) + \max\{\mathrm{rk}(\bar{\omega}) : \bar{\omega} \in \Omega_1\}.$$

5. The heuristic assumption

We continue to assume that $\mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}$. The goal of this section is to explain our heuristic assumption stated in Definition 5.8.

Definition 5.1. Fix $\mathfrak{d} \in \mathcal{D}$ and $\omega \in \Omega_{\mathfrak{d}}$. For every prime $\mathfrak{q} \notin \Sigma(\mathfrak{d})$, define

- $V_{\mathfrak{q}}(\omega) := \mathrm{Im}(\mathrm{Sel}_2(J,\omega)^{(\mathfrak{q})} \longrightarrow H^1(K_{\mathfrak{q}}, J[2]))$,
- $V_{\mathfrak{q},\mathrm{ur}} := H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, J[2])$,
- $\mathcal{P}_{n,i} := \{\mathfrak{q} \in \mathcal{P}_n : \dim_{\mathbf{F}_2}(V_{\mathfrak{q}}(\omega) \cap V_{\mathfrak{q},\mathrm{ur}}) = i\}$,
- $\mathcal{P}_{n,i}(X) := \mathcal{P}_{n,i} \cap \mathcal{P}_n(X)$.

Then it follows that $V_{\mathfrak{q},\mathrm{ur}}$ and $V_{\mathfrak{q}}(\omega)$ are Lagrangian subspaces of the metabolic space $H^1(K_{\mathfrak{q}}, J[2])$ from Definition 4.5, Lemma 4.6 and the following lemma.

Lemma 5.2. *For every prime $\mathfrak{q}$ and $\omega \in \Omega_{\mathfrak{d}}$, the space $V_{\mathfrak{q}}(\omega)$ is a Lagrangian subspace of $H^1(K_{\mathfrak{q}}, J[2])$.*

Proof. Let $x \in \mathrm{Sel}_2(J,\omega)^{(\mathfrak{q})}$. Recall that for every place v, q_v is a Tate quadratic form on $H^1(K_v, J[2])$. We have $q_v(x) = 0$ for $v \neq \mathfrak{q}$ by Lemma 2.4 and the definition of Lagrangian spaces. Together with this fact, [14, Lemma 5.8] implies $\mathrm{res}_{\mathfrak{q}}(x) = 0$. Lemma 4.11 shows $V_{\mathfrak{q}}(\omega)$ is of dimension $\dim_{\mathbf{F}_2}(H^1(K_{\mathfrak{q}}, J[2]))/2$, so the lemma follows from Definition 2.1. □

Remark 5.3. Let V be a metabolic space of dimension $2n$ over $\mathbf{F}_2$. Let A and B be Lagrangian subspaces of V (so $\dim_{\mathbf{F}_2}(A) = \dim_{\mathbf{F}_2}(B) = n$) such that $\dim(A \cap B) = i$. Now suppose a Lagrangian subspace X is randomly

chosen in the set

$$\{X \in L_V : X \cap B = \{0\}\}.$$

Then the probability that $\dim_{\mathbf{F}_2}(X \cap A) = j$ is given by

$$d_{n,i}(j) := \frac{b_{n,i}(j)}{\sum_{m=0}^{n-i} b_{n,i}(m)},$$

where the integers $b_{n,i}(j)$ are defined by taking $p = 2$ in Definition 3.2. Here we explain our heuristic model. Suppose $\omega \in \Omega_{\mathfrak{d}}$ is fixed. If $\mathfrak{q} \in \mathcal{P}_{n,i}$, we have $\dim_{\mathbf{F}_2}(V_{\mathfrak{q}}(\omega) \cap V_{\mathfrak{q},\mathrm{ur}}) = i$. For $\psi \in \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$, we have $\alpha_{\mathfrak{q}}(\psi) \cap V_{\mathfrak{q},\mathrm{ur}} = \{0\}$ by Lemma 4.6. Now suppose that $\mathfrak{q} \in \mathcal{P}_{n,i}$ and $\psi \in \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$ are chosen at random. Our heuristic model for $\alpha_{\mathfrak{q}}(\psi)$, since there is no other systematic restriction on $\alpha_{\mathfrak{q}}(\psi)$, is then a random Lagrangian subspace in the set

$$\{X \in L_{H^1(K_{\mathfrak{q}},J[2])} : X \cap V_{\mathfrak{q},\mathrm{ur}} = \{0\}\}.$$

An easy consequence of this is that

$$\mathrm{Prob}(\dim_{\mathbf{F}_2}(\alpha_{\mathfrak{q}}(\psi) \cap V_{\mathfrak{q}}(\omega)) = j) = d_{n,i}(j).$$

Although this is just a heuristic assumption, we give a name for C satisfying this assumption (Definition 5.8) to ease the statement of our results. We also remark here that the randomness of Lagrangian subspaces was used to model Selmer groups in [12] and [3].

Remark 5.4. Let $\omega \in \Omega_{\mathfrak{d}}$ and $\mathfrak{q} \nmid \mathfrak{d}$. Let $\mathfrak{q} \in \mathcal{P}_{n,i}$. For $\omega' \in \eta_{\mathfrak{d},\mathfrak{q}}^{-1}(\omega)$, noting that $\dim_{\mathbf{F}_2}(V_{\mathfrak{q}}(\omega) \cap V_{\mathfrak{q},\mathrm{ur}}) = i$ since $\mathfrak{q} \in \mathcal{P}_{n,i}$, we have by Lemma 5.5(i) that

$$\mathrm{rk}(\omega') = \mathrm{rk}(\omega) + \dim_{\mathbf{F}_2}(\alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}}) \cap V_{\mathfrak{q}}(\omega)) - i, \tag{3}$$

where $\omega'_{\mathfrak{q}} \in \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$ is the $\mathfrak{q}$-component of ω'. Therefore, knowing the distribution of $\dim_{\mathbf{F}_2}(\alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}}) \cap V_{\mathfrak{q}}(\omega))$ is equivalent to knowing that of $\mathrm{rk}(\omega')$.

Lemma 5.5. *Let $\omega \in \Omega_{\mathfrak{d}}$ and $\mathfrak{q} \nmid \mathfrak{d}$. Let $\mathfrak{q} \in \mathcal{P}_n$ and $\omega' \in \eta_{\mathfrak{d},\mathfrak{q}}^{-1}(\omega)$. Then*

(i) $\mathrm{rk}(\omega') = \mathrm{rk}(\omega) + \dim_{\mathbf{F}_2}(\alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}}) \cap V_{\mathfrak{q}}(\omega)) - \dim_{\mathbf{F}_2}(V_{\mathfrak{q}}(\omega) \cap V_{\mathfrak{q},\mathrm{ur}})$,

(ii) *if n is odd,* $\mathrm{rk}(\omega') \not\equiv \mathrm{rk}(\omega) \pmod 2$.

Proof. Note that the following restriction (at $\mathfrak{q}$) maps are surjective by definition.

$$\mathrm{Sel}_2(J,\omega) \longrightarrow V_{\mathfrak{q}}(\omega) \cap V_{\mathfrak{q},\mathrm{ur}},$$
$$\mathrm{Sel}_2(J,\omega') \longrightarrow V_{\mathfrak{q}}(\omega) \cap \alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}}).$$

Both maps have the same kernel $\mathrm{Sel}_2(J,\omega)_{(\mathfrak{q})}$. Therefore (i) follows from comparing the dimensions over $\mathbf{F}_2$. For (ii), recall that $V_{\mathfrak{q}}(\omega), V_{\mathfrak{q},\mathrm{ur}}$ and $\alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}})$ are Lagrangian subspaces of $H^1(K_{\mathfrak{q}}, J[2])$ by Definition 4.5, Lemma 4.6 and Lemma 5.2. It follows from (i) and Lemma 2.2(iii) that

$$\mathrm{rk}(\omega') - \mathrm{rk}(\omega) \equiv n - \dim_{\mathbf{F}_2}(V_{\mathfrak{q},\mathrm{ur}} \cap \alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}})) \pmod 2.$$

Now (ii) follows from Lemma 4.6. □

We record here some properties of $d_{n,i}(j)$, which will be used in the proof of Theorem 6.9.

Lemma 5.6. *We have*

(i) *If* $n \not\equiv i+j \pmod 2$, *then* $d_{n,i}(j) = 0$.

(ii) $d_{n,i}(j) = d_{n-i,0}(j)$.

(iii) $d_{k+i,0}(k-i) = \dfrac{c_{2i}\prod_{h=1}^{2i}\frac{2^{k+i-h+1}-1}{2^h-1}}{2^{(k+i)(k+i-1)/2}}$, *where* $c_{2i} = b_{2i,0}(0)$ *for* $p=2$.

(iv)
$$d_{k+i-1,0}(k-i-1) = \frac{c_{2i}\prod_{h=1}^{2i}\frac{2^{k+i-h}-1}{2^h-1}}{2^{(k+i-1)(k+i-2)/2}} = d_{k+i,0}(k-i)\frac{(2^{k-i}-1)2^{k+i-1}}{2^{k+i}-1}.$$

(v) $d_{k+i+1,0}(k-i-1) = d_{k+i,0}(k-i)\dfrac{(2^{k+i+1}-1)(2^{k-i}-1)}{2^{k-i}(2^{2i+2}-1)}$.

Proof. (i) follows from Lemma 3.5(v). (ii) follows from Lemma 3.5(ii). Lemma 3.5(iii) and Lemma 3.5(iv) imply (iii) and the first equality of (iv), so the second equality of (iv) follows. (v) is a consequence of (iii) and Lemma 3.5(vii). □

Definition 5.7. We fix $\omega = (\omega_v)_v \in \Omega_{\mathfrak{d}}$. For every $\mathfrak{q} \notin \Sigma(\mathfrak{d})$, let

$$t(\mathfrak{q}) := \dim_{\mathbf{F}_2}\left(\mathrm{Im}\left(\mathrm{Sel}_2(J,\omega) \xrightarrow{\mathrm{res}_{\mathfrak{q}}} H^1_{\mathrm{ur}}(K_q, J[2])\right)\right).$$

In particular, $\mathfrak{q} \in \mathcal{P}_{n,i}$ if and only if $\mathfrak{q} \in \mathcal{P}_n$ and $t(\mathfrak{q}) = i$.

Definition 5.8. We say that a hyperelliptic curve C has *UDRL*[1] if there exists a function $\tilde{\mathcal{L}} : [1,\infty) \to [1,\infty)$ such that if $X > \tilde{\mathcal{L}}(Y)$, then

$$\left| \frac{\displaystyle\sum_{\mathfrak{q}\in\mathcal{P}_n(X),\mathfrak{q}\nmid\mathfrak{d},t(\mathfrak{q})=i} |\,\{\psi\in\mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}}) \mid \dim_{\mathbf{F}_2}(\alpha_{\mathfrak{q}}(\psi)\cap V_{\mathfrak{q}}(\omega))=j\}\,|}{\displaystyle\sum_{\mathfrak{q}\in\mathcal{P}_n,\mathfrak{q}\nmid\mathfrak{d},t(\mathfrak{q})=i} |\,\mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})\,|} - d_{n,i}(j) \right| < \frac{1}{9gY}$$

for each $\omega\in\Omega_{\mathfrak{d}}$, $0\le n\le 2g$ and $0\le j\le n-i$.

Remark 5.9. When $j<0$ or $j>n-i$, the inequality in Definition 5.8 is clearly true since both terms between the absolute value bars become zero.

Remark 5.10. The constant $\frac{1}{9g}$ in Definition 5.8 is not very crucial, which could have been chosen to be any other constant less than $\frac{1}{9g}$ (see the proof of Theorem 6.9 and Lemma 6.8).

Remark 5.11. One can check that elliptic curves E with $\mathrm{Gal}(K(E[2])/K) \cong S_3$ have UDRL. This follows from Remark 4.7, Lemma 5.2, and Lemma 5.6(i). However, in the hyperelliptic curve of $g\ge 2$ case, if $v\in\mathcal{P}_n$ for $n\ge 3$, it follows from Lemma 3.5(iv) that there are $2^{n(n-1)/2}$ (>2) Lagrangian subspaces in $\mathcal{H}_{\mathrm{ram}}(q_v)$, whereas $\mathcal{C}_{\mathrm{ram}}(K_v)$ has only two elements. Because of this, it seems not easy to check whether or not C has UDRL.

We nevertheless expect the following statement is true.

Conjecture 5.12. *Let C be a hyperellipitc curve over a number field K of genus $g\ge 2$. Suppose that* $\mathrm{Gal}(K(J[2])/K)\cong S_{2g+1}$. *Then C has UDRL.*

6. Selmer ranks controlled by primes in $\mathcal{P}_1$

The main goal of this section is to prove Theorem 6.9. Roughly speaking, Theorem 6.9 means the 2-Selmer ranks in the family of local quadratic twists are controlled by the primes in $\mathcal{P}_1$ (see Remark 6.10). We start this section by recalling the *effective version of Chebotarev density theorem.*

Theorem 6.1. *There is a nondecreasing function $\overline{\mathcal{L}} : [1,\infty)\to[1,\infty)$ such that for*

[1]UDRL stands for uniformly distributed ramified Lagrangians.

- *every* $Y \geq 1$,
- *every* $\mathfrak{d} \in \mathcal{D}$ *with* $\mathbf{N}(\mathfrak{d}) < Y$,
- *every Galois extension* F *of* K *that is abelian of exponent* 2 *over* $K(J[2])$, *and unramified outside* $\Sigma(\mathfrak{d})$,
- *every pair of subsets* $S, S' \subset \mathrm{Gal}(F/K)$ *stable under conjugation, with* S *nonempty, and*
- *every* $X > \overline{\mathcal{L}}(Y)$,

we have

$$\left| \frac{|\{\mathfrak{q} \notin \Sigma(\mathfrak{d}) : \mathbf{N}(\mathfrak{q}) \leq X, \mathrm{Frob}_{\mathfrak{q}}(F/K) \in S'\}|}{|\{\mathfrak{q} \notin \Sigma(\mathfrak{d}) : \mathbf{N}(\mathfrak{q}) \leq X, \mathrm{Frob}_{\mathfrak{q}}(F/K) \in S\}|} - \frac{|S'|}{|S|} \right| \leq \frac{1}{9gY}.$$

In particular, $\{\mathfrak{q} \notin \Sigma(\mathfrak{d}) : \mathbf{N}(\mathfrak{q}) \leq X, \mathrm{Frob}_{\mathfrak{q}}(F/K) \in S\}$ *is nonempty.*

Proof. Let $\varphi : [1, \infty) \to [1, \infty)$ be the function sending Y to $9gY$. Let $\mathcal{L}$ be as in [8, Theorem 8.1]. Letting $\overline{\mathcal{L}}$ be the composition of $\mathcal{L}$ and φ, the theorem follows from [8, Theorem 8.1]. □

Definition 6.2. Supppse that $\mathfrak{d} \in \mathcal{D}$ and $\omega \in \Omega_{\mathfrak{d}}$. Let $\mathrm{Res}_{K(J[2])}$ denote the restriction map

$$H^1(K, J[2]) \to \mathrm{Hom}(G_{K(J[2])}, J[2])^{\mathrm{Gal}(K(J[2])/K)}.$$

Let $F_{\mathfrak{d},\omega}$ be the fixed field of $\cap_{c \in \mathrm{Sel}_2(J,\omega)} \ker(\mathrm{Res}_{K(J[2])}(c))$. Then $F_{\mathfrak{d},\omega}$ is a Galois extension over K.

The following proposition is proved for elliptic curves E with

$$\mathrm{Gal}(K(E[2])/K) \cong S_3$$

in [8, Proposition 9.3]. Recall that we assume $\mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}$.

Proposition 6.3. *For every* $\mathfrak{d} \in \mathcal{D}$ *and* $\omega \in \Omega_{\mathfrak{d}}$, *we have*

(i) *there is a* $\mathrm{Gal}(K(J[2])/K)$*-module isomorphism* $\mathrm{Gal}(F_{\mathfrak{d},\omega}/K(J[2])) \cong J[2]^{\mathrm{rk}(\omega)}$.

(ii) *the map*

$$\mathrm{Res}_{K(J[2])} : \mathrm{Sel}_2(J,\omega) \to \mathrm{Hom}(G_{K(J[2])}, J[2])$$

induces isomorphisms

$$\mathrm{Sel}_2(J,\omega) \cong \mathrm{Hom}(\mathrm{Gal}(F_{\mathfrak{d},\omega}/K(J[2])), J[2])^{\mathrm{Gal}(K(J[2])/K)},$$
$$\mathrm{Gal}(F_{\mathfrak{d},\omega}/K(J[2])) \cong \mathrm{Hom}(\mathrm{Sel}_2(J,\omega), J[2]).$$

(iii) $F_{\mathfrak{d},\omega}/K$ *is unramified outside* $\Sigma(\mathfrak{d})$.

Proof. Note that the following statements are true:

(1) $J[2]$ is a simple $\mathrm{Gal}(K(J[2])/K)$-module.

(2) $\dim_{\mathbf{F}_2}(\mathrm{Hom}_{\mathrm{Gal}(K(J[2])/K)}(J[2], J[2])) = 1$.

(3) $H^1(\mathrm{Gal}(K(J[2])/K), J[2]) = 0$.

(1) and (2) are easy to check and left to the reader. For (3), see [14, Lemma 3.2]. Now the proposition follows exactly as in the proof of [8, Proposition 9.3]. □

Proposition 6.4. *Fix* $\mathfrak{d} \in \mathcal{D}$ *and* $\omega \in \Omega_{\mathfrak{d}}$. *Let* $\mathrm{rk}(\omega) = r$ *and define*

$$E_{n,i,r} := (2^{-r})^{n-i} \prod_{h=0}^{i-1} (1 - 2^{-r+h}) \prod_{m=1}^{n-i} \frac{2^{i+m}-1}{2^m - 1}.$$

If $\overline{\mathcal{L}}$ *is a function as in Theorem 6.1, then for every* $Y > \mathbf{N}(\mathfrak{d})$ *and every* $X > \overline{\mathcal{L}}(Y)$, *we have*

$$\left| \frac{|\{\mathfrak{q} \in \mathcal{P}_n(X) : \mathfrak{q} \nmid \mathfrak{d}, t(\mathfrak{q}) = i\}|}{|\{\mathfrak{q} \in \mathcal{P}_n(X) : \mathfrak{q} \nmid \mathfrak{d}\}|} - E_{n,i,r} \right| < \frac{1}{9gY}.$$

Proof. Let loc_τ denote the evaluation map at $\tau \in \mathrm{Gal}(\overline{K}/K)$:

$$\mathrm{loc}_\tau : \mathrm{Sel}_2(J,\omega) \subset H^1(K, J[2]) \to J[2]/(\tau - 1)J[2].$$

Define

$$S := \{\tau \in \mathrm{Gal}(F_{\mathfrak{d},\omega}/K) \mid \dim_{\mathbf{F}_2}(J[2]/(\tau-1)J[2]) = n\},$$
$$S' := \{\tau \in S \mid \dim_{\mathbf{F}_2}(\mathrm{Im}(\mathrm{loc}_\tau : \mathrm{Sel}_2(J,\omega) \longrightarrow J[2]/(\tau-1)J[2]) = i\},$$
$$S'' := \{\sigma \in \mathrm{Gal}(K(J[2])/K) \mid \dim_{\mathbf{F}_2}(J[2]/(\sigma-1)J[2]) = n\}.$$

By Theorem 6.1, it is enough to show that

$$\frac{|S'|}{|S|} = E_{n,i,r}.$$

Clearly $|S| = |\mathrm{Gal}(F_{\mathfrak{d},\omega}/K(J[2]))||S''| = 2^{2gr}|S''|$ by Proposition 6.3(i). For $\tau \in \mathrm{Gal}(F_{\mathfrak{d},\omega}/K)$, if $\xi \in \mathrm{Gal}(F_{\mathfrak{d},\omega}/K(J[2]))$, then

$$J[2]/(\tau - 1)J[2] = J[2]/(\tau\xi - 1)J[2].$$

We define

$$\begin{aligned}\lambda_\tau &: \mathrm{Sel}_2(J,\omega) \longrightarrow J[2]/(\tau-1)J[2],\\ \lambda_{\tau\xi} &: \mathrm{Sel}_2(J,\omega) \longrightarrow J[2]/(\tau\xi-1)J[2] = J[2]/(\tau-1)J[2],\end{aligned}$$

given by evaluations at τ and $\tau\xi$, respectively. For $c \in \mathrm{Sel}_2(J,\omega)$, we have

$$\lambda_{\tau\xi}(c) = c(\tau\xi) = c(\tau) + \tau c(\xi) = \lambda_\tau(c) + c(\xi).$$

By Proposition 6.3(ii), We also have

$$\begin{aligned}\mathrm{Gal}(F_{\mathfrak{d},\omega}/K(J[2])) &\cong \mathrm{Hom}(\mathrm{Sel}_2(J,\omega), J[2])\\ &\twoheadrightarrow \mathrm{Hom}(\mathrm{Sel}_2(J,\omega), J[2]/(\tau-1)J[2]).\\ \xi &\mapsto (c \mapsto c(\xi))\end{aligned}$$

Therefore, for any $\tau|_{K(J[2])} \in S''$, there are

$$2^{(2g-n)r}|\{\phi \in \mathrm{Hom}_{\mathbf{F}_2}(\mathbf{F}_2^r \longrightarrow \mathbf{F}_2^n)|\dim_{\mathbf{F}_2}(\mathrm{Im}(\phi)) = i\}|$$

embeddings $\xi \in \mathrm{Gal}(F_{\mathfrak{d},\omega}/K(J[2]))$ such that $\dim_{\mathbf{F}_2}(\mathrm{Im}(\lambda_{\tau\xi})) = i$. Therefore

$$|S'| = 2^{(2g-n)r}|S''||\{\phi \in \mathrm{Hom}_{\mathbf{F}_2}(\mathbf{F}_2^r \longrightarrow \mathbf{F}_2^n)|\dim_{\mathbf{F}_2}(\mathrm{Im}(\phi)) = i\}|.$$

It is easy to prove that

$$|\{\phi \in \mathrm{Hom}_{\mathbf{F}_2}(\mathbf{F}_2^r \longrightarrow \mathbf{F}_2^n)|\dim_{\mathbf{F}_2}(\mathrm{Im}(\phi)) = i\}| = \prod_{h=0}^{i-1}(2^r - 2^h)\prod_{m=1}^{n-i}\frac{2^{i+m}-1}{2^m-1},$$

which completes the proof. □

Remark 6.5. Let $\mathrm{rk}(\omega) = r$ and $\omega \in \Omega_{\mathfrak{d}}$. Suppose that $\mathfrak{q} \in \mathcal{P}_1$, $\mathfrak{q} \nmid \mathfrak{d}$, and $\omega' \in \eta_{\mathfrak{d},q}^{-1}(\omega)$. Let $\mathrm{rk}(\omega') = s$. Recall that

(i) $b_{1,0}(0) + b_{1,0}(1) = 1$,

(ii) $\alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}}) \cap V_{\mathfrak{q},\mathrm{ur}} = \{0\}$,

(iii) $\dim_{\mathbf{F}_2}(\alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}}) \cap V_{\mathfrak{q}}(\omega)) \not\equiv \dim_{\mathbf{F}_2}(V_{\mathfrak{q}}(\omega) \cap V_{\mathfrak{q},\mathrm{ur}}) \pmod 2$,

which follow from Lemmas 3.5(iv),4.6, and 3.5(v), respectively. Then by (3) in Remark 5.4 one can check that

$$s = \begin{cases} r-1 & \text{if } t(\mathfrak{q}) = 1, \\ r+1 & \text{if } t(\mathfrak{q}) = 0. \end{cases}$$

In virtue of Proposition 6.4, this means (as $\mathfrak{q}$ is chosen randomly in $\mathcal{P}_1$)

$$\mathrm{Prob}(s = r-1) = 1 - 2^{-r} \quad \text{and} \quad \mathrm{Prob}(s = r+1) = 2^{-r}.$$

Definition 6.6. For $r, s \geq 0$, we define a matrix $M_L = [m_{r,s}]$ by

$$m_{r,s} = \begin{cases} 1 - 2^{-r} & \text{if } s = r-1, \\ 2^{-r} & \text{if } s = r+1, \\ 0 & \text{otherwise.} \end{cases}$$

Define $m_{r,s}^{(n)} \geq 0$ so that $M_L^n = [m_{r,s}^{(n)}]$. In other words, $m_{r,s}^{(n)}$ is the entry of M_L^n at its r-th row and j-th column.

Definition 6.7. Suppose C has UDRL. Define the function $\mathcal{L}$ from $[1, \infty)$ to itself

$$\mathcal{L}(Y) := \max(\overline{\mathcal{L}}(Y), \tilde{\mathcal{L}}(Y)).$$

Lemma 6.8. *For $0 \leq n \leq 2g$, $0 \leq e \leq n$, and $0 < \epsilon < 1$, let $0 \leq a_e$, b_e, c_e, $d_e \leq 1$ be such that $|a_e - c_e| < \epsilon$ and $|b_e - d_e| < \epsilon$. Then $\sum_{k=0}^{n} |a_e b_e - c_e d_e| < 9\epsilon g$.*

Proof. It is easy to prove and left to the reader. □

Theorem 6.9. *Fix $\omega \in \Omega_{\mathfrak{d}}$. If C has UDRL and $\mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}$, then for $X > \mathcal{L}(Y)$ with $Y > N(\mathfrak{d})$, we have*

$$\left| \frac{\sum_{\mathfrak{q} \in \mathcal{P}_n(X), \mathfrak{q} \nmid \mathfrak{d}} \mid \{\omega' \in \eta_{\mathfrak{d},\mathfrak{q}}^{-1}(\omega) : \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J, \omega') = s)\} \mid}{\sum_{\mathfrak{q} \in \mathcal{P}_n(X), \mathfrak{q} \nmid \mathfrak{d}} \mid \eta_{\mathfrak{d},\mathfrak{q}}^{-1}(\omega) \mid} - m_{\mathrm{rk}(\omega),s}^{(n)} \right| < \frac{1}{Y}.$$

Proof. Recall from Lemma 5.5(i) that for $\omega' \in \eta_{\mathfrak{d},\mathfrak{q}}^{-1}(\omega)$, we have

$$\mathrm{rk}(\omega') = \mathrm{rk}(\omega) + \dim_{\mathbf{F}_2}(V_{\mathfrak{q}}(\omega) \cap \alpha_{\mathfrak{q}}(\omega'_{\mathfrak{q}})) - \dim_{\mathbf{F}_2}(V_{\mathfrak{q}}(\omega) \cap V_{\mathfrak{q},\mathrm{ur}}).$$

Let $e = \dim_{\mathbf{F}_2}(V_{\mathfrak{q}}(\omega) \cap V_{\mathfrak{q},\mathrm{ur}})$, $r = \mathrm{rk}(\omega)$, and $s = \mathrm{rk}(\omega')$. Then we have

$$\begin{aligned} 0 \le\ & e \le n, \\ 0 \le\ & s + e - r \le n, \\ 0 \le\ & s + 2e - r \le n. \end{aligned}$$

Define

$$\begin{aligned} a_e &= \frac{\mid \{\mathfrak{q} \in \mathcal{P}_n(X) : \mathfrak{q} \nmid \mathfrak{d}, t(\mathfrak{q}) = e\} \mid}{\mid \{\mathfrak{q} \in \mathcal{P}_n(X) : \mathfrak{q} \nmid \mathfrak{d}\} \mid}, \\ b_e &= \frac{\displaystyle\sum_{\mathfrak{q} \in \mathcal{P}_n(X), \mathfrak{q} \nmid \mathfrak{d}, t(\mathfrak{q}) = e} \mid \{\psi \in \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}}) \mid \dim_{\mathbf{F}_2}(\alpha_{\mathfrak{q}}(\psi) \cap V_{\mathfrak{q}}(\omega)) = s + e - r\} \mid}{\displaystyle\sum_{\mathfrak{q} \in \mathcal{P}_n, \mathfrak{q} \nmid \mathfrak{d}, t(\mathfrak{q}) = e} \mid \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}}) \mid}, \\ c_e &= E_{n,e,r}, \\ d_e &= d_{n,e}(s + e - r). \end{aligned}$$

Then by (3) we have

$$\sum_{e=0}^{n} a_e b_e = \frac{\sum_{\mathfrak{q} \in \mathcal{P}_n(X), \mathfrak{q} \nmid \mathfrak{d}} \mid \{\omega' \in \eta_{\mathfrak{d},\mathfrak{q}}^{-1}(\omega) : \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J, \omega') = s)\} \mid}{\sum_{\mathfrak{q} \in \mathcal{P}_n(X), \mathfrak{q} \nmid \mathfrak{d}} \mid \eta_{\mathfrak{d},\mathfrak{q}}^{-1}(\omega) \mid}.$$

It follows from Proposition 6.4 that $|a_e - c_e| < \frac{1}{9gY}$. Since C has UDRL, we have $|b_e - d_e| < \frac{1}{9gY}$, that is Definition 5.8. Therefore, by Lemma 6.8, we only need to show that

$$F_{n,r}(s) := \sum_{e=0}^{n} d_{n,e}(s + e - r) E_{n,e,r} = m_{r,s}^{(n)}. \tag{4}$$

If $r + s + n$ is odd then $m_{r,s}^{(n)} = 0$, and $F_{n,r}(s)$ is also equal to zero by Lemma 5.6(ii). Moreover, if $|r - s| > n$, both $m_{r,s}^{(n)} = 0$, and $F_{n,r}(s) = 0$. Hence it remains to show (4) when $n + r + s$ is even and $|r - s| \le n$. We will show (4) by induction on n. When $n = 1$, it is clear (see Remark 6.5). For $0 \le k \le n$, it follows from Lemma 5.6(ii) (and the fact that $E_{n,n-k-i,r} = 0$

if $n-k-i<0$) that

$$F_{n,r}(r-n+2k)=\sum_{i=0}^{k} d_{k+i,0}(k-i)E_{n,n-k-i,r}.$$

We want to show that

$$m^{(n)}_{r,r-n+2k}=\sum_{i=0}^{k} d_{k+i,0}(k-i)E_{n,n-k-i,r}.$$

By induction hypothesis for $n-1$, we have

$$\begin{aligned} m^{(n)}_{r,r-n+2k} &= (1-2^{-r})m^{(n-1)}_{r-1,(r-1)-(n-1)+2k} + 2^{-r}m^{(n-1)}_{r+1,(r+1)-(n-1)+2(k-1)} \\ &= (1-2^{-r})\sum_{i=0}^{k} d_{k+i,0}(k-i)E_{n-1,n-k-i-1,r-1} \\ &\quad + 2^{-r}\sum_{i=1}^{k} d_{k+i-2,0}(k-i)E_{n-1,n-k-i+1,r+1}. \end{aligned}$$

Let

- $S_1=\sum_{i=0}^{k} d_{k+i,0}(k-i)E_{n,n-k-i,r}$,
- $S_2=(1-2^{-r})\sum_{i=0}^{k} d_{k+i,0}(k-i)E_{n-1,n-k-i-1,r-1}$,
- $S_3=2^{-r}\sum_{i=1}^{k} d_{k+i-2,0}(k-i)E_{n-1,n-k-i+1,r+1}$.

We want to show that $S_1=S_2+S_3$. We have

$$\begin{aligned} S_1-S_2 &= \sum_{i=0}^{k} d_{k+i,0}(k-i)\left(E_{n,n-k-i,r}-(1-2^{-r})E_{n-1,n-k-i-1,r-1}\right) \\ &= \sum_{i=0}^{k} d_{k+i,0}(k-i)(2^{-r})^{k+i}\prod_{h=0}^{n-k-i-1}(1-2^{-r+h})\prod_{m=1}^{k+i-1}\frac{2^{n-k-i+m}-1}{2^m-1}, \\ S_3 &= 2^{-r}\sum_{i=1}^{k} d_{k+i-2,0}(k-i)E_{n-1,n-k-i+1,r+1} \\ &= \sum_{i=1}^{k} 2^{-r}d_{k+i-2,0}(k-i)(2^{-r-1})^{k+i-2} \\ &\quad \times \prod_{h=0}^{n-k-i}(1-2^{-r-1+h})\prod_{m=1}^{k+i-2}\frac{2^{n-k-i+1+m}-1}{2^m-1}. \end{aligned}$$

Let

- $d_{k+i,0}(k-i)U_i :=$ i-th summand of $S_1 - S_2$,
- $V_i :=$ i-th summand of S_3,
- $g_i := d_{k+i,0}(k-i)\frac{2^{k-i}-1}{2^{k+i}-1}$, and
- $h_i := d_{k+i,0}(k-i) - g_i = d_{k+i,0}(k-i)\frac{2^{k+i}-2^{k-i}}{2^{k+i}-1}$.

Now it is enough to show that

$$g_i U_i + h_{i+1}U_{i+1} = V_{i+1}. \tag{5}$$

One can show $h_{i+1} = d_{k+i,0}(k-i)\frac{2^{k-i}-1}{2}$ by Lemma 5.6(v). Using this and Lemma 5.6(iv) for V_{i+1}, it is straightforward to check (5) and left to the reader. □

Remark 6.10. Let $\mathfrak{d} \in \mathcal{D}$ and $\omega \in \Omega_{\mathfrak{d}}$. Let $S = \mathrm{Sel}_2(J,\omega)$ for convenience. By Remark 6.5, $m^{(1)}_{\mathrm{rk}(\omega),s} = m_{\mathrm{rk}(\omega),s}$ (an entry of M_L in Definition 6.6) denotes the probability that s is the Selmer rank of a "local twist" of S by a ramified character at a random prime in $\mathcal{P}_1$. Therefore $m^{(n)}_{\mathrm{rk}(\omega),s}$ means the probability that s is the Selmer rank of a "local twist" of S by n ramified characters at randomly chosen n primes in $\mathcal{P}_1$. In the statement of Theorem 6.9, the fraction

$$\frac{\sum_{\mathfrak{q}\in\mathcal{P}_n(X),\mathfrak{q}\nmid\mathfrak{d}} \mid \{\omega' \in \eta^{-1}_{\mathfrak{d},\mathfrak{q}}(\omega) : \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J,\omega') = s)\} \mid}{\sum_{\mathfrak{q}\in\mathcal{P}_n(X),\mathfrak{q}\nmid\mathfrak{d}} \mid \eta^{-1}_{\mathfrak{d},\mathfrak{q}}(\omega) \mid}$$

(as $X \to \infty$) is the probability that s is the Selmer rank of a "local twist" of S by a ramified character at a random prime in $\mathcal{P}_n$. Hence Theorem 6.9 can be phrased as "the Selmer ranks of local quadratic twists are (statistically) controlled by the twisting data at primes in $\mathcal{P}_1$."

7. Local and global twists

Many results in this section and the next section are already done in the elliptic curve case in Section 10 and Section 11 of [8]. We will explain how their results can be applied to the hyperelliptic curve case as well when it is necessary. We continue to assume $\mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}$. For the rest of

this paper we assume that the set Σ satisfies (enlarge Σ if necessary)

$$\mathrm{Pic}(O_{K,\Sigma}) = 0, \tag{6}$$

where $\mathcal{O}_{K,\Sigma}$ is the ring of Σ-integers of K. By [14, Lemma 4.9], we have

$$\mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^2 \longrightarrow \prod_{v\in\mathcal{P}_0} K_v^{\times}/(K_v^{\times})^2 \quad \text{is injective.} \tag{7}$$

Recall that C is given by an affine model $y^2 = f(x)$ of degree $2g+1$. Let

$$\Delta := \Delta_f := \text{the discriminant of } f.$$

Lemma 7.1. *Define the subgroup $\mathcal{A} \subset K^{\times}/(K^{\times})^2$ by*

$$\mathcal{A} := \ker(K^{\times}/(K^{\times})^2 \to K(J[2])^{\times}/(K(J[2])^{\times})^2).$$

Then $\mathcal{A} \cong \mathbf{Z}/2\mathbf{Z}$, generated by $\Delta \in \mathcal{O}_{K,\Sigma}^{\times}$.

Proof. If $b \in \mathcal{A}$, then there exists $x \in K(J[2])^{\times}$ such that $x^2 = b$. Note that $K(\sqrt{\Delta})$ is the only nontrivial quadratic subextension of $K(J[2])$ over K since S_{2g+1} has only one normal subgroup of index 2, so the lemma follows. □

Lemma 7.2. *Let $\mathfrak{q} \in \mathcal{P}_n$.*

(i) *If n is even and $\chi \in \mathcal{C}(K_{\mathfrak{q}})$, then $\chi(\Delta) = 1$.*

(ii) *If n is odd and $\chi \in \mathcal{C}(K_{\mathfrak{q}})$, then $\chi(\Delta) = 1$ if and only if χ is unramified.*

Proof. This is [14, Lemma 6.1]. □

Definition 7.3. If $\chi \in \mathcal{C}(K)$ and v is a place of K, we let $\chi_v \in \mathcal{C}(K_v)$ denote the restriction of χ to G_{K_v}. For $\mathfrak{d} \in \mathcal{D}$, define

$$\mathcal{C}(\mathfrak{d}) := \{\chi \in \mathcal{C}(K) : \chi \text{ is ramified at all } \mathfrak{q} \text{ dividing } \mathfrak{d} \text{ and unramified outside } \Sigma(\mathfrak{d}) \cup \mathcal{P}_0\}.$$

For $X > 0$ define

- $\mathcal{C}(X) = \{\chi \in \mathcal{C}(K) : \chi \text{ is unramified outside } \Sigma \cup \{\mathfrak{q} : \mathbf{N}(\mathfrak{q}) < X\}\}$,
- $\mathcal{C}(\mathfrak{d}, X) := \mathcal{C}(\mathfrak{d}) \cap \mathcal{C}(X)$.

Let $\eta_{\mathfrak{d}} : \mathcal{C}(\mathfrak{d}) \to \Omega_{\mathfrak{d}}$ be the natural map $\chi \to (\ldots, \chi_v, \ldots)_{v\in\Sigma(\mathfrak{d})}$, where $\chi_v \in \mathcal{C}(K_v)$ is the restriction of χ to G_{K_v}.

Recall the definition of $\overline{\mathcal{L}}$ in Theorem 6.1.

Lemma 7.4. *Suppose* $\mathfrak{d} \in \mathcal{D}$, $\alpha \in \mathcal{O}_{K,\Sigma(\mathfrak{d})}^{\times}/(\mathcal{O}_{K,\Sigma(\mathfrak{d})}^{\times})^2$, *and* $\alpha \neq 1$. *If* $\alpha \neq \Delta$, *then there exists a prime* $\mathfrak{q} \in \mathcal{P}_0$ *with* $\mathbf{N}(\mathfrak{q}) \leq \overline{\mathcal{L}}(\mathbf{N}(\mathfrak{d}))$ *such that* $\alpha \notin (\mathcal{O}_{\mathfrak{q}}^{\times})^2$.

Proof. Note that

$$K(\sqrt{\alpha}) \cap K(J[2]) = K.$$

Choose $\tau \in \mathrm{Gal}(K(J[2], \sqrt{\alpha})/K)$ such that

$$\tau|_{K(J[2])} \in \mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}$$

is a single orbit of length $2g+1$, and $\tau|_{K(\sqrt{\alpha})} \neq 1$. By Theorem 6.1 applied with $F = K(J[2], \sqrt{\alpha})$ and S equal to the conjugacy class of τ, we see that there exists $\mathfrak{q} \notin \Sigma(\mathfrak{d})$ with $\mathbf{N}(\mathfrak{q}) \leq \overline{\mathcal{L}}(\mathbf{N}(\mathfrak{d}))$ whose Frobenius in $\mathrm{Gal}(K(J[2], \sqrt{\alpha})/K)$ is in the conjugacy class of τ. We have $\alpha \notin (\mathcal{O}_{\mathfrak{q}}^{\times})^2$ and it follows from [14, Lemma 2.12] that $\mathfrak{q} \in \mathcal{P}_0$. □

Definition 7.5. Define $\mathrm{sign}_{\Delta} : \Omega_1 \to \{\pm 1\}$ by

$$\mathrm{sign}_{\Delta}(\ldots, \omega_v, \ldots) := \prod_{v \in \Sigma} \omega_v(\Delta).$$

Define

$$S^+ := \{\omega \in \Omega_1 : \mathrm{sign}_{\Delta}(\omega) = 1\}, \quad S^- := \{\omega \in \Omega_1 : \mathrm{sign}_{\Delta}(\omega) = -1\}.$$

We will often write $\Omega_{\mathfrak{d}}^1 := \Omega_{\mathfrak{d}}^+ := \Omega_{\mathfrak{d}}^{S^+}$ and $\Omega_{\mathfrak{d}}^{-1} := \Omega_{\mathfrak{d}}^- := \Omega_{\mathfrak{d}}^{S^-}$.

Proposition 7.6. *Suppose that* $\mathfrak{d} \in \mathcal{D}$ *and* $X > \overline{\mathcal{L}}(\mathbf{N}(\mathfrak{d}))$.

(i) $\eta_{\mathfrak{d}}(\mathcal{C}(\mathfrak{d}, X)) = \begin{cases} \Omega_{\mathfrak{d}}^+ & \text{if } w(\mathfrak{d}) \text{ is even} \\ \Omega_{\mathfrak{d}}^- & \text{if } w(\mathfrak{d}) \text{ is odd.} \end{cases}$

(ii) *For every* $\omega \in \eta_{\mathfrak{d}}(\mathcal{C}(\mathfrak{d}, X))$ *we have*

$$\frac{|\{\chi \in \mathcal{C}(\mathfrak{d}, X) : \eta_{\mathfrak{d}}(\chi) = \omega\}|}{|\mathcal{C}(\mathfrak{d}, X)|} = 1/|\Omega_{\mathfrak{d}}^{(-1)^{w(\mathfrak{d})}}|.$$

Proof. The proof is analogous to that of [8, Proposition 10.7]. By (6), we have $\mathrm{Pic}(\mathcal{O}_{K,\Sigma(\mathfrak{d})}) = 0$. Therefore by global class field theory, we have

$$\begin{aligned}\mathcal{C}(K) &\cong \mathrm{Hom}(\mathbf{A}_K^\times/K^\times, \pm 1)\\ &\cong \mathrm{Hom}((\textstyle\prod_{v\in\Sigma(\mathfrak{d})} K_v^\times \times \prod_{\mathfrak{q}\notin\Sigma(\mathfrak{d})} \mathcal{O}_\mathfrak{q}^\times)/\mathcal{O}_{K,\Sigma(\mathfrak{d})}^\times, \pm 1).\end{aligned}$$

Let

$$\begin{aligned}Q_1 &:= \{\mathfrak{q} : \mathfrak{q} \in \mathcal{P}_0, \mathbf{N}(\mathfrak{q}) \le X\},\\ Q_2 &:= \{\mathfrak{q} : \mathfrak{q} \in \mathcal{P}_1 \cup \mathcal{P}_2 \cup \cdots \cup \mathcal{P}_{2g}, \mathfrak{q} \nmid \mathfrak{d}\} \cup \{\mathfrak{q} : \mathfrak{q} \in \mathcal{P}_0, \mathbf{N}(\mathfrak{q}) \ge X\}.\end{aligned}$$

Let

$$G := \textstyle\prod_{\mathfrak{q}\in Q_1} \mathcal{O}_\mathfrak{q}^\times, \quad H := \prod_{v\in\Sigma(\mathfrak{d})} K_v^\times \times \prod_{\mathfrak{q}\in Q_2} \mathcal{O}_\mathfrak{q}^\times, \quad J := \mathcal{O}_{K,\Sigma(\mathfrak{d})}^\times.$$

Lemma 7.4 shows that $\ker(J/J^2 \to G/G^2)$ is generated by Δ, so by [8, Lemma 10.4(i)], the image of the restriction map

$$\mathcal{C}(K) \longrightarrow \mathrm{Hom}(\textstyle\prod_{v\in\Sigma(\mathfrak{d})} K_v^\times \times \prod_{\mathfrak{q}\in Q_2} \mathcal{O}_\mathfrak{q}^\times, \pm 1)$$

is exactly

$$\mathrm{Hom}((\prod_{v\in\Sigma(\mathfrak{d})} K_v^\times \times \prod_{\mathfrak{q}\in Q_2} \mathcal{O}_\mathfrak{q}^\times)/\langle\Delta\rangle, \{\pm 1\}).$$

Note also that for $\chi \in \mathcal{C}(K)$, we have

$$\chi \in \mathcal{C}(\mathfrak{d}, X) \iff \chi_\mathfrak{q}(\mathcal{O}_\mathfrak{q}^\times) = 1 \text{ for } \mathfrak{q} \in Q_2 \text{ and } \chi_\mathfrak{q}(\mathcal{O}_\mathfrak{q}^\times) \ne 1 \text{ if } \mathfrak{q} \mid \mathfrak{d}.$$

By Lemma 7.2, for $\mathfrak{q} \in \mathcal{P}_n$ we have

$$\begin{aligned}&\Delta \in (K_\mathfrak{q}^\times)^2 \iff n \text{ is even},\\ &\Delta \text{ generates } \mathcal{O}_\mathfrak{q}^\times/(\mathcal{O}_\mathfrak{q}^\times)^2 \cong \mathbf{Z}/2\mathbf{Z} \iff n \text{ is odd}.\end{aligned}$$

Then it follows that for $\omega \in \Omega_\mathfrak{d}$ (noting $\omega_\mathfrak{q}$ is ramified for $\mathfrak{q}|\mathfrak{d}$ by definition), we have

$$\omega \in \eta_\mathfrak{d}(\mathcal{C}(\mathfrak{d}, X)) \iff (-1)^{w(\mathfrak{d})} \prod_{v\in\Sigma} \omega_v(\Delta) = 1 \iff \mathrm{sign}_\Delta(\omega) = (-1)^{w(\mathfrak{d})},$$

which proves (i). For the second assertion, note that for $\chi_1, \chi_2 \in \mathcal{C}(\mathfrak{d}, X)$, we have

$$\eta_\mathfrak{d}(\chi_1) = \eta_\mathfrak{d}(\chi_2) \iff \chi_1\chi_2^{-1} \in \ker(\eta_1) \ (\subseteq \mathcal{C}(1, X)).$$

It follows that all nonempty fibers of $\eta_{\mathfrak{d}} : \mathcal{C}(\mathfrak{d}, X) \to \Omega_{\mathfrak{d}}$ have the same order $|\ker(\eta_1)|$. Now (ii) follows from (i). □

8. The distribution of 2-Selmer ranks

A large part of this section follows the exposition of [8] as mentioned before. We include proofs of many results already in [8] here for the convenience of the reader.

Let D denote the set of probability distributions on $\mathbf{Z}_{\geq 0}$.

$$D := \left\{ h : \mathbf{Z}_{\geq 0} \to \mathbf{R}_{\geq 0} \mid \sum_{n=0}^{\infty} h(n) = 1 \right\}.$$

Definition 8.1. A matrix $M = [m_{i,j}]_{i,j \in \mathbf{Z}_{\geq 0}}$ is called a *Markov operator* on D if the following conditions hold.

(i) $m_{i,j} \geq 0$ for all $i, j \in \mathbf{Z}_{\geq 0}$,

(ii) $\sum_{j \geq 0} m_{i,j} = 1$ for every i.

A Markov operator M acts on D so that for $h \in D$,

$$M(h)(j) = \sum_{i \geq 0} m_{i,j} h(i).$$

Define

$$\begin{aligned} D^{\text{even}} :=& \{h \in D : h(n) = 0 \text{ if } n \text{ is odd}\}, \\ D^{\text{odd}} :=& \{h \in D : h(n) = 0 \text{ if } n \text{ is even}\}. \end{aligned}$$

Example 8.2. Recall that $M_L = [m_{i,j}]_{i,j \in \mathbf{Z}_{\geq 0}}$ given by

$$m_{i,j} = \begin{cases} 1 - 2^{-i} & \text{if } j = i - 1, \\ 2^{-i} & \text{if } j = i + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then M_L is a Markov operator on D.

Definition 8.3. Let h be a probability distribution on $\mathbf{Z}_{\geq 0}$. We define the *parity* $\rho(h)$ of h by

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

Recall

$$f_n = \prod_{j=1}^{\infty}(1+2^{-j})^{-1}\prod_{j=1}^{n}\frac{2}{2^j-1}.$$

Definition 8.4. Define $\mathbf{E}^+ \in D^{\text{even}}$ and $\mathbf{E}^- \in D^{\text{odd}}$ by

$$\mathbf{E}^+(n) := \begin{cases} f_n & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd,} \end{cases} \quad \mathbf{E}^-(n) := \begin{cases} 0 & \text{if } n \text{ is even} \\ f_n & \text{if } n \text{ is odd.} \end{cases}$$

It follows from [12, Proposition 2.6(f)] for $p = 2$ that $\mathbf{E}^+$ and $\mathbf{E}^-$ are indeed elements of D.

Proposition 8.5. *For every $h \in D$,*

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

Proof. For terminology, we refer the reader to [11]. Since $M_L^2(D^{\text{even}}) \in D^{\text{even}}$, we may regard M_L^2 as a *Markov process* on $\mathbf{Z}_{\geq 0,\text{even}}$. It is not difficult to check $M_L(\mathbf{E}^+) = \mathbf{E}^-$ and $M_L(\mathbf{E}^-) = \mathbf{E}^+$, so $M_L^2(\mathbf{E}^+) = \mathbf{E}^+$ (and $M_L^2(\mathbf{E}^-) = \mathbf{E}^-$). Hence $\mathbf{E}^+$ is an *equilibrium state* for the Markov process M_L^2 on D^{even}. By [11, Theorem 1.8.3], the equilibrium state for M_L^2 on D^{even} is unique. Therefore for every $h \in D^{\text{even}}$, we have

$$\lim_{k\to\infty} M_L^{2k}(h) = \mathbf{E}^+.$$

Similarly, $\mathbf{E}^-$ is the unique equilibrium state for M_L^2 on D^{odd}, so for every $h \in D^{\text{odd}}$ we have

$$\lim_{k\to\infty} M_L^{2k}(h) = \mathbf{E}^-.$$

For every $h \in D$, there exist $h^+ \in D^{\text{even}}$ and $h^- \in D^{\text{odd}}$ such that

$$h = (1-\rho(h))h^+ + \rho(h)h^-,$$

from which the proposition follows. □

For $\omega \in \Omega_{\mathfrak{d}}$, recall that

$$\mathrm{rk}(\omega) = \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J,\omega)).$$

If $\chi \in \mathcal{C}(K)$ then $\chi \in \mathcal{C}(\mathfrak{d})$ for a (unique) $\mathfrak{d} \in \mathcal{D}$, and we define

$$\mathrm{Sel}_2(J,\chi) := \mathrm{Sel}_2(J,\eta_{\mathfrak{d}}(\chi)) \quad \text{and} \quad \mathrm{rk}(\chi) := \mathrm{rk}(\eta_{\mathfrak{d}}(\chi)),$$

where $\eta_{\mathfrak{d}} : \mathcal{C}(\mathfrak{d}) \to \Omega_{\mathfrak{d}}$ is as in Definition 7.3. Then $\mathrm{Sel}_2(J,\chi)$ is the classical 2-Selmer group of J^χ/K, so $\mathrm{rk}(\chi) = \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^\chi/K))$.

Definition 8.6. Suppose $\mathfrak{d} \in \mathcal{D}$. Let $\Omega_{\mathfrak{d}}^+$ and $\Omega_{\mathfrak{d}}^-$ be the sets given by Definition 7.5. Let $E_{\mathfrak{d}}^\pm$ be the probability distribution corresponding to $\Omega_{\mathfrak{d}}^\pm$ so that

$$E_{\mathfrak{d}}^+(n) := \frac{|\{\omega \in \Omega_{\mathfrak{d}}^+ : \mathrm{rk}(\omega) = n\}|}{|\Omega_{\mathfrak{d}}^+|},$$
$$E_{\mathfrak{d}}^-(n) := \frac{|\{\omega \in \Omega_{\mathfrak{d}}^- : \mathrm{rk}(\omega) = n\}|}{|\Omega_{\mathfrak{d}}^-|}.$$

We generalize here several lemmas in [8] due to Klagsbrun, Mazur, and Rubin.

Lemma 8.7. *Suppose $\mathfrak{d} \in \mathcal{D}$ and $X > \overline{\mathcal{L}}(\mathbf{N}(\mathfrak{d}))$. Then*

(i) $$\frac{|\{\chi \in \mathcal{C}(\mathfrak{d},X) : \mathrm{rk}(\chi) = n\}|}{|\mathcal{C}(\mathfrak{d},X)|} = \begin{cases} E_{\mathfrak{d}}^+(n) & \text{if } w(\mathfrak{d}) \text{ is even} \\ E_{\mathfrak{d}}^-(n) & \text{if } w(\mathfrak{d}) \text{ is odd.} \end{cases}$$

(ii) $|\mathcal{C}(\mathfrak{d},X)| = |\mathcal{C}(1,X)|$.

Proof. For (i), suppose that $w(\mathfrak{d})$ is even as it follows similarly when $w(\mathfrak{d})$ is odd. By Proposition 7.6, we have $\eta_{\mathfrak{d}} : \mathcal{C}(\mathfrak{d},X) \to \Omega_{\mathfrak{d}}^+$ is surjective, and all fibers have the same size. Note also that if $\eta_{\mathfrak{d}}(\chi) = \omega$, we have $\mathrm{rk}(\chi) = \mathrm{rk}(\omega)$ by definition. Therefore (i) follows. For (ii), note first that $\mathcal{C}(\mathfrak{d},X)$ is nonempty by Proposition 7.6, so one can choose $\varphi \in \mathcal{C}(\mathfrak{d},X)$. Then the map $\mathcal{C}(1,X) \to \mathcal{C}(\mathfrak{d},X)$ defined by multiplication by φ is a bijection (its inverse is also multiplication by φ), so (ii) follows. □

For the rest of the paper, we assume that C has UDRL. Recall the definition of $\mathcal{L}$ in Definition 6.7.

Definition 8.8. Define a sequence of real valued functions $\{L_n(Y)\}_{n\geq 1}$ by

$$\begin{aligned} L_1(Y) &:= \mathcal{L}(Y), \\ L_{n+1}(Y) &:= \max\{\mathcal{L}(\textstyle\prod_{j\leq n} L_j(Y)), YL_n(Y)\} \quad \text{for} \quad n \geq 1. \end{aligned}$$

If $m, k \in \mathbf{Z}_{\geq 0}$ and $X \in \mathbf{R}_{>0}$, define the "fan"

$$\begin{aligned} \mathcal{D}_{m,k,X} := \{\mathfrak{d} \in \mathcal{D} : w(\mathfrak{d}) = k \text{ and} \\ \mathfrak{d} = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_m \text{ with } \mathbf{N}(\mathfrak{q}_j) < L_j(X) \text{ for all } j\}. \end{aligned}$$

Definition 8.9. For $m, k \geq 0$, define

$$\mathcal{B}_{m,k,X} := \coprod_{\mathfrak{d}\in\mathcal{D}_{m,k,X}} \mathcal{C}(\mathfrak{d}, \mathcal{L}(L_{m+1}(X))) \subset \mathcal{C}(K).$$

We call $\mathcal{B}_{m,k,X}$ a *fan structure* on $\mathcal{C}(K)$.

Lemma 8.10. *Suppose that C has UDRL and $\mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}$. Suppose that $m, k, n \geq 0$ and $\cup_X \mathcal{D}_{m,k,X}$ is nonempty, then*

(i) $\lim_{X\to\infty} \dfrac{1}{|\mathcal{D}_{m,k,X}|} \sum_{\mathfrak{d}\in\mathcal{D}_{m,k,X}} E_{\mathfrak{d}}^{(-1)^k} = M_L^k(E_1^{(-1)^k})$

(ii) $\lim_{X\to\infty} \dfrac{|\{\chi \in \mathcal{B}_{m,k,X} : \mathrm{rk}(\chi) = n\}|}{|\mathcal{B}_{m,k,X}|} = \begin{cases} M_L^k(E_1^+)(n) & \text{if } k \text{ is even} \\ M_L^k(E_1^-)(n) & \text{if } k \text{ is odd.} \end{cases}$

Proof. (i) follows from [8, Theorem 4.3]. Note that the assumption of [8, Theorem 4.3] holds by Proposition 4.12. Note also that the "convergence rates" ([8, Section 3.7]) condition is assumed implicitly in the theorem. This condition is satisfied by Theorem 6.9, which assumes that C has UDRL and $\mathrm{Gal}(K(J[2])/K) \cong S_{2g+1}$. This is why the UDRL condition (and also the Galois condition) is necessary in our case. For (ii), we first note that

$$\begin{aligned} &\frac{|\{\chi \in \mathcal{B}_{m,k,X} : \mathrm{rk}(\chi) = n\}|}{|\mathcal{B}_{m,k,X}|} \\ &= \frac{\sum_{\mathfrak{d}\in\mathcal{D}_{m,k,X}} |\{\chi \in \mathcal{C}(\mathfrak{d}, \mathcal{L}(L_{m+1}(X))) : \mathrm{rk}(\chi) = n\}|}{\sum_{\mathfrak{d}\in\mathcal{D}_{m,k,X}} \mathcal{C}(\mathfrak{d}, \mathcal{L}(L_{m+1}(X)))}. \end{aligned}$$

Assume that X is large enough (e.g. $X > \mathbf{N}(\mathfrak{d})$). Then $\mathcal{C}(\mathfrak{d}, \mathcal{L}(L_{m+1}(X)))$ is the same for all $\mathfrak{d} \in \mathcal{D}_{m,k,X}$ by Lemma 8.7(ii), and the right hand side of

this equality is equal to

$$\frac{1}{|\mathcal{D}_{m,k,X}|}\sum_{\mathfrak{d}\in\mathcal{D}_{m,k,X}} E_{\mathfrak{d}}^{(-1)^k}(n)$$

by Lemma 8.7(i). Now (ii) is an immediate consequence of (i). □

Definition 8.11. If $\psi,\psi'\in\mathcal{C}(K_v)$, let

$$h(\psi,\psi') := \dim_{\mathbf{F}_2}(\alpha_v(\psi)/(\alpha_v(\psi)\cap\alpha_v(\psi')))$$

where $\alpha_v:\mathcal{C}(K_v)\to\mathcal{H}(q_v)$ is given in Definition 4.5, and define

$$\gamma_v(\psi) := (-1)^{h(\mathbf{1}_v,\psi)}\psi(\Delta)\in\{\pm1\},$$
$$\delta_v = \frac{1}{|\mathcal{C}(K_v)|}\sum_{\psi\in\mathcal{C}(K_v)}\gamma_v(\psi),\quad\text{and}\quad \delta(J/K) := \frac{(-1)^{\mathrm{rk}(\mathbf{1})}}{2}\prod_{v\in\Sigma}\delta_v.$$

Lemma 8.12. *Suppose that* $\mathrm{Gal}(K(J[2])/K)\cong S_{2g+1}$. *We enlarge* Σ *if necessary to contains a prime* $\mathfrak{q}\nmid 2$ *for which* J *has good reduction and* $\dim_{\mathbf{F}_2}(J(K_\mathfrak{q})[2])$ *is odd. Then*

$$\rho(E_1^+) = \tfrac{1}{2}-\delta(J/K)\quad\textit{and}\quad \rho(E_1^-) = \tfrac{1}{2}+\delta(J/K).$$

Proof. Let $\varphi\in\Omega_1$ so that

$$\varphi_\mathfrak{q}\in\mathcal{C}_{\mathrm{ram}}(K_\mathfrak{q}),$$
$$\varphi_v = 1_v\quad\text{if } v\neq\mathfrak{q}\text{ and } v\in\Sigma.$$

In particular, $\varphi_\mathfrak{q}(\Delta)=-1$ by Lemma 7.2(ii). Let $\omega\in\Omega_1$. Combining Remark 4.3, Lemma 4.6 and Lemma 7.2(ii), we get

$$(-1)^{h(1_\mathfrak{q},\omega_\mathfrak{q})} = \omega_\mathfrak{q}(\Delta),\qquad (-1)^{h(1_\mathfrak{q},\omega_\mathfrak{q}\varphi_\mathfrak{q})} = \omega_\mathfrak{q}\varphi_\mathfrak{q}(\Delta) = -\omega_\mathfrak{q}(\Delta).$$

We also have

$$\mathrm{rk}(\omega')\not\equiv\mathrm{rk}(\omega)\pmod 2$$

by Lemma 5.5(ii). Then the lemma follows as in the proof of [8, Lemma 11.10]. □

Theorem 8.13. *Suppose* C *over* K *has UDRL and* $\mathrm{Gal}(K(J[2])/K)\cong S_{2g+1}$. *We enlarge* Σ *if necessary to contain a prime* $\mathfrak{q}\nmid 2$ *where* J *has good*

reduction and $\dim_{\mathbf{F}_2}(J(K_\mathfrak{q})[2])$ *is odd. Let* $\mathcal{B}_m(X) := \cup_k \mathcal{B}_{m,k,X}$. *Then for every* $n \geq 0$ *we have*

$$\lim_{m\to\infty}\lim_{X\to\infty}\frac{|\{\chi \in \mathcal{B}_m(X) \mid \mathrm{rk}(\chi) = n\}|}{|\mathcal{B}_m(X)|} = \left(\frac{1}{2} + \delta(J/K)\right)\mathbf{E}^+(n) + \left(\frac{1}{2} - \delta(J/K)\right)\mathbf{E}^-(n).$$

Proof. The theorem follows from Lemma 8.10(ii), Lemma 8.12, and Proposition 8.5. □

If we assume Conjecture 5.12, we obtain the following.

Conjecture 8.14. *Theorem 8.13 holds without the UDRL condition.*

Acknowledgements

The author is grateful to Karl Rubin for sharing his idea into the subject. He thanks Dennis Eichhorn for providing the proof of Lemma 3.8. He also would like to thank the referee for many comments to vastly improve the readability of the paper.

References

[1] G. E. Andrews, The Theory of Partitions, Cambridge Mathematical Library, Cambridge University Press, Cambridge (1998), ISBN 0-521-63766-X. Reprint of the 1976 original.

[2] M. Bhargava and B. H. Gross, *The average size of the* 2*-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, in: Automorphic Representations and *L*-Functions, Vol. 22 of Tata Inst. Fundam. Res. Stud. Math., pp. 23–91, Tata Inst. Fund. Res., Mumbai (2013).

[3] M. Bhargava, D. M. Kane, H. W. Lenstra, Jr., B. Poonen, and E. Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Camb. J. Math. **3** (2015), no. 3, 275–321.

[4] T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64.

[5] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370. With an appendix by P. Monsky.

[6] D. Kane, *On the ranks of the 2-Selmer groups of twists of a given elliptic curve*, Algebra Number Theory **7** (2013), no. 5, 1253–1279.

[7] Z. Klagsbrun, B. Mazur, and K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320.

[8] Z. Klagsbrun, B. Mazur, and K. Rubin, *A Markov model for Selmer ranks in families of twists*, Compos. Math. **150** (2014), no. 7, 1077–1106.

[9] B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96.

[10] A. Morgan, *Quadratic twists of abelian varieties and disparity in Selmer ranks*, Algebra Number Theory **13** (2019), no. 4, 839–899.

[11] J. R. Norris, Markov chains, Vol. 2 of Cambridge Series in Statistical and Probabilistic Mathematics, Cambridge University Press, Cambridge (1998), ISBN 0-521-48181-3. Reprint of 1997 original.

[12] B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269.

[13] P. Swinnerton-Dyer, *The effect of twisting on the* 2*-Selmer group*, Math. Proc. Cambridge Philos. Soc. **145** (2008), no. 3, 513–526.

[14] M. Yu, *Selmer ranks of twists of hyperelliptic curves and superelliptic curves*, J. Number Theory **160** (2016), 148–185.

Center for Mathematical Challenges
Korea Institute for Advanced Study
85 Hoegiro, Dongdaemun-gu, Seoul, Republic of Korea
E-mail address: mjyu.math@gmail.com

Received October 31, 2017