Journal of Number Theory 153 (2015) 270–282

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Descent via $(5, 5)$-isogeny on Jacobians of genus 2 curves

E.V. Flynn

Mathematical Institute, University of Oxford, Andrew Wiles Building, Woodstock Road, Oxford OX2 6GG, United Kingdom

ARTICLE INFO

Article history:
Received 18 August 2014
Received in revised form 8 January 2015
Accepted 29 January 2015
Available online 6 March 2015
Communicated by Michael E. Pohst

MSC:
primary 11G30
secondary 11G10, 14H40

Keywords:
Higher genus curves
Jacobians
Tate–Shafarevich group

ABSTRACT

We describe a family of curves $\mathcal{C}$ of genus 2 with a maximal isotropic $(\mathbb{Z}/5)^2$ in $J[5]$, where J is the Jacobian variety of $\mathcal{C}$, and develop the theory required to perform descent via $(5, 5)$-isogeny. We apply this to several examples, where it can be shown that non-reducible Jacobians have nontrivial 5-part of the Tate–Shafarevich group.

1. Introduction

In this article we construct a family of curves $\mathcal{C}$ of genus 2 over a field k of characteristic not 2 or 3, with Jacobian J, where $J[5](\bar{k})$ contains a group Σ of order 25 which is defined over k. As we show in Section 2, when $\mathcal{C}$ has the form

$$y^2 = F(x) = \lambda G(x)^2 + H(x)^5, \tag{1}$$

E-mail address: flynn@maths.ox.ac.uk.

http://dx.doi.org/10.1016/j.jnt.2015.01.018

where $G(x)$ is quadratic and $H(x)$ is linear in x, then the divisor $D = [(x_0, \sqrt{\lambda}G(x_0)) - \infty]$, where x_0 is the root of $H(x)$ and ∞ is the point at infinity on the curve, represents a point in $J[5](\bar{k})$, as can be seen from the fact that $5D$ is linearly equivalent to the divisor of the function $y - \sqrt{\lambda}G(x)$. Furthermore the group generated by D is defined over k.

In Section 2, we shall describe curves which can be written in the form (1) in two ways, such that $\Sigma \subset J[5]$ is maximally isotropic with respect to the Weil pairing, so that $\widetilde{J} = J/\Sigma$ is also principally polarized and in fact has a $\Sigma^\vee$-level structure. In Section 3, we shall give an explicit family of such curves and in Section 4 we identify a curve $\widetilde{\mathcal{C}}_r$ such that its Jacobian $\widetilde{J}_r$ is J_r/Σ. This gives rise to a $(5,5)$-isogeny $\phi : J_r \mapsto \widetilde{J}_r$, defined over k, and a dual isogeny $\tilde{\phi} : \widetilde{J}_r \mapsto J_r$ such that $\tilde{\phi} \circ \phi = [5]$. The explicit derivation of the model of $\widetilde{\mathcal{C}}_r$ and the isogeny ϕ will require some significant computation on the Kummer surface.

In Section 5, we describe explicitly how to perform a descent via $(5,5)$-isogeny, which allows us to compute a bound on the rank on $J(k)$, and to obtain information about $Ш(J/k)[5]$, using ideas from [3] and [6]. This allows us to give an example of an absolutely simple abelian surface with nontrivial elements of $Ш(J/\mathbb{Q})[5]$; as far as we are aware, this is the first such known example.

The broad strategy will be similar to that developed for $(3,3)$-isogenies in [2], using maps on the Kummer surface, but with considerably greater computational complexity, due to the larger dimensional space of quintics required here and the fact that, for our family, the members of the kernel are not individually defined over $\mathbb{Q}$. We shall also, in our second example, use a finesse in which a nontrivial element of $Ш(J/\mathbb{Q})[5]$ is exhibited using the easier direction of the $(5,5)$-isogeny which requires only quadratic number fields for the descent map.

2. Five-torsion on genus two Jacobians

Let k be a field of characteristic different from 2, 3 and let $\mathcal{C}$ be a smooth projective curve of genus 2 over k given by an affine model

$$\mathcal{C}: y^2 = F(x),$$

where $F(x) \in k[x]$ is of degree 5 or 6 (this only mildly restricts the admissible $\mathcal{C}$ if k is a finite field of 5 elements). Let J be the Jacobian of $\mathcal{C}$. The group $J(k)$ is isomorphic to the group of divisor classes of k-rational degree 0 divisors on $\mathcal{C}$. Since $\mathcal{C}$ is of genus 2, every degree 0 class contains a representative of the form

$$D - \kappa,$$

where D is an effective divisor of degree 2 and κ is an effective canonical divisor. Furthermore, for any non-principal class, the divisor D is unique. In the following, our curves will all have $F(x)$ of degree 5 and we shall take $\kappa = 2\infty$.

Lemma 1. *Let $\mathcal{C}$ be a curve of genus 2 of the form*

$$\mathcal{C}: y^2 = F(x) = \lambda_1 G_1(x)^2 + H_1(x)^5 = \lambda_2 G_2(x)^2 + H_2(x)^5,$$

where $H_1, H_2, G_1, G_2, F \in k[x]$, $\lambda_1, \lambda_2 \in k^\times$, G_1, G_2 are of degree 2, H_1, H_2 are of degree 1 and $\gcd(H_1, H_2) = 1$. Then $\mathrm{Pic}(\mathcal{C}/\bar{k})[5]$ has a subgroup Σ of size 25 which is defined over k.

Proof. For each $i = 1, 2$, let x_i be the root of H_i, and let $T_i = [\big(x_i, \sqrt{\lambda_i}\, G_i(x_i)\big) - \infty]$. By considering the divisor of the function $y - \sqrt{\lambda_i} G_i(x_i)$ we see that $5T_i = \mathcal{O}$, the identity, and T_i has order 5. Furthermore, $\langle T_i \rangle$, the group generated by T_i, is:

$$\begin{aligned}
0T_i &= \mathcal{O},\\
1T_i &= [\big(x_i, \sqrt{\lambda_i} G_i(x_i)\big) - \infty],\\
2T_i &= [2\big(x_i, \sqrt{\lambda_i} G_i(x_i)\big) - 2\infty],\\
3T_i &= [2\big(x_i, -\sqrt{\lambda_i} G_i(x_i)\big) - 2\infty],\\
4T_i &= [\big(x_i, -\sqrt{\lambda_i} G_i(x_i)\big) - \infty],
\end{aligned}$$

so that $\langle T_i \rangle$ is defined over k. Furthermore $T_2 \notin \langle T_1 \rangle$, so that $\langle T_1, T_2 \rangle$ is of order 25 and is defined over k. □

The torsion subgroup scheme $J[5]$ comes equipped with a non-degenerate, bilinear, alternating *Weil pairing*

$$e_5: J[5] \times J[5] \to \mu_5,$$

where μ_5 is the group scheme representing the fifth roots of unity.

We say that a subgroup $\Sigma \subset J[5]$ is *isotropic* if e_5 restricts to the trivial pairing on Σ. If Σ is of degree 25 then Σ is *maximal isotropic*, meaning Σ is not properly contained in an isotropic subgroup. From the properties of the Weil pairing, there is an induced isomorphism $J[5]/\Sigma \to \Sigma^\vee = \mathrm{Hom}(\Sigma, \mu_5)$. In fact, we have a direct sum decomposition $J[5] = \Sigma \times \Sigma^\vee$. In particular, if $\Sigma = \mathbb{Z}/5 \times \mathbb{Z}/5$ then we have $\Sigma^\vee = \mu_5 \times \mu_5$. The isotropy guarantees that J/Σ is principally polarized.

Ed Schaefer has communicated the following lemma and proof, which gives the required property of the Weil pairing in our case.

Lemma 2. *Let p be an odd prime, k be a field of characteristic 0, $\mathcal{C}/k$ be a curve of genus greater than 1, $\mathcal{C}(k) \neq \emptyset$, J be its Jacobian, $\alpha, \beta \in J[p]$ and $\mu_p \nsubseteq K(\alpha, \beta)$ (the minimal field of definition of α and β over k). Then $e_p(\alpha, \beta) = 1$.*

Proof. Since $\mathcal{C}(k) \neq \emptyset$ there are degree 0 divisors D_α and D_β, defined over $K(\alpha)$ and $K(\beta)$ respectively, with disjoint supports, such that $\alpha = [D_\alpha]$ and $\beta = [D_\beta]$. There are

also functions f_α and f_β, defined over $K(\alpha)$ and $K(\beta)$ respectively, such that $\mathrm{divis}(f_\alpha) = pD_\alpha$ and $\mathrm{divis}(f_\beta) = pD_\beta$. Using the Weil reciprocity definition of the Weil pairing on a Jacobian, we have $e_p(\alpha,\beta) = f_\beta(D_\alpha)/f_\alpha(D_\beta)$ and $e_p(\alpha,\beta) \in K(\alpha,\beta) \cap \mu_p = \{1\}$. □

The above motivates that we should expect to be able to find an isogenous Jacobian. In Sections 3, 4 we shall find a family of curves $\mathcal{C}_r$ and $\widetilde{\mathcal{C}}_r$, and the computation in Section 4 will show independently that there is an isogeny between the Jacobians J_r and $\widetilde{J}_r$ with kernel Σ.

3. A family of genus 2 curves with a maximal isotropic $(\mathbb{Z}/5)^2$ in $J[5]$

Let k be a field of characteristic different from 2, 3 and let $r \in k$. In this section we derive a genus 2 curve $\mathcal{C}_r$ over k with two non-trivial divisor classes $T_1, T_2 \in \mathrm{Pic}(\mathcal{C}_r/k)[5]$ with $T_1 \notin \langle T_2 \rangle$ and $e_5(T_1,T_2) = 1$.

In order for $\mathcal{C}$ to have the form given in Lemma 1, we shall apply a linear transformation to map the roots of H_1, H_2 to r, 0, respectively, and assume $H_1(x) = x - r$, $H_2(x) = x$. Then $\lambda_1 G_1(x)^2 + H_1(x)^5 = \lambda_2 G_2(x)^2 + H_2(x)^5$. Let $F_i(x) = \sqrt{\lambda_i} G_i(x)$ so that $F_1(x)^2 + H_1(x)^5 = F_2(x)^2 + H_2(x)^5$. Then

$$\big(F_1(x) + F_2(x)\big)\big(F_1(x) - F_2(x)\big) = x^5 - (x-r)^5 = w_1 w_2,$$

where

$$w_1 = \frac{\sqrt{r}}{2}\big((5+\sqrt{5})x^2 - r(5+\sqrt{5})x + 2r^2\big),$$
$$w_2 = \frac{\sqrt{r}}{2}\big((5-\sqrt{5})x^2 - r(5-\sqrt{5})x + 2r^2\big).$$

A natural approach here would be to solve F_1, F_2 for $F_1 + F_2 = w_1$, $F_1 - F_2 = w_2$, that is, $F_1 = (w_1 + w_2)/2$ and $F_2 = (w_1 - w_2)/2$. This gives:

$$F_1(x) = \frac{\sqrt{r}}{2}\big(5x^2 - 5rx + 2r^2\big), \quad F_2(x) = \frac{\sqrt{5r}}{2}x(x-r).$$

These are each of the required type, and they satisfy the required $F_1(x)^2 + (x-r)^5 = F_2(x)^2 + x^5$, but $y^2 = F_1(x)^2 + (x-r)^5 = F_2(x)^2 + x^5$ has a repeated root at 0, and so is not of genus 2.

Instead we vary the above idea, by taking any unit u in the ring of integers of $\mathbb{Q}(\sqrt{5})$, such as $u = (1+\sqrt{5})/2$, and now adjust by taking: $v_1 = uw_1$ and $v_2 = (1/u)w_2$. We now take $F_1 = (v_1 + v_2)/2$ and $F_2 = (v_1 - v_2)/2$, so that $F_1^2 - F_2^2 = v_1 v_2 = w_1 w_2$. This gives

$$F_1(x) = \frac{\sqrt{5r}}{2}(3x^2 - 3rx + r^2), \quad F_2(x) = \frac{\sqrt{r}}{2}(5x^2 - 5rx + r^2).$$

So, now we have $y^2 = F_1(x)^2 + (x-r)^5 = F_2(x)^2 + x^5$ satisfying our requirements. In order to clear denominators, we replace x, y with $x/4$, $y/2$, giving

$$\begin{aligned}\mathcal{C}_r : y^2 &= 5r(3x^2 - 12rx + 16r^2)^2 + (x-4r)^5 \\ &= r(5x^2 - 20rx + 16r^2)^2 + x^5.\end{aligned}$$

This can be summarized as follows.

Lemma 3. *Let* $G_1(x) = 3x^2 - 12rx + 16r^2$, $G_2(x) = 5x^2 - 20rx + 16r^2$, $\lambda_1 = 5r$, $\lambda_2 = r$, $H_1(x) = x - 4r$ *and* $H_2(x) = x$, *for* $r \in k^\times$. *Then*

$$\mathcal{C}_r\colon y^2 = F(x) = \lambda_1 G_1(x)^2 + H_1(x)^5 = \lambda_2 G_2(x)^2 + H_2(x)^5,$$

has $T_1 = [(4r, 16r^2\sqrt{5r}) - \infty]$, $T_2 = [(0, 16r^2\sqrt{r}) - \infty]$ *in* $J[5]$, *with* $\langle T_1, T_2\rangle$ *defined over* k.

We note also that the curve $\mathcal{C}_1$ can be shown to have absolutely simple Jacobian, using the technique in [7] at the prime 19. Since this is a family of quadratic twists, they are geometrically the same curve, and so each $\mathcal{C}_r$ has absolutely simple Jacobian.

4. The isogeny

We consider the curve $\mathcal{C}_r$ as defined in Lemma 3 and its Jacobian J_r. In this section we determine a curve $\widetilde{\mathcal{C}_r}$ whose Jacobian $\widetilde{J_r}$ is isogenous to J_r via an isogeny $\phi : J_r \to J_r/\Sigma$, where $\Sigma = \langle T_1, T_2\rangle$. We do so by determining the corresponding map between their Kummer surfaces.

For $\mathcal{C}$ a general curve of genus 2 given by a model

$$\mathcal{C}\colon y^2 = f_6x^6 + f_5x^5 + \cdots + f_0,$$

with Jacobian J, we follow [4, p. 17] and choose a particular set of coordinates for the Kummer surface, given by $\xi = \xi(D) = \xi_0, \ldots, \xi_3$ as functions on J in terms of a divisor class $D = [(x_1, y_1) + (x_2, y_2) - \kappa]$ on $\mathcal{C}$ as follows.

$$\begin{gathered}\xi_0 = 1, \quad \xi_1 = x_1 + x_2, \quad \xi_2 = x_1x_2, \quad \xi_3 = \frac{\Phi(\xi_0, \xi_1, \xi_2) - 2y_1y_2}{\xi_1^2 - 4\xi_0\xi_2}, \text{ where} \\ \Phi(\xi_0, \xi_1, \xi_2) = 2f_0\xi_0^3 + f_1\xi_0^2\xi_1 + 2f_2\xi_0^2\xi_2 + f_3\xi_0\xi_1\xi_2 + 2f_4\xi_0\xi_2^2 + f_5\xi_2^2\xi_1 + 2f_6\xi_2^3.\end{gathered} \tag{2}$$

The quartic equation for the model of $\mathcal{K}$ arising from these coordinates has the shape

$$\mathcal{K}\colon (\xi_1^2 - 4\xi_0\xi_2)\xi_3^2 + \Phi(\xi_0, \xi_1, \xi_2)\xi_3 + \Psi(\xi_0, \xi_1, \xi_2) = 0,$$

where $\Psi(\xi_0,\xi_1,\xi_2)$ is a quartic form we do not need explicitly here. The important observation is that one can read off the coefficients $f_0,\dots,f_6$ directly from Φ and thus recover $\mathcal{C}$ from it.

Let $\mathcal{C}=\mathcal{C}_r$. In order to produce Σ-invariant forms on $\mathcal{K}_r$, we use biquadratic forms from [4, p. 23], arising from the addition structure on J_r. For $i,j=0,\dots,3$ we have forms

$$B_{i,j}\in k[\xi_0,\dots,\xi_3,\xi'_0,\dots,\xi'_3],$$

biquadratic in $(\xi_0,\dots,\xi_3)$ and $(\xi'_0,\dots,\xi'_3)$ such that for points D_1, D_2 on J_r we have, as projective matrices,

$$\Big(\xi_i(D_1+D_2)\,\xi_j(D_1-D_2)+\xi_i(D_1-D_2)\,\xi_j(D_1+D_2)\Big)=\Big(B_{ij}(\xi(D_1),\xi(D_2))\Big). \tag{3}$$

Let $T_1,T_2\in J_r[5]$ be as in Lemma 3, that generate Σ, write $\xi(T_1),\xi(T_2)$ for the coordinate vectors of their images on the quartic model of $\mathcal{K}_r$ and define

$$\begin{aligned}
R_{ij}(\xi_0,\dots,\xi_3)&=B_{ij}\big(\xi_0,\dots,\xi_3,\xi(T_1)\big),\\
S_{ij}(\xi_0,\dots,\xi_3)&=B_{ij}\big(\xi_0,\dots,\xi_3,\xi(T_2)\big),\\
R'_{ij}(\xi_0,\dots,\xi_3)&=B_{ij}\big(\xi_0,\dots,\xi_3,\xi(2T_1)\big),\\
S'_{ij}(\xi_0,\dots,\xi_3)&=B_{ij}\big(\xi_0,\dots,\xi_3,\xi(2T_2)\big).
\end{aligned} \tag{4}$$

We see that the quintic forms

$$\begin{aligned}
R_{ijkl}=\;&\xi_iR_{jk}R'_{lm}+\xi_iR_{jl}R'_{km}+\xi_iR_{jm}R'_{kl}\\
&+\xi_iR_{kl}R'_{jm}+\xi_iR_{km}R'_{jl}+\xi_iR_{lm}R'_{jk}\\
&+\xi_jR_{ik}R'_{lm}+\xi_jR_{il}R'_{km}+\xi_jR_{im}R'_{kl}\\
&+\xi_jR_{kl}R'_{im}+\xi_jR_{km}R'_{il}+\xi_jR_{lm}R'_{ik}\\
&+\xi_kR_{ji}R'_{lm}+\xi_kR_{jl}R'_{im}+\xi_kR_{jm}R'_{il}\\
&+\xi_kR_{il}R'_{jm}+\xi_kR_{im}R'_{jl}+\xi_kR_{lm}R'_{ji}\\
&+\xi_lR_{jk}R'_{im}+\xi_lR_{ji}R'_{km}+\xi_lR_{jm}R'_{ki}\\
&+\xi_lR_{ki}R'_{jm}+\xi_lR_{km}R'_{ji}+\xi_lR_{im}R'_{jk}\\
&+\xi_mR_{jk}R'_{li}+\xi_mR_{jl}R'_{ki}+\xi_mR_{ji}R'_{kl}\\
&+\xi_mR_{kl}R'_{ji}+\xi_mR_{ki}R'_{jl}+\xi_mR_{li}R'_{jk},
\end{aligned}$$

with $i,j,k,l\in\{0,\dots,3\}$, are invariant under translation by T_1. Similarly the forms S_{ijkl}, defined as above but with each R, R' replaced by S, S', are invariant under translation

by T_2. The R_{ijk} and S_{ijk} each generate spaces of dimension 12 that intersect in a space of dimension 4. This intersection provides us with a map on the Kummer surface of J_r.

We find a basis $\tilde{\xi}_0, \ldots, \tilde{\xi}_3$ for $\phi^*(\mathcal{O}_{\tilde{J}_r}(2\Theta_{\tilde{J}_r}))$ that is the pullback of a basis of the type described by (2). We can then read off the curve $\widetilde{\mathcal{C}}_r$, at least up to quadratic twist, from the resulting equation for $\widetilde{\mathcal{K}}_r$. The basis choice can largely be characterized by the order of vanishing of each ξ_i at the identity element. This leads us to conclude that, up to scalar multiples, we should take the basis choice

$$\begin{aligned}\tilde{\xi}_0 &= (1\xi_0 + 0\xi_1 + 0\xi_2)\xi_3^4 + \cdots,\\ \tilde{\xi}_1 &= (0\xi_0 + 1\xi_1 + 0\xi_2)\xi_3^4 + \cdots,\\ \tilde{\xi}_2 &= (0\xi_0 + 0\xi_1 + 1\xi_2)\xi_3^4 + \cdots.\end{aligned}$$

The determination of $\tilde{\xi}_3$ is a little more involved. The resulting quintic forms are too large to reproduce here, but we have made them available electronically at [5]. We can then find the quartic satisfied by these quintic forms, and read the equation of $\widetilde{\mathcal{C}}_r$, up to a quadratic twist, from its Kummer surface equation. We can then find the correct twist by applying the map to a member of $J_r(\mathbb{Q})$. This gives the following result, shown in the Maple file at [5].

Theorem 4. *Let $\mathcal{C}_r$ be as described by Lemma 3. Then $\widetilde{J}_r = J_r/\Sigma$ is the Jacobian of the genus 2 curve*

$$\widetilde{\mathcal{C}}_r\colon y^2 = \tilde{\lambda}_1\widetilde{G}_1(x)^2 + \widetilde{H}_1(x)^5 = \tilde{\lambda}_2\widetilde{G}_2(x)^2 + \widetilde{H}_2(x)^5,$$

where $\widetilde{G}_1(x) = x^2+100r^2(15+4\sqrt{5})$, $\widetilde{G}_2(x) = x^2+100r^2(15-4\sqrt{5})$, $\tilde{\lambda}_1 = 25r(-5+2\sqrt{5})$, $\tilde{\lambda}_2 = 25r(-5-2\sqrt{5})$, $\widetilde{H}_1(x) = x - 10r\sqrt{5}$, $\widetilde{H}_2(x) = x + 10r\sqrt{5}$. The curve $\mathcal{C}_r$ is defined over k, and there is a $(5,5)$-isogeny $\phi : J_r \mapsto \widetilde{J}_r$, defined over k with kernel $\langle T_1, T_2\rangle$. The dual isogeny $\tilde{\phi} : \widetilde{J}_r \mapsto J_r$ has kernel $\langle \widetilde{T}_1, \widetilde{T}_2\rangle$, where

$$\begin{aligned}\widetilde{T}_1 &= [\big(10r\sqrt{5}, 2000r^2\sqrt{10r(-5+\sqrt{5})}\big) - \infty],\\ \widetilde{T}_2 &= [\big(-10r\sqrt{5}, 2000r^2\sqrt{10r(-5-\sqrt{5})}\big) - \infty].\end{aligned}$$

5. Isogeny descent

Galois cohomology associates with an isogeny

$$0 \to J[\phi] \to J \xrightarrow{\phi} \widetilde{J} \to 0$$

between abelian varieties over a field k an exact sequence

$$0 \to \widetilde{J}(k)/\phi J(k) \xrightarrow{\gamma} H^1(k, J[\phi]) \to H^1(k, J).$$

For k a number field and v a place of k, we consider the completion k_v and its separable closure k_v^{sep} and identify $\mathrm{Gal}(k_v^{\mathrm{sep}}/k_v)$ with a relevant decomposition group inside $\mathrm{Gal}(k^{\mathrm{sep}}/k)$. This allows us to consider restriction maps $\mathrm{res}_v\colon H^i(k,.) \to H^i(k_v,.)$. Writing γ_v for the relevant connecting homomorphism over the base field k_v, this allows us to define the *Selmer group*

$$\mathrm{Sel}^{\phi}(J/k) = \{\delta \in H^1(k, J[\phi]) : \mathrm{res}_v(\delta) \in \mathrm{im}\gamma_v \text{ for all places } v \text{ of } k\}. \tag{5}$$

The Selmer group contains the image of γ. If this containment is strict then part of the Selmer group represents non-trivial elements in $Ш(J/k)$. To be precise, we have

$$0 \to \widetilde{J}(k)/\phi J(k) \to \mathrm{Sel}^{\phi}(J/k) \to Ш(J/k)[\phi] \to 0.$$

Therefore, the computation of Selmer groups can be used to exhibit non-trivial elements in Tate–Shafarevich groups.

Lemma 5. *Let $\mathcal{C}_r$ and $\widetilde{\mathcal{C}_r}$ be as in Lemma 3 and Theorem 4, with Jacobians J_r, $\widetilde{J_r}$, and $(5,5)$-isogenies $\phi : J_r \to \widetilde{J_r}$, $\tilde{\phi}\colon \widetilde{J_r} \to J_r$. Then there is a homomorphism*

$$\begin{aligned} q\colon \widetilde{J_r}(k)/\phi J_r(k) &\longmapsto ((k[t]/(t^4+10rt^2+5r^2))^*/((k[t]/(t^4+10rt^2+5r^2))^*)^5)^{\times 2} \\ &= k\Big(\sqrt{r(-5+2\sqrt{5})}\Big)^*/\Big(k\Big(\sqrt{r(-5+2\sqrt{5})}\Big)^*\Big)^5 \\ &\quad \times k\Big(\sqrt{r(-5-2\sqrt{5})}\Big)^*/\Big(k\Big(\sqrt{r(-5-2\sqrt{5})}\Big)^*\Big)^5 \end{aligned}$$

given by $[P_1 + P_2 - 2\infty] \mapsto \gamma(P_1)\gamma(P_2)$, where

$$\begin{aligned} \gamma : (x,y) \longmapsto [&y - 5\sqrt{r(-5+2\sqrt{5})}\,(x^2 + (15+4\sqrt{5})100r^2), \\ &y - 5\sqrt{r(-5-2\sqrt{5})}\,(x^2 + (15-4\sqrt{5})100r^2)]. \end{aligned}$$

Similarly

$$\begin{aligned} \tilde{q}\colon J_r(k)/\tilde{\phi}\widetilde{J_r}(k) &\longmapsto (k[t]/(t^2-5r))^*/((k[t]/(t^2-5r))^*)^5 \\ &\quad \times (k[t]/(t^2-r))^*/((k[t]/(t^2-r))^*)^5 \\ &= k(\sqrt{5r})^*/(k(\sqrt{5r})^*)^5 \times k(\sqrt{r})^*/(k(\sqrt{r})^*)^5 \end{aligned}$$

is given by $[P_1 + P_2 - 2\infty] \mapsto \tilde{\gamma}(P_1)\tilde{\gamma}(P_2)$, where

$$\begin{aligned} \tilde{\gamma} : (x,y) \longmapsto [&y - \sqrt{5r}(3x^2 - 12rx + 16r^2), \\ &y - \sqrt{r}(5x^2 - 20rx + 16r^2)]. \end{aligned}$$

The image of q is in the kernel of the norm map to $k(\sqrt{5})^*/(k(\sqrt{5})^*)^5 \times k(\sqrt{5})^*/(k(\sqrt{5})^*)^5$. The image of $\tilde{q}$ is in the kernel of the norm map to $k^*/(k^*)^5 \times k^*/(k^*)^5$. For any completion k_v, we let

$$\begin{aligned} j_v : &\left((k[t]/(t^4+10rt^2+5r^2))^*/((k[t]/(t^4+10rt^2+5r^2))^*)^5\right)^{\times 2} \\ &\longrightarrow \left((k_v[t]/(t^4+10rt^2+5r^2))^*/((k_v[t]/(t^4+10rt^2+5r^2))^*)^5\right)^{\times 2} \end{aligned}$$

and

$$\begin{aligned} \tilde{j}_v : &(k[t]/(t^2-5r))^*/((k[t]/(t^2-5r))^*)^5 \times (k[t]/(t^2-r))^*/((k[t]/(t^2-r))^*)^5 \\ &\longrightarrow (k_v[t]/(t^2-5r))^*/((k_v[t]/(t^2-5r))^*)^5 \times (k_v[t]/(t^2-r))^*/((k_v[t]/(t^2-r))^*)^5 \end{aligned}$$

be the natural maps. Let q_v be the map on $\widetilde{J}_r(k_v)/\phi(J_r(k_v))$ and $\tilde{q}_v$ the map on $J_r(k_v)/\tilde{\phi}(\widetilde{J}_r(k_v))$, the local versions of q, $\tilde{q}$. Then the Selmer groups can be described explicitly as the intersections over v of $j_v^{-1}(q_v(\widetilde{J}_r(k_v)/\phi(J_r(k_v))))$ and $\tilde{j}_v^{-1}(\tilde{q}_v(J_r(k_v)/\tilde{\phi}(\widetilde{J}_r(k_v))))$.

Proof. This is a direct application of the theory developed in [3] and [6]. □

We take S to be the set of primes consisting of 5 and the primes of bad reduction of $\mathcal{C}_r$. By [3, Proposition 9.2], the Selmer groups lie in the subgroups that are unramified outside S. We can represent those using S-units in the above number fields. Note that, for any curve in our family, the descent can be performed using at worst quartic number fields. This already provides us with explicit finite groups that contain the Selmer groups. The remaining conditions come from the local images at $v \in S$ (note that $\mathbb{R}^\times/\mathbb{R}^{\times 5}$ is trivial, so the archimedian place does not provide any information). With the explicit description of the maps q_v and $\tilde{q}_v$ we can generate elements in their images. Suppose now that $k = \mathbb{Q}$. Using [6, Lemma 3.8, Proposition 3.9] we have

$$\#\widetilde{J}_r(\mathbb{Q}_v)/\phi(J_r(\mathbb{Q}_v))\,\#J_r(\mathbb{Q}_v)/\tilde{\phi}(\widetilde{J}_r(\mathbb{Q}_v)) = \frac{\#J_r[\phi](\mathbb{Q}_v)\,\#\widetilde{J}_r[\tilde{\phi}](\mathbb{Q}_v)}{|5|_p^2}. \tag{6}$$

So we know when we have found enough elements to generate the entire image. By explicitly computing the restrictions j_v and $\tilde{j}_v$, we can compute the Selmer groups using essentially the definition in (5).

We now give two examples. The first example will illustrate a situation where a $(5,5)$-isogeny descent gives a rank bound of 0; this is the same as the bound obtained by a complete 2-descent, but it only requires easier computations over fields of smaller degree. The second example has a nonzero rank bound for the $(5,5)$-isogeny descent (which can be shown, using only the easier direction of the isogeny for which only a quadratic number field is required for the Cassels map), and a rank bound of 0 for complete 2-descent, giving a nontrivial element in $Ш(J/\mathbb{Q})[5]$. The computations involved in these examples are given in detail at the end of the Maple file at [5].

Example 6. Let J_1 be the Jacobian of the curve

$$\mathcal{C}_1 \colon y^2 = 5(3x^2 - 12x + 16)^2 + (x-4)^5 = (5x^2 - 20x + 16)^2 + x^5.$$

Then $J_1(\mathbb{Q})$ has a rank bound of 0 using descent via $(5,5)$-isogeny.

Proof. For $r = 1$, we have

$$\begin{aligned}\widetilde{\mathcal{C}_1} : y^2 &= 25(-5 + 2\sqrt{5})(x^2 + 100(15 + 4\sqrt{5}))^2 + (x - 10\sqrt{5})^5 \\ &= 25(-5 - 2\sqrt{5})(x^2 + 100(15 - 4\sqrt{5}))^2 + (x + 10\sqrt{5})^5,\end{aligned}$$

also defined over $\mathbb{Q}$. We note here that the quartic number field can be identified with $\mathbb{Q}(\zeta_5)$, and so we shall express our maps in terms of elements of this field. The kernel of $\phi : J_1 \to \widetilde{J_1}$ is generated by

$$\begin{aligned}T_1 &= [(4, 16\sqrt{5}) - \infty], \\ T_2 &= [(0, 16) - \infty].\end{aligned}$$

The kernel of $\tilde{\phi} : \widetilde{J_1} \to J_1$ is generated by

$$\begin{aligned}\widetilde{T_1} &= [\big(10(1 + 2\zeta_5 + 2\zeta_5^4), 4000(2 + 4\zeta_5 + \zeta_5^2 + 3\zeta_5^3)\big) - \infty] \\ \widetilde{T_2} &= [\big(10(-1 - 2\zeta_5 - 2\zeta_5^4), 4000(1 + 2\zeta_5 + 3\zeta_5^2 - \zeta_5^3\big) - \infty]\end{aligned}$$

Then, for $r = 1$,

$$q \colon \widetilde{J_1}(k)/\phi J_1(k) \longmapsto \mathbb{Q}(\zeta_5)^*/(\mathbb{Q}(\zeta_5)^*)^5 \times \mathbb{Q}(\zeta_5)^*/(\mathbb{Q}(\zeta_5)^*)^5$$

is given by $[P_1 + P_2 - 2\infty] \mapsto \gamma(P_1)\gamma(P_2)$, where

$$\begin{aligned}\gamma : (x,y) \longmapsto [&y - 5(1 + 2\zeta_5 + 2\zeta_5^3)(x^2 + 100(15 + 4(1 + 2\zeta_5 + 2\zeta_5^4))), \\ &y - 5(1 + 2\zeta_5 + 2\zeta_5^2)(x^2 + 100(15 - 4(1 + 2\zeta_5 + 2\zeta_5^4)))].\end{aligned}$$

Similarly

$$\tilde{q} \colon J_1(k)/\tilde{\phi}\widetilde{J_1}(k) \longmapsto \mathbb{Q}(\sqrt{5})^*/(\mathbb{Q}(\sqrt{5})^*)^5 \times \mathbb{Q}^*/(\mathbb{Q}^*)^5$$

is given by $[P_1 + P_2 - 2\infty] \mapsto \tilde{\gamma}(P_1)\tilde{\gamma}(P_2)$, where

$$\begin{aligned}\tilde{\gamma} : (x,y) \longmapsto [&y - \sqrt{5}(3x^2 - 12x + 16), \\ &y - (5x^2 - 20x + 16)].\end{aligned}$$

The only bad primes are 2, 5, ∞. The units of $\mathbb{Q}(\zeta_5)$ are generated by $-\zeta_5$, $1+\zeta_5$, and -1 is trivial modulo fifth powers, so we can replace $-\zeta_5$ with ζ_5. The primes above 2, 5 are 2, $1-\zeta_5$, so

$$\mathrm{im}(q) \subseteq \langle [\zeta_5, 1], [1+\zeta_5, 1], [2, 1], [1-\zeta_5, 1], [1, \zeta_5], [1, 1+\zeta_5], [1, 2], [1, 1-\zeta_5] \rangle.$$

Note that the norms from $\mathbb{Q}(\zeta_5)$ to $\mathbb{Q}(\sqrt{5})$ of ζ_5, $1+\zeta_5$, 2, $1-\zeta_5$ are 1, $(3+\sqrt{5})/2$, 4, $(5-\sqrt{5})/2$. After taking into account that the image of q is contained in the kernel of the norm map to $\mathbb{Q}(\sqrt{5})^*/(\mathbb{Q}(\sqrt{5})^*)^5$, we can reduce to $\langle [\zeta_5, 1], [1, \zeta_5] \rangle$. After taking into account that the second component of q is the image of the first component under $\zeta_5 \mapsto \zeta_5^2$, we see that in fact

$$\mathrm{im}(q) \subseteq \langle [\zeta_5, \zeta_5^2] \rangle.$$

The units of $\mathbb{Q}(\sqrt{5})$ are generated by $(1-\sqrt{5})/2$ and the primes above 2, 5 are 2, $\sqrt{5}$, so the first component of $\tilde{q}$ is contained in $\langle (1-\sqrt{5})/2, 2, \sqrt{5} \rangle$. These have norms -1, 4, -5, so that in fact the first component is contained in $\langle (1-\sqrt{5})/2 \rangle$. The second component of $\tilde{q}$ is contained in $\langle 2, 5 \rangle$. Hence

$$\mathrm{im}(\tilde{q}) \subseteq \langle [(1+\sqrt{5})/2, 1], [1, 2], [1, 5] \rangle.$$

Taking into account that $\#J_1[5](\mathbb{Q}) = 5$, we already have an a priori bound of 3 on the rank.

First consider $p = 2$. Using Eq. (6) and the fact that $\#J_1[\phi](\mathbb{Q}_2) = 5^1$, and $\#\widetilde{J}_1[\tilde{\phi}](\mathbb{Q}_2) = 5^0$, we have

$$\#\widetilde{J}_1(\mathbb{Q}_2)/\phi(J_1(\mathbb{Q}_2))\,\#J_1(\mathbb{Q}_2)/\tilde{\phi}(\widetilde{J}_1(\mathbb{Q}_2)) = 5^1.$$

Note that substituting $x = -2$ into the quintic of $\widetilde{\mathcal{C}}_1$ gives $-2^8 \cdot 330\,047$, which is a square in $\mathbb{Q}_2$. Let $y_0 \in \mathbb{Q}_2$ be such that $y_0^2 = -2^8 \cdot 330\,047$ with $y_0 \equiv 48 \pmod{64}$. Then $q_2 : [(-2, y_0) - \infty] \mapsto [\zeta_5, \zeta_5^2]$ and $[\zeta_5, \zeta_5^2] \neq [1, 1]$ in $\mathbb{Q}_2(\zeta_5)^*/(\mathbb{Q}_2(\zeta_5)^*)^5 \times \mathbb{Q}_2(\zeta_5)^*/(\mathbb{Q}_2(\zeta_5)^*)^5$. Hence we have now found all of $\#\widetilde{J}_1(\mathbb{Q}_2)/\phi(J_1(\mathbb{Q}_2)) = 5^1$ and $\#J_1(\mathbb{Q}_2)/\tilde{\phi}(\widetilde{J}_1(\mathbb{Q}_2)) = 5^0$. Also, j_2 has trivial kernel and $\tilde{j}_2$ has kernel $\langle [(1-\sqrt{5})/2, 1], [1, 5] \rangle$. Hence

$$\begin{aligned} j_2^{-1}(q_2(\widetilde{J}_1(\mathbb{Q}_2)/\phi(J_1(Q_2)))) &= \langle [\zeta_5, \zeta_5^2] \rangle, \\ \tilde{j}_2^{-1}(\tilde{q}_2(J_1(\mathbb{Q}_2)/\tilde{\phi}(\widetilde{J}_1(Q_2)))) &= \langle [(1-\sqrt{5})/2, 1], [1, 5] \rangle. \end{aligned}$$

At this point, the bound of the rank has been lowered to 2.

We now consider $p = 5$. Using Eq. (6) and the fact that $\#J_1[\phi](\mathbb{Q}_5) = 5^1$, and $\#\widetilde{J}_1[\tilde{\phi}](\mathbb{Q}_5) = 5^0$, we have

$$\#\widetilde{J}_1(\mathbb{Q}_5)/\phi(J_1(\mathbb{Q}_5))\,\#J_1(\mathbb{Q}_5)/\tilde{\phi}(\widetilde{J}_1(\mathbb{Q}_5)) = 5^3.$$

Note that substituting $x = 1$ into the quintic of $\widetilde{\mathcal{C}_1}$ gives a square in $\mathbb{Q}_5$, so let $y_1 \in \mathbb{Q}_5$ be such that $(1, y_1) \in \widetilde{\mathcal{C}_1}(\mathbb{Q}_5)$. Then q_5 maps $[(1, y_1) - \infty]$ to a nontrivial element which is not even in the image of j_5. On $\mathcal{C}_1$, note that there is a point $(3, y_2) \in \mathcal{C}_1(\mathbb{Q}_5)$ and that $\tilde{q}_5 : [(1, y_1) - \infty] \mapsto [1, 2]$. Also $\tilde{q}_5 : T2 \mapsto [(1 - \sqrt{5})/2, 1]$. Furthermore, $[1, 2]$ and $[(1-\sqrt{5})/2, 1]$ are independent in $\mathbb{Q}_5(\sqrt{5})^*/(\mathbb{Q}_5(\sqrt{5})^*)^5 \times \mathbb{Q}^*/(\mathbb{Q}^*)^5$. We have now found all of $\#\widetilde{J_1}(\mathbb{Q}_5)/\phi(J_1(\mathbb{Q}_5)) = 5^1$ and $\#J_1(\mathbb{Q}_5)/\tilde{\phi}(\widetilde{J_1}(\mathbb{Q}_5)) = 5^2$. Also, j_5 and $\tilde{j}_5$ have trivial kernel. Hence

$$j_5^{-1}(q_5(\widetilde{J_1}(\mathbb{Q}_5)/\phi(J_1(Q_5)))) = \langle [1, 1] \rangle,$$
$$\tilde{j}_5^{-1}(\tilde{q}_5(J_1(\mathbb{Q}_5)/\tilde{\phi}(\widetilde{J_1}(Q_5)))) = \langle [(1 - \sqrt{5})/2, 1], [1, 2] \rangle.$$

Taking the intersection of the information at $p = 2$ and $p = 5$, we see that $\mathrm{im}(q)$ is the trivial group, and so $\widetilde{J_1}(\mathbb{Q})/\phi(J_1(Q))$ is the trivial group, and $\mathrm{im}(\tilde{q})$ is contained in $\langle [(1 - \sqrt{5})/2, 1] \rangle$, and indeed these are equal, since $\tilde{q} : T_2 \mapsto [(1 - \sqrt{5})/2, 1]$. We finally deduce that $\#J_1(\mathbb{Q})/5J_1(\mathbb{Q}) = 5^1$, and $\#J_1(\mathbb{Q})[5] = 5^1$, so that the rank is 0. □

The same result can also be obtained by performing a 2-descent, for example using Magma [1], which requires working over a degree 5 number field.

For the next example, we do not find completely the Selmer bound for the $(5, 5)$-isogeny, but we do enough to show that the bound is nonzero, and deduce the existence of 5-part of Ш by comparison with a complete 2-descent, for which the rank bound is 0. We first require the following technical lemma.

Lemma 7. *Let p be prime, satisfying $p \equiv 1$ or $4 \pmod 5$, and $p \equiv 3 \pmod 4$, and let $\epsilon_1 = a + b\sqrt{5p}$, with $a, b \in \mathbb{Z}$ and $a, b > 0$, be a fundamental unit of $\mathbb{Z}[\sqrt{5p}]$. Let $w_0 \in \mathbb{Q}_5$ satisfy $w_0^2 = p$ (such w_0 exists, since $p \equiv 1$ or $4 \pmod 5$). Suppose that $(w_0^5 - w_0^4\sqrt{5p})/2 = \epsilon_1^i$ in $\mathbb{Q}_5(\sqrt{5p})^*/(\mathbb{Q}_5(\sqrt{5p})^*)^5$, for some $i = 1, \ldots 4$, that a is odd, b is even, and that a is a quadratic residue mod p. Then the rank bound on $J_p(\mathbb{Q})$ from descent via $(5, 5)$-isogeny is nonzero.*

Proof. The bad primes here are: 2, 5, p, ∞. Consider whether the element $[\epsilon_1, 1]$ can be in the image of $\tilde{q}$.

First note that $[\epsilon_1, 1]$ is in the kernel of $\tilde{j}_\infty$ and so $[\epsilon_1, 1]$ cannot be disqualified by local arguments at infinity.

Let $f(x) = x^5 - \epsilon_1$, considered over $\mathbb{Q}_2(\sqrt{5p})$. Then, since a is odd and b is even, we have $|f(1)|_5 < 1$ and $|f'(1)|_2 = 1$, and so $f(x)$ has a root in $\mathbb{Q}_2(\sqrt{5p})$ by Hensel's Lemma. This means that $\epsilon_1 \in (\mathbb{Q}_2(\sqrt{5p})^*)^5$, so that $[\epsilon_1, 1]$ is in the kernel of $\tilde{j}_2$ and cannot be disqualified by local arguments at 2.

Now, let $g(x) = x^5 - \epsilon_1$, considered over $\mathbb{Q}_p(\sqrt{5p})$. Since a is a quadratic residue mod p, there exists v_0 such that $v_0^2 \equiv a \pmod p$. Then $|g(v_0)|_p < 1$ and $|g'(v_0)|_p = 1$, and so $g(x)$ has a root in $\mathbb{Q}_p(\sqrt{5p})$ by Hensel's Lemma. This means that $\epsilon_1 \in (\mathbb{Q}_p(\sqrt{5p})^*)^5$, so that $[\epsilon_1, 1]$ is in the kernel of $\tilde{j}_p$ and cannot be disqualified by local arguments at p.

Since we are given the existence of $w_0 \in \mathbb{Q}_5$ satisfying $w_0^2 = p$, we now note that $T_2 = [(0, 16p^2\sqrt{p}) - \infty] \in J_p(\mathbb{Q}(\sqrt{p}))$ has an image in $J_p(\mathbb{Q}_5)$, namely $[(0, 16p^2 w_0) - \infty] \in J_p(\mathbb{Q}_5)$, which is mapped by $\tilde{q}_p$ to $[(w^5 - w^4\sqrt{5p})/2, 1]$, which we are given to be the same as $[\epsilon_1^i, 1]$, for some $i = 1, \ldots, 4$. Hence again, $[\epsilon_1, 1]$ cannot be disqualified by local arguments at 5.

Since also $J_p[\phi](\mathbb{Q})$ and $\widetilde{J}_p[\tilde{\phi}](\mathbb{Q})$ are the trivial groups, it follows that the rank bound from descent via $(5, 5)$-isogeny is nonzero. □

Example 8. Let J_{11} be the Jacobian of the curve

$$\begin{aligned} \mathcal{C}_{11} : y^2 &= 5 \cdot 11(3x^2 - 12 \cdot 11x + 16 \cdot 11^2)^2 + (x - 4 \cdot 11)^5 \\ &= 11(5x^2 - 20 \cdot 11x + 16 \cdot 11^2)^2 + x^5. \end{aligned}$$

Then $J_{11}(\mathbb{Q})$ has a nonzero rank bound using descent via $(5, 5)$-isogeny, and a rank bound of 0 via complete 2-descent, and so there is a nontrivial element of $Ш(J_{11}/\mathbb{Q})[5]$.

Proof. Here $p = 11$ and the fundamental unit for $\mathbb{Q}(\sqrt{55})$ is $\epsilon_1 = a + b\sqrt{55} = 89 + 12\sqrt{55}$, which satisfies: a odd, b even, and $a = 89$ is a quadratic residue mod 11. Let $w_0 \in \mathbb{Q}_5$ be such that $w_0^2 = 11$, and choose $w_0 \equiv 1 \pmod 5$. Note that then $w_0 \equiv 56 \pmod{5^3}$. Consider $h(x) = x^5 - \epsilon_1^2(w_0^5 - w_0^4\sqrt{55})$. Then $|h(56 \cdot 18 + 15\sqrt{55})|_5 \leq 5^{-3}$ (as can be seen, just using the approximation 56 for w_0) and $|h'(56 \cdot 18 + 15\sqrt{55})|_5 = 5^{-1}$, so by Hensel's Lemma, $\epsilon_1^2(w_0^5 - w_0^4\sqrt{55}) \in (\mathbb{Q}_5(\sqrt{55})^*)^5$, giving that $w_0^5 - w_0^4\sqrt{55} = \epsilon_1^3$ in $\mathbb{Q}_5(\sqrt{55})^*/(\mathbb{Q}_5(\sqrt{55})^*)^5$, as required. Hence by the previous lemma, $[\epsilon_1, 1]$ represents a nontrivial element in the Selmer group, and the rank bound on $J_{11}(\mathbb{Q})$ from descent via $(5, 5)$-isogeny is nonzero.

On the other hand, performing a descent via 2-isogeny one obtains a rank bound of 0, so that there must exist a nontrivial element in $Ш(J_{11}/\mathbb{Q})[5]$. □

References

[1] The MAGMA computer algebra system is described in Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265.

[2] Nils Bruin, E. Victor Flynn, Damiano Testa, Descent via $(3, 3)$-isogeny on Jacobians of genus 2 curves, Acta Arith. 165 (2014) 201–223.

[3] Nils Bruin, Bjorn Poonen, Michael Stoll, Generalized explicit descent and its application to curves of genus 3, available at arXiv:1205.4456, 2012.

[4] 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, Cambridge, 1996, MR1406090 (97i:11071).

[5] E. Victor Flynn, Electronic resources, http://people.ox.ac.uk/flynn/genus2/pn3, 2014.

[6] Edward F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve, Math. Ann. 310 (3) (1998) 447–471, MR1612262 (99h:11063).

[7] Michael Stoll, Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell–Weil rank at least 19, C. R. Acad. Sci. Paris Sér. I Math. 321 (1995) 1341–1344.