Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jiali YAN

**Computing the Cassels-Tate Pairing on the Selmer group of a Richelot Isogeny**

Tome 35, nº 3 (2023), p. 659-674.

https://doi.org/10.5802/jtnb.1259



CENTRE MERSENNE

*Le* Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

*Journal de Théorie des Nombres de Bordeaux* **35** (2023), 659–674

# Computing the Cassels-Tate Pairing on the Selmer group of a Richelot Isogeny

par Jiali YAN

Résumé. Dans cet article, nous étudions l'accouplement de Cassels-Tate sur les jacobiennes des courbes de genre 2 possédant une isogénie dite de Richelot. Soit $\phi : J \to \widehat{J}$ une isogénie de Richelot entre les jacobiennes de deux courbes de genre 2. Nous donnons une formule explicite et un algorithme pratique pour calculer l'accouplement de Cassels-Tate sur $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$ où $\widehat{\phi}$ est l'isogénie duale de $\phi$. Ces résultats sont obtenus sous l'hypothèse simplificatrice que tous les points de 2-torsion sur $J$ sont définis sur $K$. Nous donnons un exemple explicite qui montre que nous pouvons transformer la descente par l'isogénie de Richelot en 2-descente en calculant l'accouplement de Cassels-Tate.

Abstract. In this paper, we study the Cassels-Tate pairing on Jacobians of genus two curves admitting a special type of isogenies called Richelot isogenies. Let $\phi : J \to \widehat{J}$ be a Richelot isogeny between two Jacobians of genus two curves. We give an explicit formula as well as a practical algorithm to compute the Cassels-Tate pairing on $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$ where $\widehat{\phi}$ is the dual isogeny of $\phi$. The formula and algorithm are under the simplifying assumption that all two-torsion points on $J$ are defined over $K$. We also include a worked example demonstrating we can turn the descent by Richelot isogeny into a 2-descent via computing the Cassels-Tate pairing.

## 1. Introduction

For any principally polarized abelian variety $A$ defined over a number field $K$, Cassels and Tate [6], [7] and [23] constructed a pairing

$$Ш(A) \times Ш(A) \to \mathbb{Q}/\mathbb{Z},$$

that is nondegenerate after quotienting out the maximal divisible subgroup of $Ш(A)$. This pairing is called the Cassels-Tate pairing and it naturally lifts to a pairing on Selmer groups. One application of this pairing is in improving the bound on the Mordell-Weil rank $r(A)$ obtained by performing a standard descent calculation. Suppose $Ш(A)$ is finite, then carrying out an $n$-descent and computing the Cassels-Tate pairing on $\mathrm{Sel}^n(A) \times \mathrm{Sel}^n(A)$

Manuscrit reçu le 23 janvier 2022, révisé le 5 juillet 2023, accepté le 12 juillet 2023.
2020 *Mathematics Subject Classification.* 11N56, 14G42.
*Mots-clefs.* Genus 2 Curve, Cassels-Tate Pairing, Richelot isogeny.

gives the same bound as obtained from the $n^2$-descent where $\mathrm{Sel}^{n^2}(A)$ needs to be computed. Since the kernel of the pairing equals the image of the $n^2$-Selmer group in the $n$-Selmer group, the rank bound one gets is the same as that obtained by $n^2$-descent (as shown in [24, Proposition 1.9.3]).

There have been many results on computing the Cassels-Tate pairing in the case of elliptic curves. For example, in addition to defining the pairing, Cassels also described a method for computing the pairing on $\mathrm{Sel}^2(E) \times \mathrm{Sel}^2(E)$ in [8] by solving conics over the field of definition of a two-torsion point. Donnelly [10] then described a method that only requires solving conics over $K$ and Fisher [12] used the invariant theory of binary quartics to give a new formula for the Cassels-Tate pairing on $\mathrm{Sel}^2(E) \times \mathrm{Sel}^2(E)$ without solving any conics. In [2, 3], van Beek and Fisher computed the Cassels-Tate pairing on the 3-isogeny Selmer group of an elliptic curve. For $p = 3$ or 5, Fisher computed the Cassels-Tate pairing on the $p$-isogeny Selmer group of an elliptic curve in a special case in [11]. In [13], Fisher and Newton computed the Cassels-Tate pairing on $\mathrm{Sel}^3(E) \times \mathrm{Sel}^3(E)$. We are interested in the natural problem of generalizing the different algorithms for computing the Cassels-Tate pairing for elliptic curves to computing the pairing for abelian varieties of higher dimensions.

In this paper, we study the Cassels-Tate pairing on Jacobians of genus two curves admitting a special type of isogeny called a Richelot isogeny. Let $\phi : J \to \widehat{J}$ be a Richelot isogeny between Jacobians of two genus two curves. We will be working under the assumption that all two-torsion points on $J$ are defined over $K$. This simplifies the computation. Because computing the 2-Selmer group is cheap, the goal of this paper is not to improve the rank bound. Instead, the goal of this paper is to illustrate a method that explicitly computes the CT pairing in higher dimensions, which has not been done before. Consider the following long exact sequence

(1.1)
$$0 \to J[\phi](\mathbb{Q}) \to J[2](\mathbb{Q}) \to \widehat{J}[\widehat{\phi}](\mathbb{Q}) \to \mathrm{Sel}^{\phi}(J) \to \mathrm{Sel}^2(J) \xrightarrow{\alpha} \mathrm{Sel}^{\hat{\phi}}(\widehat{J}).$$

Let $\langle \cdot, \cdot \rangle_{CT}$ denote the Cassels-Tate pairing on $\mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. It is shown in Remark 3.4 that we can replace $\mathrm{Sel}^{\hat{\phi}}(\widehat{J})$ with $\ker\langle \cdot, \cdot \rangle_{CT}$ and (1.1) remains exact. Although it is not the goal of the paper, this shows computing the pairing $\langle \cdot, \cdot \rangle_{CT}$ potentially improves the rank bound given by carrying out a descent by Richelot isogeny. Then later in the paper, we describe an explicit algorithm to compute the pairing $\langle \cdot, \cdot \rangle_{CT}$.

In Section 2, we give some background results needed for the later sections and we define a pairing on $\mathrm{Sel}^{\phi}(J) \times \mathrm{Sel}^{\phi}(J)$ following the Weil pairing definition of the Cassels-Tate pairing for the Richelot isogeny $\phi$. In Section 3, we then give an explicit formula as well as a practical algorithm to compute the Cassels-Tate pairing on $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$ where $\widehat{\phi}$ is the dual isogeny of $\phi$ and also a Richelot isogeny. In Section 4, we give some details of the explicit computation and show directly that the formula for the Cassels-Tate pairing is always a finite product with a computable bound. In Section 5, we include a worked example demonstrating we can turn the descent by Richelot isogeny into a 2-descent via computing the Cassels-Tate pairing. The content of this paper is based on Chapter 2 of the thesis of the author [24].

## 2. Preliminary Results

**2.1. The set-up.** In this paper, we are working over a number field $K$. For any field $k$, we let $\overline{k}$ denote its algebraic closure and let $\mu_n \subset \overline{k}$ denote the $n^{th}$ roots of unity in $\overline{k}$. We let $G_k$ denote the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$.

Let $\mathcal{C}$ be a general *genus two curve* defined over $K$ with all Weierstrass points defined over $K$, which is a smooth projective curve and it can be given in the following hyperelliptic form:

$$C : y^2 = f(x) = G_1(x)G_2(x)G_3(x), \tag{2.1}$$

where $G_1(x) = \lambda(x-\omega_1); G_2(x) = (x-\omega_2)(x-\omega_3); G_3(x) = (x-\omega_4)(x-\omega_5)$ with $\lambda, \omega_i \in K$, $\omega_i$ pairwise distinct and $\lambda \neq 0$.

We let $J$ denote the *Jacobian variety* of $\mathcal{C}$, which is an abelian variety of dimension 2 defined over $K$ that can be identified with $\mathrm{Pic}^0(\mathcal{C})$. We denote the identity element of $J$ by $\mathcal{O}_J$ and the point at infinity by $\infty$. Via the natural isomorphism $\mathrm{Pic}^2(\mathcal{C}) \to \mathrm{Pic}^0(\mathcal{C})$ sending $[P_1+P_2] \mapsto [P_1+P_2-2\infty]$, a point $P \in J$ can be identified with an unordered pair of points of $\mathcal{C}$, $\{P_1, P_2\}$. This identification is unique unless $P = \mathcal{O}_J$, in which case it can be represented by any pair of points on $\mathcal{C}$ in the form $\{(x, y), (x, -y)\}$ or $\{\infty, \infty\}$. Moreover, $J[2] = \{\mathcal{O}_J, \{(\omega_i, 0), (\omega_j, 0)\}$ for $i \neq j, \{(\omega_i, 0), \infty\}\}$. Let $e_2 : J[2] \times J[2] \to \mu_2$ denote the Weil pairing on $J[2]$. As described in [9, Chapter 3, Section 3], suppose $\{P_1, P_2\}$ and $\{Q_1, Q_2\}$ represent $P, Q \in J[2]$ where $P_1, P_2, Q_1, Q_2$ are Weierstrass points, then

$$e_2(P, Q) = (-1)^{|\{P_1,P_2\}\cap\{Q_1,Q_2\}|}. \tag{2.2}$$

**2.2. Richelot isogenies.** A *Richelot isogeny* is a polarized $(2, 2)$-isogeny between Jacobians of genus 2 curves. In particular, it is an isogeny $\phi : J \to \widehat{J}$ such that $J[\phi] \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and $J, \widehat{J}$ are Jacobians of genus two curves.

A special case of [16, Proposition 16.8] and [5, Lemma 2.4] shows that the kernel of a Richelot isogeny is actually a maximal isotropic subgroup of $J[2]$ with respect to the Weil pairing $e_2$ on $J[2] \times J[2]$. We have the following general proposition on Richelot isogenies from [9, Chapter 9 Section 2] and [14, Section 3]. In Remark 2.2, we give the extra details for the case where the hyperelliptic form of the underlying curve is of degree 5.

**Proposition 2.1.** *Suppose the curve $\mathcal{C}$ is of the form*

$$\mathcal{C} : y^2 = f(x) = G_1(x)G_2(x)G_3(x),$$

*where $G_j(x) = g_{j2}x^2 + g_{j1}x + g_{j0}$, with $g_{ji} \in K$. Let $\Delta = \det(g_{ij})$, which we assume to be non-zero. Then there is a Richelot isogeny $\phi$ from $J$, the Jacobian of $\mathcal{C}$, to $\widehat{J}$, the Jacobian of the following genus two curve:*

$$\widehat{\mathcal{C}} : \Delta y^2 = L_1(x)L_2(x)L_3(x), \tag{2.3}$$

*where each $L_i(x) = G'_j(x)G_k(x) - G_j(x)G'_k(x)$, for $[i,j,k] = [1,2,3]$, $[2,3,1]$, $[3,1,2]$.*

*In addition, the kernel of $\phi$ consists of the identity $\mathcal{O}_J$ and the 3 divisors of order 2 given by $G_i = 0$. We have a similar result for the dual isogeny $\widehat{\phi}$.*

*Moreover, any genus two curve $\mathcal{C}$ that admits a Richelot isogeny with all the elements of the kernel $K$-rational is of the form $y^2 = f(x) = G_1(x)G_2(x)G_3(x)$ as above.*

**Remark 2.2.** We exclude the case $\Delta = 0$ in the above proposition. In fact, by [9, Chapter 14], $\Delta = 0$ implies that the Jacobian of $\mathcal{C}$ is isogenous (via the Richelot isogeny) to a product of elliptic curves. It can be checked that the analogue of $\Delta$ for $\widehat{C}$ is $2\Delta^2$, so the corresponding condition for $\widehat{C}$ is automatically satisfied. Also, in the case where $G_i$ is linear, say $G_i = a(x-b)$, then we say $\{(b,0), \infty\}$ is the divisor given by $G_i = 0$ which gives an element in $\ker\phi$.

We use the notation in Proposition 2.1 and denote the nontrivial elements in the kernel of $\phi$ by $P_i$ corresponding to the divisors of order 2 given by $G_i = 0$ as well as denote the nontrivial elements in the kernel of $\widehat{\phi}$ by $P'_i$. From [9, Chapter 9, Section 2] and [22, Section 3.2], we have the following description of the Richelot isogeny $\phi$. Associated with a Weierstrass point $P = (\omega_1, 0)$ with $G_1(\omega_1) = 0$, for a generic $(x,y) \in \mathcal{C}$, $\phi : J \to \widehat{J}$ is given explicitly as

$$\{(x,y), P\} \mapsto \{(z_1,t_1),(z_2,t_2)\},$$

where $z_1, z_2$ satisfy

$$G_2(x)L_2(z) + G_3(x)L_3(z) = 0;$$

and $(z_i, t_i)$ satisfies

$$yt_i = G_2(x)L_2(z_i)(x - z_i).$$

Denote the set of two points on $\mathcal{C}$ given by $G_i = 0$ by $S_i$ for $i = 1,2,3$. From the explicit description above, we know that the preimages of $P'_1$ under $\phi$ are precisely $\{\{Q_1,Q_2\} \in J[2]$ such that $Q_1 \in S_2, Q_2 \in S_3\}$. Similarly we know the preimages of $P'_2$ and $P'_3$.

**2.3. The Weil pairing for the Richelot isogeny.** Let $J$ and $\widehat{J}$ be Jacobian varieties of genus two curves defined over $K$. Assume there is a Richelot isogeny $\phi : J \to \widehat{J}$ with $\widehat{\phi}$ being its dual, i.e. $\phi \circ \widehat{\phi} = [2]$. Then we have the Weil pairing

$$e_\phi : J[\phi] \times \widehat{J}[\widehat{\phi}] \to \overline{K}^*,$$

where $e_\phi(P,Q) = e_{2,J}(P,Q')$ for any $Q' \in J[2]$ such that $\phi(Q') = Q$. The image of $e_\phi$ is in fact $\mu_2(\overline{K}^*) \subset \overline{K}^*$. Recall $J[\phi]$ is isotropic with respect to $e_{2,J}$ as discussed in Section 2.2. This implies that $e_{2,J}(P,Q') = e_{2,J}(P,Q'')$ if $\phi(Q') = \phi(Q'')$ and hence $e_\phi$ is well-defined. By (2.2) and the end of Section 2.2, $e_\phi(P_i, P_i') = 1$ for any $i = 1,2,3$ and $e_\phi(P_i, P_j') = -1$ for any $i \neq j$. Furthermore, given any $P \in J[2], Q \in \widehat{J}[2]$, we know $e_{2,J}(P, \widehat{\phi}(Q)) = e_{2,\hat{J}}(\phi(P), Q)$ by [18, Proposition 13.2(a)], which implies that $e_\phi(P,Q) = e_{\hat{\phi}}(Q,P)$ for any $P \in J[\phi], Q \in \widehat{J}[\widehat{\phi}]$.

**2.4. Definition of the Cassels-Tate pairing in the case of a Richelot isogeny.** In this section, we give the definition of the Cassels-Tate pairing in the case of a Richelot isogeny. There are four equivalent definitions of the Cassels-Tate pairing stated and proved in [19]. The compatibility of the definition below with the Weil Pairing definition of the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ is shown in [24, Proposition 2.1.6].

Let $J$ and $\widehat{J}$ be Jacobian varieties of genus two curves defined over a number field $K$ such that there exists a Richelot isogeny $\phi : J \to \widehat{J}$ with $\widehat{\phi} : \widehat{J} \to J$ being its dual isogeny and all points in $J[\phi]$ are defined over $K$. The following lemma shows that for any $b \in \mathrm{Sel}^\phi(J)$, there exists $b_1 \in H^1(G_K, \widehat{J}[2])$ mapping to $b$ under the map induced by $\widehat{J}[2] \xrightarrow{\hat{\phi}} J[\phi]$.

**Lemma 2.3.** *Let $J$ and $\widehat{J}$ be Jacobian varieties of genus two curves such that there exists a Richelot isogeny $\phi : J \to \widehat{J}$ with $\widehat{\phi} : \widehat{J} \to J$ being its dual isogeny. Suppose all points in $J[\phi]$ are defined over $K$, We have the following:*

(i) *The map $H^2(G_K, J[\phi]) \xrightarrow{res} \prod_v H^2(G_{K_v}, J[\phi])$ is injective.*
(ii) *For any $b \in \mathrm{Sel}^\phi(J)$, there exists $b_1 \in H^1(G_K, \widehat{J}[2])$ mapping to $b$.*

*Proof.* Since $J[\phi] \cong (\mu_2)^2$ over $K$ and $\mathrm{Br}(K)[2] \cong H^2(G_K, \mu_2)$, we have $H^2(G_K, J[\phi]) \cong (H^2(G_K, \mu_2))^2 \cong (\mathrm{Br}(K)[2])^2$ and similarly $H^2(G_{K_v}, J[\phi]) \cong (\mathrm{Br}(K_v)[2])^2$. Hence, via the injection of $\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v)$, we have $H^2(G_K, J[\phi]) \xrightarrow{res} \prod_v H^2(G_{K_v}, J[\phi])$ is injective, which is (i). Note that by the formula in Proposition 2.1, all points in $\widehat{J}[\widehat{\phi}]$ are also defined over $K$, therefore $H^2(G_K, \widehat{J}[\widehat{\phi}]) \to \prod_v H^2(G_{K_v}, \widehat{J}[\widehat{\phi}])$, is also injective.

Now, consider the following commutative diagram of short exact sequences.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{J}[\widehat{\phi}] & \longrightarrow & \widehat{J}[2] & \xrightarrow{\hat{\phi}} & J[\phi] & \longrightarrow & 0 \\
 & & \Big\downarrow{=} & & \Big\downarrow{inc} & & \Big\downarrow{inc} & & \\
0 & \longrightarrow & \widehat{J}[\widehat{\phi}] & \longrightarrow & \widehat{J} & \xrightarrow{\hat{\phi}} & J & \longrightarrow & 0
\end{array}$$

We then obtain the following commutative diagram of long exact sequences along the rows by taking Galois cohomology.

$$\begin{array}{ccccc}
H^1(G_K, \widehat{J}[2]) & \xrightarrow{\hat{\phi}} & H^1(G_K, J[\phi]) & \longrightarrow & H^2(G_K, \widehat{J}[\widehat{\phi}]) \\
\Big\downarrow & & \Big\downarrow{b \mapsto c} & & \Big\downarrow{=} \\
H^1(G_K, \widehat{J}) & \xrightarrow{\hat{\phi}} & H^1(G_K, \widehat{J}) & \longrightarrow & H^2(G_K, \widehat{J}[\widehat{\phi}]) \\
\Big\downarrow{res} & & \Big\downarrow{res} & & \Big\downarrow{inj} \\
\prod_v H^1(G_{K_v}, \widehat{J}) & \xrightarrow{\hat{\phi}} & \prod_v H^1(G_{K_v}, J) & \longrightarrow & \prod_v H^2(G_{K_v}, \widehat{J}[\widehat{\phi}])
\end{array}$$

Since $b \in \mathrm{Sel}^{\phi}(J)$, its image $c \in H^1(G_K, \widehat{J})$ is locally trivial. Hence, its image is also trivial in $\prod_v H^2(G_{K_v}, \widehat{J}[\widehat{\phi}])$. Via the injectivity of the map $H^2(G_K, \widehat{J}[\widehat{\phi}]) \to \prod_v H^2(G_{K_v}, \widehat{J}[\widehat{\phi}])$, we get that $b \mapsto 0 \in H^2(G_K, \widehat{J}[\widehat{\phi}])$. Thus $b$ has a lift $b_1 \in H^1(G_K, \widehat{J}[2])$. Hence (ii) holds. ☐

**The definition of the pairing**

Let $a, a' \in \mathrm{Sel}^{\phi}(J)$. Let $a_1 \in H^1(G_K, \widehat{J}[2])$ be an element that maps to $a \in \mathrm{Sel}^{\phi}(J) \subset H^1(G_K, J[\phi])$ under the map induced by $\widehat{J}[2] \xrightarrow{\hat{\phi}} J[\phi]$, which exists by Lemma 2.3.

Let $v$ be a place of $K$. Let $P_v \in \widehat{J}(K_v)$ be a lift of $a_v \in H^1(G_{K_v}, J[\phi])$. Consider the commutative diagram below.

$$\begin{array}{ccccc}
\widehat{J}(K_v) & \xrightarrow[\hat{\phi}]{} & J(K_v) & \xrightarrow[\delta_{\hat{\phi}}]{} & H^1(G_{K_v}, \widehat{J}[\widehat{\phi}]) \\
{=}\Big\downarrow & & {\phi}\Big\downarrow & & {\iota}\Big\downarrow{\rho_v \mapsto \delta_2(P_v) - a_{1,v}} \\
\widehat{J}(K_v) & \xrightarrow[2]{} & \widehat{J}(K_v) & \xrightarrow[\delta_2]{} & H^1(G_{K_v}, \widehat{J}[2]) \\
{\hat{\phi}}\Big\downarrow & & {=}\Big\downarrow & & {\hat{\phi}}\Big\downarrow{\delta_2(P_v) \mapsto a_v \quad a_{1,v} \mapsto a_v} \\
J(K_v) & \xrightarrow[\phi]{} & \widehat{J}(K_v) & \xrightarrow[\delta_{\phi}]{P_v \mapsto a_v} & H^1(G_{K_v}, J[\phi])
\end{array}$$

Then $\delta_2(P_v)$ and $a_{1,v}$ in $H^1(G_{K_v}, \widehat{J}[2])$ both map to $a_v$. Hence, we choose $\rho_v \in H^1(G_{K_v}, \widehat{J}[\widehat{\phi}])$ a lift of $\delta_2(P_v) - a_{1,v}$ and define $\eta_v = \rho_v \cup_{\hat{\phi},v} a'_v \in H^2(G_{K_v}, \overline{K_v}^*)$. Here $\cup_{\hat{\phi},v}$ denotes the cup product $H^1(G_{K_v}, \widehat{J}[\widehat{\phi}]) \times$

$H^1(G_{K_v}, J[\phi]) \to H^2(G_{K_v}, \overline{K}^*)$ associated to $e_{\hat{\phi}}$. The Cassels-Tate pairing is defined by

$$\langle a, a' \rangle_{CT} := \sum_v \mathrm{inv}_v(\eta_v).$$

We sometimes refer to $\mathrm{inv}_v(\eta_v)$ above as the local Cassels-Tate pairing between $a, a' \in \mathrm{Sel}^{\phi}(J)$ for a place $v$ of $K$, noting that this depends on the choice of the global lift $a_1$.

**Remark 2.4.** The Weil pairing definition of the Cassels-Tate pairing is proved to be independent of the choices made in the definition in [19] and more details are given in [24, Proposition 1.8.4]. Since the above pairing is compatible with the Weil pairing definition as in [24, Proposition 2.1.6], we know it is also independent of the choices we make.

## 3. Computation of the Cassels-Tate Pairing

Recall that we are working with a genus two curve $\mathcal{C}$ in the form (2.1) and we fix a choice of Richelot isogeny $\phi : J \to \widehat{J}$ where $J$ is the Jacobian of $\mathcal{C}$ and $\widehat{J}$ is the Jacobian of the genus two curve defined by (2.3). We write $\widehat{\phi}$ for the dual of $\phi$. This implies that all points in $J[2]$ are defined over $K$ and all points in $\widehat{J}[\widehat{\phi}]$ are defined over $K$ by Proposition 2.1. Recall, we denote the nontrivial elements in $J[\phi]$ by $P_1, P_2, P_3$ where $P_i$ corresponds to the divisor given by $G_i = 0$ and the nontrivial elements in $\widehat{J}[\widehat{\phi}]$ by $P_1', P_2', P_3'$ where $P_i'$ corresponds to the divisor given by $L_i = 0$ as in the same Proposition. In this section, we will give a practical formula for the explicit computation for the Cassels-Tate pairing in the case of Richelot isogenies.

**3.1. Explicit embeddings of $\mathbf{H^1(G_K, J[\phi])}$ and $\mathbf{H^1(G_K, J[2])}$.** In order to give the formula for the Cassels-Tate pairing, we first describe some well-known embeddings that are useful for the explicit computation.

Recall all points in $J[2]$ and $\widehat{J}[\widehat{\phi}]$ are defined over $K$. From the exact sequence

$$0 \to J[\phi] \xrightarrow{w_\phi} (\mu_2)^3 \xrightarrow{N} \mu_2 \to 0,$$

where $w_\phi : P \mapsto (e_\phi(P, P_1'), e_\phi(P, P_2'), e_\phi(P, P_3'))$ and $N : (a, b, c) \mapsto abc$, we get

$$H^1(G_K, J[\phi]) \xrightarrow{inj} H^1(G_K, (\mu_2)^3) \cong (K^*/(K^*)^2)^3 \xrightarrow{N_*} H^1(G_K, \mu_2) \cong K^*/(K^*)^2,$$

where $\cong$ denotes the Kummer isomorphism derived from Hilbert's Theorem 90 and $N_*$ is induced by $N$. The induced map $H^1(G_K, J[\phi]) \to H^1(G_K, (\mu_2)^3)$ is injective as the map $(\mu_2)^3 \xrightarrow{N} \mu_2$ is surjective. Furthermore, the image of this injection contains precisely all the elements with norm a square by the exactness of the sequence above, i.e. $H^1(G_K, J[\phi]) \cong$

$\ker((K^*/(K^*)^2)^3 \xrightarrow{N_*} K^*/(K^*)^2)$. We have a similar embedding for $H^1(G_K, \widehat{J}[\widehat{\phi}])$.

Also, from the exact sequence

$$0 \to J[2] \xrightarrow{w_2} (\mu_2)^5 \xrightarrow{N} \mu_2 \to 0,$$

where $w_2 : P \mapsto (e_2(P, \{(\omega_1, 0), \infty\}), \ldots, e_2(P, \{(\omega_5, 0), \infty\}))$ and $N : (a, b, c, d, e) \mapsto abcde$, we get

$$H^1(G_K, J[2]) \xrightarrow{inj} H^1(G_K, (\mu_2)^5) \cong (K^*/(K^*)^2)^5 \xrightarrow{N_*} H^1(G_K, \mu_2) \cong K^*/(K^*)^2,$$

where $\cong$ denotes the Kummer isomorphism derived from Hilbert's Theorem 90 and $N_*$ is induced by $N$. Again the induced map $H^1(G_K, J[2]) \to H^1(G_K, (\mu_2)^5)$ is injective as the map $(\mu_2)^5 \xrightarrow{N} \mu_2$ is surjective. Furthermore, the image of this injection also contains precisely all the elements with norm a square from the exact sequence above. In particular, we have

$$H^1(G_K, J[2]) \cong \ker((K^*/(K^*)^2)^5 \xrightarrow{N} K^*/(K^*)^2)$$

**3.2. Explicit Formula.** Using the embeddings described in Section 3.1, we can now state and prove the explicit formula for the Cassels-Tate pairing in the case of a Richelot isogeny.

**Proposition 3.1.** *Under the embeddings of $H^1(G_K, J[\phi])$ and $H^1(G_K, \widehat{J}[\widehat{\phi}])$ in $(K^*/(K^*)^2)^3$ as described in Section 3.1, we get that the cup product $\cup_\phi$ induced by $e_\phi$ is*

$$H^1(G_K, J[\phi]) \times H^1(G_K, \widehat{J}[\widehat{\phi}]) \to \mathrm{Br}(K)[2]$$
$$((a_1, b_1, c_1), (a_2, b_2, c_2)) \mapsto (a_1, a_2) + (b_1, b_2) + (c_1, c_2),$$

*where $(\,\cdot\,,\cdot\,)$ represents the quaternion algebra and also its equivalence class in* $\mathrm{Br}(K)[2]$.

*Proof.* Recall that the embedding $J[\phi] \to (\mu_2)^3$ is given by sending $P \in J[\phi]$ to

$$(e_\phi(P, P_1'), e_\phi(P, P_2'), e_\phi(P, P_3'))$$

and the embedding $\widehat{J}[\widehat{\phi}] \to (\mu_2)^3$ is given by sending $Q \in \widehat{J}[\widehat{\phi}]$ to

$$(e_\phi(P_1, Q), e_\phi(P_2, Q), e_\phi(P_3, Q)).$$

It can be checked, via the end of the discussion of Section 2.2, that we have the following commutative diagram:

$$\begin{array}{ccc} J[\phi] \times \widehat{J}[\widehat{\phi}] & \xrightarrow{inj} & (\mu_2)^3 \times (\mu_2)^3 \\ {\scriptstyle e_\phi}\downarrow & & \downarrow{\scriptstyle f} \\ \mu_2 & \xrightarrow{=} & \mu_2, \end{array}$$

where $f$ sends $((-1)^a,(-1)^b,(-1)^c),((-1)^{a'},(-1)^{b'},(-1)^{c'})$ to $(-1)^{aa'+bb'+cc'}$ with $a,b,c \in \{0,1\}$.

Consider the natural pairing $\phi : \mu_2 \times \mu_2 \to \mu_2$ sending $((-1)^a,(-1)^b)$ to $(-1)^{ab}$. This gives a cup product pairing

$$\begin{aligned} H^1(G_K,\mu_2) \times H^1(G_K,\mu_2) &\longrightarrow H^2(G_K,\mu_2) \cong \mathrm{Br}(K)[2] \\ ([\sigma \mapsto a_\sigma],[\tau \mapsto b_\tau]) &\longmapsto [(\sigma,\tau) \mapsto \phi(a_\sigma,b_\tau)]. \end{aligned}$$

By Hilbert's Theorem 90, we can identify $H^1(G_K,\mu_2)$ with $K^*/(K^*)^2$. Under this identification, the image of $(a,b) \in K^*/(K^*)^2 \times K^*/(K^*)^2$ is precisely the equivalence class of the quaternion algebra $(a,b)$ by [21, Chapter XIV, Section 2, Proposition 5] and [15, Corollary 2.5.5(1), Proposition 4.7.3].

Therefore, we get that the induced cup product is

$$\begin{aligned} H^1(K,J[\phi]) \times H^1(K,\widehat{J}(\widehat{\phi})) &\longrightarrow \mathrm{Br}(K)[2] \\ ((a_1,b_1,c_1),(a_2,b_2,c_2)) &\longmapsto (a_1,a_2)+(b_1,b_2)+(c_1,c_2). \end{aligned}$$

□

**Proposition 3.2.** *Under the embeddings of $H^1(G_K,J[\phi])$ and $H^1(G_K,J[2])$ in $(K^*/(K^*)^2)^3$ and $(K^*/(K^*)^2)^5$ as described in Section 3.1, the map $\Psi : H^1(G_K,J[\phi]) \to H^1(G_K,J[2])$ induced from the inclusion $J[\phi] \to J[2]$ is given by*

$$(a,b,c) \longmapsto (1,c,c,b,b).$$

*Proof.* Recall the embedding of $H^1(G_K,J[2])$ in $(K^*/(K^*)^2)^5$, and the embedding of $H^1(G_K,J[\phi])$ in $(K^*/(K^*)^2)^3$ are induced from the short exact sequences in the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J[\phi] & \xrightarrow{w_\phi} & (\mu_2)^3 & \xrightarrow{N} & \mu_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle inc} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & J[2] & \xrightarrow{w_2} & (\mu_2)^5 & \xrightarrow{N} & \mu_2 & \longrightarrow & 0. \end{array}$$

Suppose $P \in J[\phi]$ maps to $(\alpha,\beta,\gamma)$ via $w_\phi$. Then $e_\phi(P,P_1') = \alpha$, $e_\phi(P,P_2') = \beta$, $e_\phi(P,P_3') = \gamma$. By definition, $e_\phi(P,\phi(Q)) = e_2(P,Q)$ for any $Q \in J[2]$. From the explicit description of $\phi$ in Section 2.2, we know $\alpha = e_2(P,\{(\omega_2,0),(\omega_4,0)\})$, $\beta = e_2(P,\{(\omega_1,0),(\omega_5,0)\})$ and $\gamma = e_2(P,\{\infty,(\omega_3,0)\})$. Recall that $J[\phi]$ is isotropic with respect to $e_2$. This implies that $w_2(P) = (1,\gamma,\gamma,\beta,\beta)$. Therefore, we define $\psi(\alpha,\beta,\gamma) = (1,\gamma,\gamma,\beta,\beta)$, which makes the above diagram commute.

Now consider $\Psi : H^1(G_K,J[\phi]) \to H^1(G_K,J[2])$ which, via the embedding in Section 3.1, is the map $H^1(G_K,(\mu_2)^3) \to H^1(G_K,(\mu_2)^5)$ induced by $\psi$. Therefore, we can verify that $\Psi(a,b,c) = (1,c,c,b,b)$. □

**Proposition 3.3.** *Under the embeddings of $H^1(G_K, \widehat{J}[\widehat{\phi}])$ and $H^1(G_K, J[2])$ in $(K^*/(K^*)^2)^3$ and $(K^*/(K^*)^2)^5$ as described in Section 3.1, the map $\Phi$ : $H^1(G_K, J[2]) \to H^1(G_K, \widehat{J}[\widehat{\phi}])$ induced from $J[2] \xrightarrow{\phi} \widehat{J}[\widehat{\phi}]$ is given by*

$$(a_1, a_2, a_3, a_4, a_5) \longmapsto (a_1, a_2a_3, a_4a_5).$$

*Proof.* Consider the following commutative diagram whose rows are exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J[2] & \xrightarrow{w_2} & (\mu_2)^5 & \xrightarrow{N} & \mu_2 & \longrightarrow & 0 \\ & & \downarrow{\phi} & & \downarrow{\psi} & & \downarrow{=} & & \\ 0 & \longrightarrow & \widehat{J}[\widehat{\phi}] & \xrightarrow{w_{\hat{\phi}}} & (\mu_2)^3 & \xrightarrow{N} & \mu_2 & \longrightarrow & 0. \end{array}$$

Suppose $P \in J[2]$ maps to $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ via $w_2$. Then $\alpha_i = e_2(P, \{(\omega_i, 0), \infty\})$. Recall that $e_{\hat{\phi}}(\phi(P), P_i) = e_2(P, P_i)$ by the discussion at the end of Section 2.3. This implies that $\phi(P)$ maps to $(\alpha_1, \alpha_2\alpha_3, \alpha_4\alpha_5)$ via $w_{\hat{\phi}}$. Therefore, we can verify that the induced map $\Phi : H^1(G_K, J[2]) \to H^1(G_K, \widehat{J}[\widehat{\phi}])$ under the embeddings in Section 3.1 is given by

$$(a_1, a_2, a_3, a_4, a_5) \longmapsto (a_1, a_2a_3, a_4a_5). \qquad \square$$

**Remark 3.4.** We observe that, under the assumption of this section, we have the following short exact sequence:

$$0 \longrightarrow H^1(G_K, J[\phi]) \longrightarrow H^1(G_K, J[2]) \longrightarrow H^1(G_K, \widehat{J}[\widehat{\phi}]) \longrightarrow 0.$$

Since the Galois action on $J[2]$ is trivial, all linear subspaces are submodules. This implies that the short exact sequence of Galois modules splits (every linear subspace has a complement), which directly implies that all connecting maps are zero. More explicitly the injectivity of the map $H^1(G_K, J[\phi]) \to H^1(G_K, J[2])$ is due to the surjectivity of $J(K)[2] \xrightarrow{\phi} \widehat{J}(K)[\widehat{\phi}]$. For surjectivity of $H^1(G_K, J[2]) \to H^1(G_K, \widehat{J}[\widehat{\phi}])$, observe that the element in $H^1(G_K, \widehat{J}[\widehat{\phi}])$ represented by $(a, b, c)$ has a preimage in $H^1(G_K, J[2])$ represented by $(a, 1, b, 1, c)$ by Proposition 3.3.

**Remark 3.5.** Let $v$ be a place of $K$. We also have the explicit embeddings of $H^1(G_K, J[\phi])$ and $H^1(G_K, J[2])$ described in Section 3.1 as well as the explicit maps given in this section if we replace $K$ with $K_v$ or $K_v^{nr}$.

Using the above three propositions, we now have the explicit formula for the Cassels-Tate pairing in the case of a Richelot isogeny.

**Theorem 3.6.** *Let $J$ be the Jacobian variety of a genus two curve defined over a number field $K$. Suppose all points in $J[2]$ are defined over $K$ and there exists a Richelot isogeny $\phi : J \to \widehat{J}$ where $\widehat{J}$ is the Jacobian variety of another genus two curve. Let $\widehat{\phi}$ be the dual isogeny of $\phi$. Consider $a, a' \in$*

$\mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. *Suppose* $(\alpha'_1, \alpha'_2, \alpha'_3) \in (K^*/(K^*)^2)^3$ *represents* $a'$. *For any place* $v$, *we let* $P_v \in J(K_v)$ *denote a lift of* $a_v \in H^1(G_{K_v}, \widehat{J}[\widehat{\phi}])$ *and suppose* $\delta_2(P_v) \in H^1(G_{K_v}, J[2])$ *is represented by* $(x_{1,v}, x_{2,v}, x_{3,v}, x_{4,v}, x_{5,v}) \in (K_v^*/(K_v^*)^2)^5$. *Then we have*

$$\langle a, a' \rangle_{CT} = \prod_v (x_{2,v}x_{4,v}, \alpha'_1)_v (x_{4,v}, \alpha'_2)_v (x_{2,v}, \alpha'_3)_v,$$

*where* $(\,\cdot\,,\cdot\,)_v$ *represents the Hilbert symbol. Note that here we identify* $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ *with* $\mu_2$.

*Proof.* Suppose $a$ is represented by $(\alpha_1, \alpha_2, \alpha_3) \in (K^*/(K^*)^2)^3$. Then it has a preimage $a_1 \in H^1(G_K, J[2])$ represented by $(\alpha_1, 1, \alpha_2, 1, \alpha_3)$ by Proposition 3.3. So following the definition of $\langle a, a' \rangle_{CT}$, we need to compute $\rho_v \cup_{\phi,v} a'_v \in H^2(G_{K_v}, \overline{K_v}^*)$ where $\rho_v \in H^1(G_{K_v}, J[\phi])$ is a lift of $\delta_2(P_v) - a_{1,v}$ and $\cup_{\phi,v}$ is the cup product induced by $e_\phi$. We know that $\delta_2(P_v) - a_{1,v}$ is in the image of $H^1(G_{K_v}, J[\phi])$, which implies (by Proposition 3.2) that $x_{1,v}/\alpha_1 = 1$, $x_{2,v} = x_{3,v}/\alpha_2$ and $x_{4,v} = x_{5,v}/\alpha_3$. Since $\delta_2(P_v) - a_{1,v}$ is represented by $(x_{1,v}/\alpha_1, x_{2,v}, x_{3,v}/\alpha_2, x_{4,v}, x_{5,v}/\alpha_3) = (1, x_{2,v}, x_{2,v}, x_{4,v}, x_{4,v})$, by Proposition 3.2, $\rho_v$ is represented by $(x_{2,v}x_{4,v}, x_{4,v}, x_{2,v})$. Hence, by Proposition 3.1, we know $\langle a, a' \rangle_{CT} = \sum_v \mathrm{inv}_v((x_{2,v}x_{4,v}, \alpha'_1) + (x_{4,v}, \alpha'_2) + (x_{2,v}, \alpha'_3)) = \prod_v (x_{2,v}x_{4,v}, \alpha'_1)_v (x_{4,v}, \alpha'_2)_v (x_{2,v}, \alpha'_3)_v$. □

## 4. Computational details

In this section, we will describe some further details for the explicit computation of the Cassels-Tate pairing using the formula in Theorem 3.6.

**4.1. Embedding of $\widehat{\mathbf{J}}(\mathbf{K})/\phi(\mathbf{J}(\mathbf{K}))$ and $\mathbf{J}(\mathbf{K})/2\mathbf{J}(\mathbf{K})$.** As discussed in [14, Section 3] [9, Chapter 10 Section 2], the composition of the connecting map $\delta_\phi : \widehat{J}(K)/\phi(J(K)) \to H^1(G_K, J[\phi])$ and the embedding described above $H^1(G_K, J[\phi]) \to (K^*/(K^*)^2)^3$ can be given explicitly as follows. We have

$$\begin{aligned} \mu^\phi : \quad & \widehat{J}(K)/\phi(J(K)) \longrightarrow K^*/(K^*)^2 \times K^*/(K^*)^2 \times K^*/(K^*)^2 \\ & \{(x_1, y_1), (x_2, y_2)\} \longmapsto (L_1(x_1)L_1(x_2), L_2(x_1)L_2(x_2), L_3(x_1)L_3(x_2)) \end{aligned}.$$

Similarly we have the injection:

(4.1)
$$\begin{aligned} \mu^{\hat{\phi}} : \quad & J(K)/\widehat{\phi}(\widehat{J}(K)) \longrightarrow K^*/(K^*)^2 \times K^*/(K^*)^2 \times K^*/(K^*)^2 \\ & \{(x_1, y_1), (x_2, y_2)\} \longmapsto (G_1(x_1)G_1(x_2), G_2(x_1)G_2(x_2), G_3(x_1)G_3(x_2)) \end{aligned}.$$

Note the following special cases. When $x_j$ is a root of $G_i$, then $G_i(x_j)$ should be taken to be $\prod_{l \in \{1,2,3\}\setminus\{i\}} G_l(x_j)$. We have a similar solution when $x_j$ is a root of $L_i$, which is replacing $L_i(x_j)$ with $\Delta \prod_{l \in \{1,2,3\}\setminus\{i\}} L_l(x_j)$. When $(x_j, y_j) = \infty$, then $G_i(x_j)$ is taken to be 1. In the case where one of $L_i$ is linear and $(x_j, y_j) = \infty$, then $L_i(x_j)$ is taken to be 1.

On the other hand, we have a standard injection, which is the composition of the connecting map $\delta_2 : J(K)/2J(K) \to H^1(G_K, J[2])$ and the embedding described above $H^1(G_K, J[2]) \to (K^*/(K^*)^2)^5$. This can also be found in [14, Section 3] [9, Chapter 10 Section 2].

$$\begin{aligned} \mu : \qquad J(K)/2J(K) &\longrightarrow (K^*/(K^*)^2)^5 \\ \{(x_1, y_1), (x_2, y_2)\} &\longmapsto ((x_1 - \omega_1)(x_2 - \omega_1), \ldots, (x_1 - \omega_5)(x_2 - \omega_5)) \end{aligned}.$$

Note the following special cases. When $(x_j, y_j) = (\omega_i, 0)$, then $x_j - \omega_i$ should be taken to be $\lambda \prod_{l \in 1,2,3,4,5 \setminus \{i\}} (\omega_i - \omega_l)$. When $(x_j, y_j) = \infty$, then $x_j - \omega_i$ is taken to be $\lambda$.

Observe the images of the maps $\mu^{\phi}$ and $\mu^{\hat{\phi}}$ are both contained in the kernel of $(K^*/(K^*)^2)^3 \xrightarrow{N} K^*/(K^*)^2$. Similarly, the image of $\mu$ is contained in the kernel of $(K^*/(K^*)^2)^5 \xrightarrow{N} K^*/(K^*)^2$.

**4.2. Bounding the set of bad primes.** The contribution to the formula coming from places outside the finite set of places $S$ for the local Cassels-Tate pairing of $a, a' \in \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$ in Theorem 3.6 vanishes, where $S = \{\text{places of bad reduction for } \mathcal{C}\} \cup \{\text{places dividing } 2\} \cup \{\text{infinite places}\}$. This is explained as follows.

By [17, Chapter I, Section 6] [20, Section 3], we have

$$\mathrm{Sel}^{\phi}(J) \subset H^1(G_K, J[\phi]; S) = \ker \left( H^1(G_K, J[\phi]) \to \prod_{v \notin S} H^1(G_{K_v^{nr}}, J[\phi]) \right).$$

Similarly, $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}) \subset H^1(G_K, \widehat{J}[\widehat{\phi}]; S)$ and $\mathrm{Sel}^2(J) \subset H^1(G_K, J[2]; S)$. It can be shown that $\ker \left(K^*/(K^*)^2 \to \prod_{v \notin S} K_v^{nr*}/(K_v^{nr*})^2\right) = K(S, 2)$, where $K(S,2)$ is defined to be $\{x \in K^*/(K^*)^2 : \mathrm{ord}_v(x) \text{ is even for all } v \notin S\}$. So $\alpha_i, \alpha_i' \in K(S,2)$ for all $i$, where $(\alpha_1, \alpha_2, \alpha_3), (\alpha_1', \alpha_2', \alpha_3') \in (K^*/(K^*)^2)^3$ represent $a, a'$ respectively. Suppose $v \notin S$. Since $a \in H^1(G_K, J[\phi])$ is a global Selmer element, it has a representation where valuation outside $S$ is even, therefore from the explicit formula given in Proposition 3.3, we know there exists a representation of the image of $a_{1,v}$ in $(K_v^*/(K_v^*)^2)^5$ such that all its coordinates have valuation 0. Since $J(K_v^{nr}) \xrightarrow{2} J(K_v^{nr})$ is surjective by [1, Lemma 3.4], the map $H^0(G_{K_v^{nr}}, J) \to H^1(G_{K_v^{nr}}, J[2])$ is the zero map and hence the image of $P_v$ is trivial in $H^1(G_{K_v^{nr}}, J[2])$. This implies that $\delta_2(P_v) \in H^1(G_{K_v}, J[2]) \subset (K_v^*/(K_v^*)^2)^5$ has a representation such that all its coordinates have valuation 0. This implies that $\delta_2(P_v) - a_{1,v} \in H^1(G_{K_v}, J[2]) \subset (K_v^*/(K_v^*)^2)^5$ has a representation such that all its coordinates have valuation 0. Then, by the formula in Proposition 3.2, $\rho_v \in H^1(G_{K_v}, \widehat{J}[\widehat{\phi}]) \subset (K_v^*/(K_v^*)^2)^3$ also has a representation such that all its coordinates have valuation 0. From the first part of the theorem, we know computing $\langle a, a' \rangle_{CT}$ requires computing the Hilbert symbol. It is well-known that the Hilbert symbol between $x$ and $y$ is trivial when the valuations of $x, y$ are both 0 and the local field has odd residue characteristic (for a detailed proof see [24, Lemma 1.4.18]). Hence, the local Cassels-Tate pairing is trivial for all but finitely many places contained in the set $S$.

## 5. Worked Example

We explicitly compute the Cassels-Tate pairing in an example where this improves the rank bound obtained via descent by Richelot isogeny. We will be using the same notation as in Section 2.4 to compute $\langle \cdot, \cdot \rangle_{CT}$ on $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. Our base field $K$ is the field of the rationals, $\mathbb{Q}$.

Let us consider the following genus two curve which is obtained by taking $k = 113$ in [14, Theorem 1]

$$\mathcal{C} : y^2 = (x + 2 \cdot 113)x(x - 6 \cdot 113)(x + 113)(x - 7 \cdot 113),$$

with $G_1 = (x+2\cdot 113), G_2 = x(x-6\cdot 113), G_3 = (x+113)(x-7\cdot 113)$ and

$$\Delta = \begin{bmatrix} 2 \cdot 113 & 1 & 0 \\ 0 & -6 \cdot 113 & 1 \\ -7 \cdot 113^2 & -6 \cdot 113 & 1 \end{bmatrix} = -7 \cdot 113^2,$$

$$\begin{aligned} L_1 &= G_2' G_3 - G_3' G_2 = -14 \cdot 113^2 (x - 3 \cdot 113), \\ L_2 &= G_3' G_1 - G_1' G_3 = (x + 5 \cdot 113)(x - 113), \\ L_3 &= G_1' G_2 - G_2' G_1 = -(x + 6 \cdot 113)(x - 2 \cdot 113). \end{aligned}$$

So we have a Richelot isogeny $\phi$ from $J$, the Jacobian variety of $\mathcal{C}$, to $\widehat{J}$, the Jacobian variety of the following curve.

$$\widehat{\mathcal{C}} : y^2 = -2(x - 3 \cdot 113)(x + 5 \cdot 113)(x - 113)(x + 6 \cdot 113)(x - 2 \cdot 113)$$

It can be shown, using MAGMA [4], that:

$$\begin{aligned} &\mathrm{Sel}^{\hat{\phi}}(\widehat{J}) \\ &= \langle (2\cdot 113, -14\cdot 113, -7), (113, 7, 7\cdot 113), (113, 113, 1), (2, 2, 1), (1, 7, 7) \rangle \\ &\subset (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^3 \end{aligned} \tag{5.1}$$

$$\begin{aligned} &\mathrm{Sel}^{\phi}(J) \\ &= \langle (113, -7 \cdot 113, -7), (2 \cdot 113, 7, 14 \cdot 113), (113, 1, 113) \rangle \\ &\subset (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^3. \end{aligned} \tag{5.2}$$

Now we will compute the Cassels-Tate pairing matrix on $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. Since $(2 \cdot 113, -14 \cdot 113, -7), (113, 7, 7 \cdot 113)$ are images of elements $\{(0,0), (-2 \cdot 113, 0)\}$ and $\{(-2 \cdot 113, 0), (-113, 0)\}$ in $J(\mathbb{Q})/\widehat{\phi}(\widehat{J}(\mathbb{Q}))$ via $\mu^{\hat{\phi}}$ in (4.1), they are in the kernel of the Cassels-Tate pairing. So it is sufficient to look at the pairing on $\langle(113,113,1),(2,2,1),(1,7,7)\rangle \times \langle(113,113,1),(2,2,1),(1,7,7)\rangle$.

Since the primes of bad reduction are $\{2,3,7,113\}$, by Section 4.2, we know these are the only primes which we need to consider in the formula for the Cassels-Tate pairing as in Theorem 3.6. The tables below give details of the local computations at these primes.

Let $a = (113,113,1) \in \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. By the formula given in Proposition 3.3, it has a lift $a_1 = (113,1,113,1,1) \in H^1(G_K, J[2])$. Then for the local calculation, we have the following table:

| place $v$ | $\infty$ | 2 | 3 | 7 | 113 |
|---|---|---|---|---|---|
| $P_v$ | id | id | $\{(0,0),(-113,0)\}$ | id | $\{(0,0),(-2\cdot 113,0)\}$ |
| $\delta_2(P_v)$ | id | id | $(-1,3,-3,-1,-1)$ | id | $(113,\ 3\cdot113,\ 3,\ 1,\ 1)$ |
| $a_{1,v}$ | id | id | $(-1,1,-1,1,1)$ | id | $(113,\ 1,\ 113,\ 1,\ 1)$ |
| $\delta_2(P_v)-a_{1,v}$ | id | id | $(1,3,3,-1,-1)$ | id | $(1,\ 3\cdot113,\ 3\cdot113,\ 1,\ 1)$ |
| $\rho_v$ | id | id | $(-3,-1,3)$ | id | $(3\cdot113,\ 1,\ 3\cdot113)$ |

Now let $a = (2,2,1) \in \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. By the formula given in Proposition 3.3, it has a lift $a_1 = (2,1,2,1,1) \in H^1(G_K, J[2])$. Then for the local calculation, we have the following table:

| place $v$ | $\infty$ | 2 | 3 | 7 | 113 |
|---|---|---|---|---|---|
| $P_v$ | id | $\{(0,0),(-2\cdot 113,0)\}$ | $\{(0,0),(-113,0)\}$ | id | id |
| $\delta_2(P_v)$ | id | $(2,6,3,-1,-1)$ | $(-1,3,-3,-1,-1)$ | id | id |
| $a_{1,v}$ | id | $(2,\ 1,\ 2,\ 1,\ 1)$ | $(-1,1,-1,1,1)$ | id | id |
| $\delta_2(P_v)-a_{1,v}$ | id | $(1,6,6,-1,-1)$ | $(1,3,3,-1,-1)$ | id | id |
| $\rho_v$ | id | $(-6,-1,6)$ | $(-3,-1,3)$ | id | id |

Lastly let $a = (1,7,7) \in \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. By the formula given in Proposition 3.3, it has a lift $a_1 = (1,1,7,1,7) \in H^1(G_K, J[2])$. Then for the local calculation, we have the following table:

| place $v$ | $\infty$ | 2 | 3 | 7 | 113 |
|---|---|---|---|---|---|
| $P_v$ | id | $\{(-2\cdot 113,0),(-113,0)\}$ | id | $\{(-2\cdot 113,0),(-113,0)\}$ | id |
| $\delta_2(P_v)$ | id | $(1,2,-2,-2,2)$ | id | $(1,\ 1,\ 7,\ 7,\ 1)$ | id |
| $a_{1,v}$ | id | $(1,1,-1,1,-1)$ | id | $(1,\ 1,\ 7,\ 1,\ 7)$ | id |
| $\delta_2(P_v)-a_{1,v}$ | id | $(1,2,2,-2,-2)$ | id | $(1,\ 1,\ 1,\ 7,7)$ | id |
| $\rho_v$ | id | $(-1,-2,2)$ | id | $(7,\ 7,\ 1)$ | id |

Following the explicit algorithm for computing the Cassels-Tate pairing, we get that the Cassels-Tate pairing between $(113,113,1)$ and $(2,2,1)$ is the only nontrivial one.

Therefore, we get the $5\times 5$ Cassels-Tate pairing matrix from the 5 generators of $\mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. More specifically, the $ij^{th}$ entry of the matrix is the Cassels-Tate pairing between the $i^{th}$ and the $j^{th}$ generators of $\mathrm{Sel}^{\hat{\phi}}(\widehat{J})$, where the generators are in the same order as listed in the Selmer group $\mathrm{Sel}^{\hat{\phi}}(\widehat{J})$ (5.1).

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

**Remark 5.1.** From the computation above, we have shown that the kernel of the Cassels-Tate pairing has dimension 3. We make the following observations:

- Let $r = \mathrm{rank}(J(\mathbb{Q}))$. We know

$$2^r = \frac{|\widehat{J}(\mathbb{Q})/\phi(J(\mathbb{Q}))| \times |J(\mathbb{Q})/\widehat{\phi}(\widehat{J}(\mathbb{Q}))|}{|J(\mathbb{Q})[\phi]| \times |\widehat{J}(\mathbb{Q})[\widehat{\phi}]|}.$$

  In a standard descent by Richelot isogeny, we have $|\widehat{J}(\mathbb{Q})/\phi(J(\mathbb{Q}))| \leq |\mathrm{Sel}^{\phi}(J)|$ and $|J(\mathbb{Q})/\widehat{\phi}(\widehat{J}(\mathbb{Q}))| \leq |\mathrm{Sel}^{\hat{\phi}}(\widehat{J})|$. Therefore, we get $r \leq 4$. However, after computing the Cassels-Tate pairing, we can bound $r$ via bounding $|J(\mathbb{Q})/\widehat{\phi}(\widehat{J}(\mathbb{Q}))|$ by $|\ker\langle\,\cdot\,,\cdot\,\rangle_{CT}| = 2^3$ instead of $|\mathrm{Sel}^{\hat{\phi}}(\widehat{J})| = 2^5$. This improves the rank bound of $J(\mathbb{Q})$ from 4 to 2.
- Consider the exact sequence (1.1). It can be shown that $\mathrm{Im}\,\alpha$ is contained inside $\ker\langle\,\cdot\,,\cdot\,\rangle_{CT}$, the kernel of the Cassels-Tate pairing on $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$. Indeed, if $a \in \mathrm{Sel}^{\hat{\phi}}(\widehat{J})$ is equal to $\alpha(b)$, where $b \in \mathrm{Sel}^2(J)$, then following the earlier notations, we can let $a_1 = b$. Then we can pick $P_v \in J(\mathbb{Q}_v)$ to be the lift of $a_{1,v}$. Therefore, $\delta_2(P_v) - a_{1,v} = 0 \in H^1(G_{\mathbb{Q}_v}, J[2])$ which implies, $a \in \ker\langle\,\cdot\,,\cdot\,\rangle_{CT}$. Hence, we can always bound $|\mathrm{Sel}^2(J)|$ using $\ker\langle\,\cdot\,,\cdot\,\rangle_{CT}$, and this bound will be sharp when $\mathrm{Im}\,\alpha = \ker\langle\,\cdot\,,\cdot\,\rangle_{CT}$.

  We used MAGMA to compute the size of $\mathrm{Sel}^2(J)$, which is equal to $2^6$, and we have the exact sequence:

$$0 \to J[\phi](\mathbb{Q}) \to J[2](\mathbb{Q}) \to \widehat{J}[\widehat{\phi}](\mathbb{Q}) \to \mathrm{Sel}^{\phi}(J) \to \mathrm{Sel}^2(J) \xrightarrow{\alpha} \ker\langle\,\cdot\,,\cdot\,\rangle_{CT} \to 0.$$

$$\text{size} = 2^2 \quad \text{size} = 2^4 \quad \text{size} = 2^2 \quad \text{size} = 2^3 \quad \text{size} = \mathbf{2^6} \quad \text{size} = 2^3$$

  So for this example, we have turned the descent by Richelot isogeny into a 2-descent via computing the Cassels-Tate pairing.

**Acknowledgments.** I express my sincere and deepest gratitude to my PhD supervisor, Tom Fisher, for his patient guidance and insightful comments at every stage during my research.

## References

[1] A. AGASHE & W. STEIN, "Visibility of Shafarevich–Tate Groups of Abelian Varieties", *J. Number Theory* **97** (2002), no. 1, p. 171-185.
[2] M. VAN BEEK, "Computing the Cassels–Tate Pairing", PhD Thesis, University of Cambridge, 2015.
[3] M. VAN BEEK & T. A. FISHER, "Computing the Cassels–Tate pairing on 3-isogeny Selmer groups via cubic norm equations", *Acta Arith.* **185** (2018), no. 4, p. 367-396.
[4] W. BOSMA, J. CANNON & C. PLAYOUST, "The Magma algebra system. I. The user language", *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265.
[5] N. BRUIN & K. DOERKSEN, "The Arithmetic of Genus Two Curves with $(4,4)$-Split Jacobians", *Can. J. Math.* **63** (2011), no. 5, p. 992-1024.
[6] J. W. S. CASSELS, "Arithmetic on Curves of Genus 1. I. On a conjecture of Selmer", *J. Reine Angew. Math.* **202** (1959), p. 52-99.
[7] ———, "J. W. S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung.", *J. Reine Angew. Math.* **211** (1962), p. 95-112.
[8] ———, "Second Descents for Elliptic Curves", *J. Reine Angew. Math.* **494** (1998), p. 101-127.
[9] J. W. S. CASSELS & E. V. FLYNN, *Prolegomena to a MiddleBrow Arithmetic of Curves of Genus 2*, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, 1996.
[10] S. DONNELLY, "Algorithms for the Cassels–Tate pairing", preprint, 2015.
[11] T. A. FISHER, "The Cassels–Tate pairing and the Platonic solids", *J. Number Theory* **98** (2003), no. 1, p. 105-155.
[12] ———, "On binary quartics and the Cassels–Tate pairing", (2016), preprint.
[13] T. A. FISHER & R. NEWTON, "Computing the Cassels–Tate pairing on the 3-Selmer group of an elliptic curve", *J. Number Theory* **10** (2014), no. 7, p. 18811907.
[14] E. V. FLYNN, "Arbitrarily Large Tate–Shafarevich Group on Abelian Surfaces", *J. Number Theory* **186** (2018), p. 248-258.
[15] P. GILLE & T. SZAMUELY, *Central Simple Algebras and Galois Cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, 2006.
[16] J. S. MILNE, "Abelian Varieties", in *Arithmetic geometry*, Springer, 1986, p. 103-150.
[17] ———, *Arithmetic Duality Theorems*, 2nd ed., BookSurge, 2006, viii+339 pages.
[18] ———, *Abelian Varieties*, 2nd ed., 2008, 166+vi pages.
[19] B. POONEN & M. STOLL, "The Cassels–Tate pairing on polarized abelian varieties", *Ann. Math.* **150** (1999), no. 3, p. 1109-1149.
[20] E. F. SCHAEFER, "2-Descent on the Jacobians of Hyperelliptic Curves", *J. Number Theory* **51** (1995), no. 2, p. 219-232.
[21] J.-P. SERRE, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer, 1979.
[22] K. TAKASHIMA & R. YOSHIDA, "An algorithm for computing a sequence of Richelot isogenies", *Bull. Korean Math. Soc.* **46** (2009), no. 4, p. 789-802.
[23] J. TATE, "Duality theorems in Galois cohomology over number fields", in *Proc. Int. Congr. Math., Stockholm 1962,*, 1963, p. 288-295.
[24] J. YAN, "Computing the Cassels–Tate Pairing for Jacobian Varieties of Genus Two Curves", PhD Thesis, University of Cambridge, 2021.

Jiali YAN
95, Finborough Road
SW10 9DU, London, UK
*E-mail*: jialiyan.lele@gmail.com